

Website Privacy Notice

Explains how Paulioskos collects, uses, shares, protects and retains personal information obtained through the public website and related business communications.

Version 1.2

Effective 7 September 2026

Last reviewed 7 September 2026

Owner: HR & Compliance Director

Documents are reviewed periodically and whenever there is a material change to our services, controls, suppliers, legal obligations or risk profile.

1. Who we are

Paulioskos Tech Consulting Ltd is a private limited company incorporated in England and Wales (company number 17354568). The company operates the website and is the controller for the personal-information processing described in this notice under the Paulioskos name.

This notice applies to www.paulioskos.com, the public enquiry channel and related pre-contract or business communications. Separate contractual, supplier, workforce or client-specific privacy information may apply after a formal relationship begins.

Current legal status. Paulioskos Tech Consulting Ltd is incorporated in England and Wales under company number 17354568. The registered office is Unit A, 82 James Carter Road, Mildenhall, IP28 7DE. The company is pre-trading and VAT registered under number 526 9835 50 from 22 July 2026. Privacy enquiries can be sent to privacy@paulioskos.com.

2. Information we collect

- **Public enquiry information.** Name, company, business email address, optional telephone number, area of interest, message content and any information voluntarily supplied.
- **Business relationship information.** Job title, organisation, professional contact details, meeting or call notes, correspondence, proposals, quotations, contracts, statements of work, actions and decisions.
- **Technical and security information.** IP address, user-agent or browser details, timestamps, requested URLs, security events, validation outcomes, error records, mail-delivery metadata and operational logs where generated.
- **Project and service information.** Technical, operational and commercial information needed to understand requirements, prepare proposals and deliver agreed work.
- **Supplier and adviser information.** Professional contact and engagement information needed to manage suppliers, delivery partners, accountants, legal advisers, insurers and other business relationships.
- **B2B prospect information.** Limited public professional information used for manually targeted business-to-business prospecting, such as name, role, employer, public business contact details, source, relevance, contact outcome and objections.

The public form does not accept file uploads and does not contain a marketing opt-in. Paulioskos does not ordinarily request passwords, authentication secrets, private keys, special-category personal information or criminal-offence information through routine enquiries. Please do not submit them.

3. Public enquiry form

Field	Status and limit
Name	Required; maximum 120 characters.
Company	Optional; maximum 120 characters.
Email	Required; maximum 180 characters and email-format validation.
Phone	Optional; maximum 80 characters.
Area of interest	General consultancy is selected by default; service categories may also be selected.
Message	Required; 20 to 5,000 characters.
Anti-spam field	A hidden honeypot field must remain blank. Server-side validation and submission rate limiting also apply.
Generated data	IP address, user-agent, date/time, enquiry reference and initial workflow status are recorded.

4. How and why we use information

Purpose	Typical lawful basis
Responding to enquiries and pre-contract scoping	Steps requested before a contract where the requester is an individual or sole trader; legitimate interests for general business correspondence or corporate contacts.
Proposals, contracts and service delivery	Contract where the individual is the contracting party; legitimate interests where corporate-client employees, representatives, suppliers or stakeholders must be contacted.
Security, abuse prevention and technical logging	Legitimate interests in protecting systems, communications and operations; legal obligation where processing or disclosure is required by law.
Accounting, taxation and business administration	Legal obligation for statutory records; contract or legitimate interests for routine invoicing and account administration.
Privacy rights, complaints and legal claims	Legal obligation and legitimate interests in investigating concerns, obtaining advice and establishing, exercising or defending legal rights.
Limited B2B prospecting	Legitimate interests, subject to a documented balancing assessment, applicable PECR rules, TPS/CTPS screening, internal suppression and the absolute right to object to direct marketing.
Consent	Used only where a specific activity or communication method requires consent. It is not relied upon for ordinary enquiries or routine service delivery.

Paulioskos does not use website enquiry information for solely automated decisions producing legal or similarly significant effects. It does not currently operate automated lead scoring, behavioural profiling, bulk email marketing or remarketing.

5. Where information comes from

- Directly from you through the website, email, telephone calls, meetings and business documents.
- From your organisation, colleagues, clients, suppliers, mutual contacts, authorised representatives or professional advisers.
- From public business sources such as company websites, Companies House, LinkedIn and professional directories.
- Automatically from Cloudflare, the reverse proxy, the website application, Microsoft services and hosting or security systems when they create technical records.

Where information comes from another source, Paulioskos will identify or record the source, use only what is reasonably necessary, take proportionate steps to check accuracy and provide privacy information at the first communication or within the applicable transparency period unless an exception applies.

6. Sharing, suppliers and international processing

Paulioskos shares personal information only where necessary for the stated purpose, subject to confidentiality, access control and data minimisation. Recipient categories currently include:

Provider or recipient	Purpose and transfer position
SSD Nodes / Strasmore	Hosts the production website and enquiry database on a VPS in Amsterdam, Netherlands. UK-to-EEA transfers may rely on UK adequacy; provider terms and processor obligations also apply.
Cloudflare	Provides DNS, CDN, TLS edge, reverse proxy and security filtering. Traffic and security metadata may be processed globally under Cloudflare contractual and transfer safeguards.
Microsoft 365, Exchange Online, Entra ID and Microsoft Graph	Provides email, shared mailboxes, identity and controlled message delivery. Microsoft may process data in the UK, EEA and other authorised locations under its service terms and transfer safeguards.
GitHub	Provides source control and deployment history. Live enquiry records, database content, secrets and backups are excluded from GitHub by design.
Veeam and Paulioskos-controlled backup infrastructure	Protects the production VPS. Recovery copies may contain website, database, configuration and log information. Repository assurance is managed as an internal control.
LinkedIn and public business sources	Used only for limited manual B2B prospect research. Website enquiry records are not uploaded to LinkedIn.
Professional advisers, insurers and authorities	Minimum necessary information may be disclosed to accountants, solicitors, insurers, regulators, courts, HMRC or law enforcement where necessary and lawful.
Approved consultants and delivery partners	Limited project contact or stakeholder information may be shared under written confidentiality, access

Provider or recipient	Purpose and transfer position
	and data-protection controls, with client approval where required.

