

FHS ENTERPRISES LIMITED

PRIVACY POLICY

How we collect, use and protect your personal information

Effective / last updated: August 2026

1. Introduction and scope

FHS Enterprises Limited (“FHS”, “we”, “us” or “our”) respects your privacy and is committed to protecting personal data. This Privacy Policy explains how we collect, use, disclose, retain and protect personal data when you visit www.fhsenterprises.eu, contact us, submit an enquiry, engage us for services, interact with us in a business or professional capacity, or otherwise provide personal data to us.

This Policy is intended to provide the information required by Regulation (EU) 2016/679 (the General Data Protection Regulation or “GDPR”) and the applicable data protection laws of the Republic of Cyprus, including Law 125(I)/2018, as amended or replaced from time to time.

This Policy applies to personal data relating to living individuals. It does not create contractual rights beyond those provided by applicable law.

2. Who is responsible for your personal data?

For the processing activities described in this Policy, the data controller is:

FHS Enterprises Limited
13 Christou Keli Street
Mesa Chorio, 8290
Paphos, Cyprus
Email: info@fhsenterprises.eu

Where another professional adviser, financial services provider, lawyer, accountant, bank, insurer, immigration professional or other third party determines independently how and why it processes your personal data, that party will normally act as a separate data controller and its own privacy notice will apply to its processing.

3. Personal data we may collect

Depending on how you interact with us and the services involved, we may collect or process the following categories of personal data:

- Identity data, such as name, title, date of birth and, where legitimately required, identification or passport information.
- Contact data, such as postal address, email address and telephone number.
- Professional and business data, such as employer, job title, business ownership, company details and information relevant to a business, HR, employment, operational, contractual or compliance matter.

- Financial and transactional data where relevant to services, introductions, billing, payments, financial-services related enquiries or lawful due-diligence requirements.
- Residency, relocation and Cyprus-establishment information where relevant to an enquiry or service.
- Correspondence and enquiry data, including information you provide through our website contact form, email, telephone, messaging services, meetings or other communications.
- Technical and usage data, which may include IP address, browser/device information, approximate location derived from IP address, referring pages, pages viewed, timestamps, diagnostic information and similar website/server information.
- Marketing and communication preferences.
- Any other personal data that you voluntarily provide to us or that is reasonably necessary for a lawful purpose connected with our relationship with you.

4. Special categories of personal data

We do not seek to collect special categories of personal data through the website as a matter of course. However, information concerning health, trade-union membership or other special-category data may occasionally arise in HR, employment, employee-benefit or other professional matters. Where we process such information, we will do so only where a lawful basis under Article 6 GDPR and an applicable condition under Article 9 GDPR exist, and with appropriate safeguards.

Please do not send sensitive or special-category personal data through the general website contact form unless it is necessary for your enquiry.

5. How we collect personal data

We may collect personal data:

- directly from you when you complete a form, email or call us, meet with us, instruct us, request information or otherwise communicate with us;
- from a business, employer, colleague, family member, representative or other person where there is a lawful reason for them to provide the information;
- from professional advisers, service providers, business partners or referral sources where appropriate and lawful;
- from public registers, public websites, professional directories and other lawfully accessible public sources;
- from website, hosting, security, analytics and communications technologies used in operating our website and business; and
- where necessary, from third parties for verification, compliance, due diligence or service-delivery purposes.

Where we obtain personal data about you from a source other than you, we will provide the information required by Article 14 GDPR where applicable, subject to the exceptions permitted by law.

6. Purposes and lawful bases for processing

We process personal data only where we have a lawful basis. Depending on the circumstances, our purposes and lawful bases may include:

Purpose	Typical lawful basis	Examples
Responding to enquiries and taking steps before engagement	Legitimate interests; steps at your request before entering a contract	Responding to contact forms, calls and emails; assessing how we may assist.
Providing and administering services	Performance of a contract; legitimate interests	Client administration, communications, coordination, introductions and service delivery.
Operating and improving our business and website	Legitimate interests	Website administration, service improvement, record management, troubleshooting and business continuity.
Security and fraud prevention	Legitimate interests; legal obligation where applicable	Protecting systems, detecting misuse, maintaining audit/security logs.
Legal, regulatory, tax, accounting and compliance obligations	Legal obligation; legitimate interests where appropriate	Required records, responding to lawful authorities, due diligence or compliance requirements applicable to us.
Establishing, exercising or defending legal claims	Legitimate interests; applicable GDPR conditions for special-category data where relevant	Dispute management, professional advice, evidence and legal proceedings.
Professional introductions and coordination	Performance of a contract; steps at your request; legitimate interests; consent where required	Introducing or coordinating with lawyers, accountants, banks, insurers, financial professionals, property professionals or other service providers where relevant.
Direct marketing and relationship communications	Consent where required; otherwise legitimate interests where permitted by law	News, insights or service information relevant to existing or prospective business relationships.

