

ZeeQuest Privacy Policy and GDPR Notice

Version 1.0 | September 2026

Effective date: 10. 9. 2026

1. Who We Are and Who Controls Your Data

ZeeQuest operates through a group structure with a global headquarters in the United States and European operations in Slovenia.

Global headquarters: ZeeQuest Inc., 16192 Coastal Highway, Lewes, Delaware 19958, United States of America.

European headquarters: ZeeQuest, Inc d.o.o., Partizanska cesta 3, 2000 Maribor, Slovenia.

General privacy contact: privacy@zeequest.com

For visitors and users in the EEA, ZeeQuest, Inc d.o.o. is the controller responsible for the general ZeeQuest website processing described in this Privacy Policy. ZeeQuest Inc. in the United States may receive personal data for specified group-level activities as described below.

Where a specific ZeeQuest product or program identifies another entity as controller, that product's specific privacy notice will apply to that processing.

2. Scope

This notice applies to personal data processed through zeequest.com and general ZeeQuest website functions, including contact forms, general account access, newsletters and communications, event or cooperation enquiries, general community interactions, website analytics, security and administration.

It does not replace product-specific notices for services such as Daty.ai, Navigator, iUnity, Pioneer programs, Pioneer Hubs, investment/crowdfunding activities, health-related services or other ventures where additional categories of data, purposes or legal bases apply.

3. Personal Data We May Collect

- Identity and contact data: name, surname, email address, telephone number, country, company and professional role.
- Account data: login identifier, account status, authentication and security information.
- Enquiry and relationship data: information submitted through contact, cooperation, partnership, event, institutional or business-development forms.
- Communications data: messages, support requests, correspondence and records of interactions with us.
- Technical data: IP address, browser/device information, operating system, language, timestamps, security logs and similar technical identifiers.
- Usage data: pages viewed, interactions, referral source, session and website-performance information, subject to applicable cookie/consent rules.
- Marketing preferences: newsletter subscription, communication preferences and consent records.
- Transaction-related data where applicable: order/reference information, billing details and transaction status. Payment-card data is processed directly by the relevant payment provider and is not stored by ZeeQuest.
- Event/community data where applicable: registrations, attendance, city/country, professional affiliation and participation information.
- Other information you voluntarily provide.

The general ZeeQuest website does not intentionally request health data, biometric data, precise relationship-profile data or other special-category personal data. Where a specific service processes such data, it will provide a separate privacy notice and identify the applicable lawful basis.

4. How We Collect Data

- Directly from you when you complete forms, create an account, subscribe, communicate with us, register for an event or request information.
- Automatically from your device when you use the website, subject to cookie and tracking choices.
- From ZeeQuest group companies where lawful and necessary for group administration or delivery of a request.
- From business partners, event partners or introducers where they are lawfully permitted to provide the data and the required Article 14 information is provided.
- From publicly available professional/business sources where permitted by law and relevant to legitimate business-development activities.

5. Why We Use Personal Data and Our Legal Bases

Purpose	Typical data	GDPR legal basis
Respond to enquiries and requests	Identity, contact, communications	Art. 6(1)(b) pre-contractual steps and/or Art. 6(1)(f) legitimate interests
Provide accounts/general website services	Identity, account, technical	Art. 6(1)(b) contract
Security, fraud prevention and system integrity	Technical, account, usage	Art. 6(1)(f) legitimate interests; legal obligation where applicable
Website measurement and non-essential analytics	Device, usage, identifiers	Consent where required by ePrivacy/cookie law; otherwise applicable lawful basis
Direct electronic marketing	Contact, preferences	Consent where required; legitimate interests only where legally permitted
Business/partnership development	Professional identity, company, communications	Art. 6(1)(f) legitimate interests and/or Art. 6(1)(b) pre-contractual steps
Events/community administration	Identity, contact, event data	Art. 6(1)(b), consent where appropriate, and/or Art. 6(1)(f)
Legal, tax, compliance and dispute management	Relevant records	Art. 6(1)(c) legal obligation and/or Art. 6(1)(f) legitimate interests
Improve general website/services	Usage, feedback, technical	Art. 6(1)(f), or consent where tracking technologies require it

Where we rely on legitimate interests, we assess the relevant business need against the impact on individuals and apply safeguards. Where consent is the legal basis, you may withdraw it at any time without affecting processing already carried out lawfully.

6. Cookies and Similar Technologies

We use strictly necessary technologies required for website operation and may use analytics, preference, advertising or social-media technologies where permitted. We do not activate non-essential cookies or similar technologies requiring consent until you have provided valid consent. Further information about cookie categories, providers, durations and available choices is provided in the ZeeQuest Cookie Policy and Cookie Preferences.

7. Who Receives Personal Data

Depending on the relevant function, recipients may include:

- ZeeQuest group entities where access is necessary and legally justified.
- Hosting, cloud, security, IT, communications, support and infrastructure providers.
- Analytics and website technology providers where enabled under the user's consent choices.
- Email/newsletter and customer-relationship-management providers.
- Payment providers for transactions, where applicable.
- Professional advisers such as lawyers, accountants, auditors and compliance advisers.
- Event, project or business partners where disclosure is necessary for the relevant request and legally permitted.
- Public authorities, courts or regulators where disclosure is legally required.
- A purchaser, investor or successor in connection with a genuine corporate transaction, subject to appropriate confidentiality and data-protection safeguards.