Where information is transferred outside the UK, Paulioskos uses an available lawful mechanism such as UK adequacy regulations, an applicable provider data-processing agreement, the UK International Data Transfer Agreement or the UK Addendum to standard contractual clauses, as appropriate.

7. Retention and secure disposal

Record type	Normal retention
Unconverted website enquiries	Delete promptly once qualified out; no later than 30 days after the last meaningful contact. If qualified in, transfer only necessary information and delete the original enquiry within 30 days.
Signed contracts, statements of work and client delivery records	Six years after the client relationship ends, unless a longer period is justified by law, a legal hold or an active claim.
Unsuccessful or expired proposals	Twelve months after expiry or last meaningful contact.
Accounting and transaction records	Six years from the end of the relevant accounting period, or longer where HMRC, a continuing transaction or another legal requirement applies.
Routine security and access logs	Normally 90 days. Security-event evidence may be retained for up to 12 months after closure, or longer where an investigation, complaint, legal hold or continuing threat requires it.
Unsolicited recruitment approaches	Delete immediately after identification; operational maximum seven calendar days. No candidate database or talent pool is maintained.
Privacy complaints and rights cases	Six years after closure, followed by secure deletion or anonymisation.
Vulnerability reports	Reporter identity and contact details: three years after closure. Anonymised finding and remediation evidence: six years.
B2B prospecting records	Twelve months after the last meaningful contact. A minimum suppression record may be retained

Record type	Normal retention
	while relevant marketing continues so that objections are honoured.

Deletion is performed from active email, database and file-storage locations. Technical logs normally expire through rotation. Deleted information may remain temporarily in protected backups until normal expiry. Backup copies are not used for routine purposes, and any relevant deletion or suppression decision must be reapplied if an older backup is restored.

Current implementation position. Automated enquiry deletion is not yet deployed. Until the controlled deletion workflow is introduced and tested, authorised administrators perform and record deletion manually.

8. Security

Paulioskos applies proportionate technical and organisational measures intended to protect personal information. These include named identities, multi-factor authentication for administrative access, role-based access, restricted management routes, HTTPS, source and secret separation, controlled changes, operational logging, daily VPS protection, incident procedures and periodic access review.

Microsoft 365 uses provider-managed encryption at rest. Paulioskos does not claim that every self-hosted disk or backup repository has been independently verified as encrypted at rest. No internet or cloud service can be guaranteed completely secure.

9. Your rights

- to be informed about the use of your personal information;
- to request access to personal information held about you;
- to ask for inaccurate information to be corrected;

- to request erasure or restriction in applicable circumstances;
- to object to processing based on legitimate interests and to object at any time to direct marketing;
- to receive certain information in a portable format where the legal conditions apply; and
- to withdraw consent where processing relies on consent.

Rights are not absolute. Paulioskos may need to verify identity or representative authority before disclosing or changing information. The normal response period is one month once any necessary verification has been received.

10. Children and sensitive information

The website is directed primarily at businesses, professional users and commercial contacts. It is not designed or marketed for children. Paulioskos does not intentionally collect children's information, special-category information or criminal-offence information through the public website. If unnecessary information is received unexpectedly, access will be restricted and it will be deleted or returned where appropriate.

11. Cookies and similar technologies

The separate Cookie Notice explains cookies, browser storage, scripts and third-party resources. No analytics, advertising, remarketing or session-replay technology is currently intended. Optional technology will not be activated without an appropriate choice mechanism where consent is required.

12. Complaints

Please raise a concern with Paulioskos first so that it can be investigated. Data-protection complaints may be sent to privacy@paulioskos.com. Paulioskos will acknowledge a complaint within 30 days and aims to respond much sooner, ordinarily within 14 days where the issue is straightforward. You may also complain to the Information Commissioner's Office.

Contact

Route	Details
Website	https://www.paulioskos.com
General enquiries	paul@paulioskos.com
Privacy and rights	privacy@paulioskos.com
Postal correspondence	Postal correspondence may be sent to the registered office: Unit A, 82 James Carter Road, Mildenhall, IP28 7DE.
UK regulator	Information Commissioner's Office - complaint routes

13. Changes to this notice

Paulioskos may update this notice when the business, website, suppliers, legal requirements or processing activities change. The current version, effective date and last-reviewed date will be published in the Trust Centre. The notice is reviewed periodically and after material change.

Reference framework

These references explain the legal and good-practice framework used when preparing this document. They do not represent certification, accreditation, endorsement or legal advice.

- [ICO - Right to be informed](#)
- [ICO - A guide to lawful basis](#)
- [ICO - Direct marketing and PECR](#)
- [ICO - Data protection complaints](#)
- [Data Protection Act 2018](#)
- [Data \(Use and Access\) Act 2025](#)

[← Back to the Trust Centre](#)