Where we rely on legitimate interests, we consider whether those interests are necessary and proportionate and whether your interests, rights or freedoms override them. You may object to processing based on legitimate interests in the circumstances described in section 15.

7. If you do not provide personal data

Where we need personal data to comply with law, respond meaningfully to an enquiry, enter into or perform a contract, or provide a requested service, failure to provide the necessary information may mean that we cannot proceed with the enquiry, engagement or service. We will seek to explain this where relevant.

8. Website, server logs, analytics and similar technologies

When you use our website, our hosting platform and related technical service providers may process technical information necessary to deliver, secure, maintain and diagnose the website. This may include IP addresses, browser/device information, timestamps, requested pages, referring information and security or diagnostic logs.

We may also use analytics or similar technologies to understand website usage and improve the website. Where applicable law requires consent for non-essential cookies or similar technologies, such technologies should not be activated until the required consent has been obtained.

The precise cookies and similar technologies in use may change as the website or its service providers change. Where a cookie banner or cookie settings tool is provided, you should use it to manage non-essential cookie preferences. This Privacy Policy should be read together with any cookie information displayed on the website.

9. Contact forms and communications

If you submit an enquiry through our website, we process the information you enter in the form, together with relevant technical information associated with the submission, for the purpose of receiving, routing, responding to and retaining the enquiry as reasonably necessary.

Website forms and website infrastructure may be provided or supported by third-party technology providers acting on our behalf. We require service providers that process personal data on our behalf to process it only for authorised purposes and subject to appropriate data-protection obligations.

10. Marketing communications

We may send service information, insights or marketing communications where permitted by applicable law. Where consent is required, we will rely on consent. In other circumstances, we may rely on legitimate interests where the law permits this, taking account of your rights and reasonable expectations.

You can ask us to stop sending direct marketing at any time by using any unsubscribe facility provided or by emailing info@fhsenterprises.eu. Opting out of marketing will not prevent us from sending service, transactional, legal or administrative communications that are necessary for an existing relationship.

11. Sharing personal data

We do not sell personal data. We may disclose personal data where reasonably necessary and lawful to:

- website hosting, IT, cybersecurity, email, communications, cloud-storage, document-management and other technology service providers;
- accountants, auditors, insurers and other professional advisers;
- lawyers, accountants, tax advisers, banks, insurers, financial services professionals, property professionals, immigration or residency professionals, corporate service providers and other specialists where relevant to an enquiry or service and where disclosure is lawful;
- government departments, regulators, courts, law-enforcement bodies, tax authorities or other competent authorities where required or permitted by law;

- a purchaser, investor, successor or adviser in connection with a genuine or proposed reorganisation, merger, acquisition, sale or transfer of all or part of our business, subject to appropriate confidentiality and data-protection safeguards; and
- other persons where you have authorised the disclosure or where another lawful basis permits or requires it.

Third parties may act as processors on our instructions or as independent controllers, depending on their role. Where a third party is an independent controller, its own privacy notice and legal responsibilities apply.

12. International transfers

Some service providers or recipients may process personal data outside the European Economic Area (“EEA”). Where personal data are transferred to a country outside the EEA that is not covered by an applicable European Commission adequacy decision, we will use an appropriate transfer mechanism where required, such as the European Commission’s Standard Contractual Clauses, together with supplementary safeguards where appropriate, or rely on another lawful derogation or transfer basis permitted by the GDPR.

You may contact us for further information about the safeguards applicable to a relevant international transfer.

13. Data security

We take appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Measures are selected having regard to the nature of the data, the processing, available technology, implementation costs and the risks presented.

Access to personal data is restricted to persons who reasonably require it for authorised purposes. Where third-party processors are used, appropriate contractual and security obligations are applied as required by law.

