

Privacy Policy

Effective date: 10 July 2025

This Privacy Policy explains how Algarve Quest collects, uses, stores and protects personal data when you visit <https://algarve-quest.com>, purchase or use our quests, contact us, or otherwise use our services. We process personal data in accordance with applicable data protection legislation, including the EU General Data Protection Regulation (GDPR) and applicable Portuguese law.

1. Who We Are

Algarve Quest is operated by:

YULIA MAXIMOVA

NIF: [286754096](#)

Travessa do Poejo 25 RC C

8200-252 Albufeira

Portugal

WhatsApp: [+351 911 540 083](#) (messages only; no phone calls)

Email: Algarvequest@gmail.com

Website: <https://algarve-quest.com>

For the purposes of applicable data protection law, YULIA MAXIMOVA is the data controller for personal data processed for the purposes described in this Privacy Policy.

2. Personal Data We May Collect

The categories of personal data we process depend on how you use our website and services.

Information You Provide

When you purchase or use our services, contact us or voluntarily provide information, we may process:

- name and surname;
- email address;
- country or city of residence, if voluntarily provided;
- information contained in communications with customer support;
- information relating to participation in quests where necessary for the operation of the service;
- reviews, comments or other content that you voluntarily submit.

Technical Information

When you visit our website, certain technical information may be collected automatically, depending on the technologies used on the website. This may include:

- IP address;
- browser type and version;
- device type;
- operating system;
- date and time of access;
- technical information about interactions with the website.

The exact information collected automatically depends on the website configuration, cookies and analytics technologies in use.

3. Payment Information

Payments are processed through Stripe.

We do not store full payment card details, such as the complete card number or CVC, on our own servers. During payment, Stripe may collect and process information necessary to process the transaction, prevent fraud and comply with applicable legal requirements.

Depending on the payment method and Stripe's requirements, this may include:

- name;
- email address;
- payment card or other payment information;
- transaction details;

- IP address;
- device and browser information;
- information used for fraud prevention and payment security.

Payment processing is subject to Stripe's applicable terms and privacy practices.

Stripe Privacy Policy:

<https://stripe.com/privacy>

4. How We Use Personal Data

We may process personal data for the following purposes.

Providing the Service

- processing purchases;
- providing access to purchased quests;
- sending access links or other access information;
- providing customer support;
- responding to enquiries and requests.

Payments, Accounting and Legal Obligations

- processing and confirming payments;
- maintaining required accounting and financial records;
- complying with tax and other legal obligations.

Security and Fraud Prevention

- protecting the website and service;
- preventing fraud, abuse and unauthorised use;
- identifying and resolving technical or security problems.

Service Improvement

Where we have an appropriate legal basis, we may use technical and statistical information to understand how the website operates, identify errors and improve the service and user experience.

Marketing Communications

We may send marketing or promotional communications where required consent has been obtained or another lawful basis applies.

You can unsubscribe from marketing communications at any time.

5. Legal Bases for Processing

Depending on the purpose, we may process personal data on the following legal bases under the GDPR:

- **Performance of a contract** — for example, to process a purchase and provide access to a purchased quest;
- **Legal obligation** — for example, to comply with accounting, tax and other legal requirements;
- **Legitimate interests** — for example, to maintain service security, prevent fraud and improve the service, where our interests are not overridden by your rights and freedoms;
- **Consent** — for example, for certain marketing communications or non-essential cookies and analytics technologies where consent is legally required.

Where processing is based on consent, you may withdraw your consent at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

6. Cookies and Analytics

Our website may use cookies and similar technologies.

Some cookies may be necessary for the operation of the website and for providing functionality requested by the user.

Non-essential analytics or marketing cookies will be used in accordance with applicable legal requirements and, where required, only after the appropriate consent has been obtained.

If Google Analytics or another analytics service is enabled on the website, the applicable cookie consent mechanism will provide the relevant information and choices.

You can also manage cookies through your browser or the cookie settings provided on the website. Disabling certain cookies may affect some website functionality.

7. Third-Party Service Providers and Data Sharing

We may use third-party service providers to operate the website and provide our services. Depending on the services actually used, these providers may include:

- **Stripe** — payment processing;
- email service providers — transactional and service-related communications;
- hosting and technical infrastructure providers;
- analytics providers, where used;
- other technical service providers necessary to operate the website and service.

We may also disclose personal data to public authorities or other persons where required by applicable law or where necessary to establish, exercise or defend legal claims.

We do not sell users' personal data.

8. International Data Transfers

Some service providers may process personal data outside the European Economic Area (EEA).

Where personal data is transferred outside the EEA, we use appropriate safeguards required by applicable data protection law, which may include European Commission Standard Contractual Clauses or another lawful transfer mechanism.

9. Data Retention

We retain personal data only for as long as necessary for the purposes for which it was collected or for as long as required by applicable law.

For example, certain purchase, payment and accounting information may need to be retained for the period required by tax, accounting and other legal obligations.

Personal data may also be retained for as long as reasonably necessary to establish, exercise or defend legal claims or protect our legitimate interests.

When personal data is no longer required, it will be deleted or otherwise securely disposed of where reasonably practicable.

10. Data Security

We use appropriate technical and organisational measures designed to protect personal data against unauthorised access, alteration, disclosure, loss or destruction.

Depending on the circumstances, these measures may include:

- HTTPS/SSL encryption;
- access controls;
- restricted access to personal data;
- use of reputable and appropriately secured service providers;
- security updates and other technical safeguards.

No method of transmission or storage over the internet can guarantee absolute security.

11. Your Data Protection Rights

Subject to the conditions and limitations established by applicable law, you may have the right to:

- request access to your personal data;
- request correction of inaccurate or incomplete personal data;
- request erasure of personal data;
- request restriction of processing;
- object to certain processing;
- request data portability where applicable;
- withdraw consent where processing is based on consent;

...