Processors acting on our behalf are required to process personal data under appropriate contractual instructions and security/confidentiality obligations.

8. International Transfers

Because ZeeQuest has operations and service providers in different countries, personal data may be accessed from or transferred outside the EEA. A transfer outside the EEA is made only where a valid transfer mechanism and appropriate safeguards are in place.

Depending on the destination and recipient, ZeeQuest will use one or more of the following mechanisms:

- An adequacy decision adopted by the European Commission under Article 45 GDPR.
- For eligible United States recipients that are actively certified under the EU-U.S. Data Privacy Framework
- The European Commission's 2021 Standard Contractual Clauses ('SCCs') under Article 46 GDPR where an adequacy mechanism does not apply.
- Where SCCs are used, a transfer impact assessment and supplementary technical/organizational measures where required by the circumstances.
- Another lawful GDPR transfer mechanism, such as approved Binding Corporate Rules, certification/code mechanisms or a narrowly applicable Article 49 derogation, where legally appropriate.

Transfers to ZeeQuest Inc. in the United States must therefore be covered by an applicable lawful mechanism. Where ZeeQuest Inc. is not covered by an applicable adequacy mechanism, transfers are protected by the appropriate Standard Contractual Clauses and any supplementary safeguards required in the circumstances.

You may request information about the safeguards relevant to your personal data by contacting us. Commercially sensitive or security-sensitive information may be redacted where legally permitted.

9. Data Retention

We retain personal data only for as long as reasonably necessary for the purpose for which it was collected, including meeting legal, accounting, tax, security and dispute-resolution requirements. Retention periods are determined by data category, processing purpose and applicable legal requirements.

- General enquiries: normally retained for the active relationship and a reasonable follow-up period.
- Account records: while the account is active and for a limited period thereafter where required for security, legal or dispute purposes.
- Marketing data: until consent is withdrawn/objection is made or the data is no longer needed, with suppression records retained where necessary to respect opt-outs.
- Security logs: retained for a proportionate security period.
- Transaction/legal records: retained for the period required by applicable accounting, tax, contractual and legal rules.

Exact retention schedules should be maintained in ZeeQuest's internal Records of Processing Activities and retention policy.

10. Automated Decision-Making and AI

The general ZeeQuest website may use automation to support routing, security, personalization or administrative functions. Unless a specific service expressly tells you otherwise, the general website does not make solely automated decisions producing legal effects or similarly significant effects about you within Article 22 GDPR.

Where a ZeeQuest product uses AI, profiling or automated decision-making in a materially different way, the relevant product-specific privacy notice will explain the data used, purpose, legal basis, relevant information about the logic where required, potential consequences and applicable rights.

11. Your GDPR Rights

Subject to the conditions and exceptions in applicable law, EEA individuals may have the right to:

- Access personal data and obtain information about its processing.
- Correct inaccurate or incomplete personal data.
- Request erasure.
- Request restriction of processing.
- Object to processing based on legitimate interests, including the right to object at any time to direct marketing.
- Receive applicable data in a portable format.
- Withdraw consent at any time where processing relies on consent.
- Not be subject to certain solely automated decisions with legal or similarly significant effects.
- Lodge a complaint with a competent supervisory authority.

For Slovenia, the supervisory authority is the Information Commissioner of the Republic of Slovenia (Informacijski pooblaščenec). You may also complain to the supervisory authority in the EEA country of your habitual residence, place of work or the alleged infringement.

12. How to Exercise Your Rights

Send privacy requests to privacy@zeequest.com. We may need to verify your identity before acting on a request. We will respond within the period required by applicable law and will explain if an extension or lawful exception applies.

We do not require you to create an account merely to exercise privacy rights. Requests are generally free of charge, although GDPR permits a reasonable fee or refusal for manifestly unfounded or excessive requests in limited circumstances.

13. Security

We use appropriate technical and organizational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Measures are selected according to risk and may include access controls, encryption, secure development and configuration practices, logging, backups, incident procedures, vendor controls and staff confidentiality obligations.

No internet or information system can be guaranteed to be completely secure. Where a personal-data breach triggers statutory notification duties, we will act in accordance with applicable law.

14. Children

The general ZeeQuest website is not intended to collect personal data from children for account, commercial or investment-related participation. Where a specific ZeeQuest product is intended for younger users, separate age requirements, parental-consent procedures where applicable, safeguards and a product-specific privacy notice will apply.

15. Third-Party Websites and Services

Our website may link to third-party websites, social networks, platforms or services. Their processing is governed by their own privacy notices where they act independently. We encourage users to review those notices before providing personal data.

16. Changes to This Privacy Policy

We may update this Privacy Policy when our processing, technology, group structure or legal obligations change. The current version and effective date will be published on the website. Where a change materially affects individuals, we will provide additional notice where required.

A change to this Privacy Policy does not retroactively convert a processing activity to consent-based processing or replace any consent that applicable law requires us to obtain.

17. Contact

European privacy/controller contact:

ZeeQuest, Inc d.o.o.
Partizanska cesta 3
2000 Maribor
Slovenia

Privacy: privacy@zeequest.com

Global headquarters:

ZeeQuest Inc.
16192 Coastal Highway
Lewes, Delaware 19958
United States of America
info@zeequest.com