No internet transmission or information system can be guaranteed to be completely secure. You should therefore use appropriate care when transmitting confidential or sensitive information electronically.

14. Data retention

We retain personal data only for as long as reasonably necessary for the purposes for which it was collected, including to provide services and to meet legal, regulatory, tax, accounting, reporting, insurance, compliance, evidential and dispute-resolution requirements.

Retention periods vary according to the nature of the information and the relationship. In determining the appropriate period, we consider the amount, nature and sensitivity of the data; the risk of harm from unauthorised use or disclosure; the purposes of processing; whether those purposes can be achieved by other means; applicable limitation periods; and legal or regulatory requirements.

When personal data are no longer required, we will delete or anonymise them, subject to lawful backup, archival or record-retention requirements.

15. Your data protection rights

Subject to the GDPR and any applicable limitations or exemptions, you may have the right to:

- request access to your personal data and information about how it is processed;
- request correction of inaccurate or incomplete personal data;
- request erasure of personal data in circumstances where the right to erasure applies;
- request restriction of processing in applicable circumstances;
- object to processing based on legitimate interests, including the right to object at any time to processing for direct marketing;
- request data portability for certain data processed by automated means on the basis of consent or contract;
- withdraw consent at any time where processing is based on consent, without affecting the lawfulness of processing before withdrawal;
- not be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects, where Article 22 GDPR applies; and
- lodge a complaint with a competent data-protection supervisory authority.

These rights are not absolute. The GDPR and other applicable laws may permit or require us to refuse, restrict or defer a request in particular circumstances.

16. Exercising your rights and response times

To exercise a data-protection right, please contact info@fhspartnerprises.eu. We may request information reasonably necessary to verify your identity and to ensure that personal data are not disclosed to an unauthorised person.

We will respond without undue delay and, in any event, within one month of receiving a valid request, as required by the GDPR. Where permitted by the GDPR, this period may be extended by up to two further months where necessary because of the complexity or number of requests. If an extension is required, we will inform you within the initial one-month period and explain the reasons.

Requests are generally dealt with free of charge. Where a request is manifestly unfounded or excessive, in particular because of its repetitive character, the GDPR permits us to charge a reasonable fee reflecting administrative costs or to refuse to act, subject to the requirements of the GDPR.

17. Complaints

If you have a concern about how we process your personal data, please contact us at info@fhspartnerprises.eu so that we have an opportunity to address it.

You also have the right to lodge a complaint with the Office of the Commissioner for Personal Data Protection in the Republic of Cyprus, which is the supervisory authority responsible for monitoring application of the GDPR and Cyprus data-protection law. You may also have the right to complain to another competent supervisory authority where the GDPR permits.

Office of the Commissioner for Personal Data Protection

P.O. Box 23378

1682 Nicosia, Cyprus

Email: commissioner@dataprotection.gov.cy

Telephone: +357 22 818 456

18. Third-party websites and external services

Our website may contain links to, or integrations with, third-party websites, social-media platforms, maps, applications or services. Those third parties may process personal data independently from us. We do not control their processing and this Privacy Policy does not govern their activities. You should review the privacy information provided by the relevant third party before providing personal data or using its services.

19. Automated decision-making

FHS does not intend to make decisions about individuals based solely on automated processing, including profiling, that produce legal effects or similarly significantly affect them. If this changes, we will provide the information and safeguards required by applicable law.

20. Children

Our website and services are not directed to children, and we do not knowingly seek to collect personal data from children through the general website. If personal data relating to a child are legitimately required in connection with a professional matter or service, we will process them only where there is an appropriate lawful basis and with safeguards appropriate to the circumstances.

21. Accuracy of personal data

Please inform us if personal data you have provided changes. We take reasonable steps to keep personal data accurate and up to date where this is necessary for the purposes for which it is processed.

22. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in law, regulatory guidance, our services, our website or our processing activities. The current version will be published on our website and the “last updated” date will be revised where appropriate. Material changes may be brought to your attention by additional means where required by law.

23. Contact us

Questions about this Privacy Policy, our processing of personal data or the exercise of data-protection rights should be sent to:

FHS Enterprises Limited

Email: info@fhsenterprises.eu

13 Christou Keli Street, Mesa Chorio, 8290, Paphos, Cyprus