

Compliance & Assurance Statement

Explains the governance, evidence and assurance approach used by Paulioskos without overstating certification, insurance or universal regulatory compliance.

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. Governance approach

- **Documented ownership.** Policies, system records and material procedures have a named owner, version, status and review point.
- **Risk-based decisions.** Security, privacy, continuity and delivery risks are recorded and treated, accepted, transferred or avoided by an appropriate owner.
- **Controlled change.** Material changes are tested, documented, version controlled and capable of rollback where practical.
- **Evidence retention.** Approvals, test results, configuration records, backup evidence and incident actions are retained according to business, legal and security need.
- **Truthful assurance.** Public claims distinguish between internal practice, framework alignment, independent assessment and accredited certification.
- **Proportionate improvement.** Controls are reviewed according to risk and after material change, incident, complaint or failed test.

2. Frameworks that inform our controls

Area	Reference point	Paulioskos position
Data protection	UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025 and ICO guidance	Processing is intended to be lawful, fair, transparent, secure and proportionate. Public notices and internal records define current activities.
Cookies and electronic communications	PECR and current ICO storage/access and direct-marketing guidance	Optional technologies and marketing communications are assessed for consent, transparency, suppression and channel-specific rules.
Cyber security	NCSC 10 Steps, vulnerability-management guidance and Cyber Essentials control themes	Controls are informed by recognised technical themes. Certification is not claimed.
Information security management	ISO/IEC 27001 principles	Risk, ownership, access, evidence, incident management and improvement concepts inform working practices. Certification is not claimed.
Business continuity	ISO 22301 principles	Priority, dependency, recovery, communication, testing and improvement concepts inform continuity planning. Certification is not claimed.
Accessibility	WCAG 2.2 Level AA	This is the website design target. A recorded conformance

Area	Reference point	Paulioskos position
		assessment has not yet been completed.

3. Current certification, accreditation and insurance position

Item	Current status
ISO/IEC 27001 certification	Not held.
ISO 22301 certification	Not held.
Cyber Essentials	Not held.
Cyber Essentials Plus	Not held.
IASME Cyber Assurance	Not held.
Independent WCAG conformance certification	Not held.
Independent website penetration-test certification	Not held.
Other organisational security or privacy accreditation	None currently verified.
Professional indemnity insurance	None currently confirmed.
Public liability insurance	None currently confirmed.
Cyber insurance	None currently confirmed.
Employers' liability insurance	None currently confirmed or identified as applicable at the pre-trading stage.

VAT registration. Paulioskos Tech Consulting Ltd is VAT registered under number 526 9835 50 with effect from 22 July 2026. The company remains pre-trading; VAT registration does not indicate that trading has started.

No public statement of insurance, certification or accreditation will be made until current evidence identifies the holder, scope, issuing body, effective date and expiry date.

4. Individual experience and qualifications

Paulioskos may describe relevant professional experience factually. No specific technology-vendor, security, ISO or other professional certification is currently verified and approved for publication as a Paulioskos credential.

An individual qualification belongs to the named holder and must not be presented as organisational certification, supplier partnership or employer endorsement. Any future claim will be recorded in the Certification and Assurance Register before publication.

5. Data-protection registration position

The ICO data-protection fee self-assessment has been completed and the evidence is retained internally. The current pre-trading assessment is that a fee is not yet required. Paulioskos expects to repeat the assessment when trading begins or when processing activities materially change.

An ICO fee registration, if required in future, is a regulatory registration. It is not security certification and does not imply ICO approval or endorsement.

6. Assurance available to clients

Subject to legitimate need, stage of engagement, confidentiality and proportionate redaction, Paulioskos may provide:

- approved policy and governance summaries;
- sanitised architecture and data-flow descriptions relevant to the engagement;
- identity, access, administrative-control and secure-development summaries;
- backup-job summaries and sanitised restore or continuity evidence;
- vulnerability, patch, change and incident-management process summaries;

- supplier and subprocessor information relevant to client data;
- accessibility test summaries;
- reasonable due-diligence questionnaires;
- certification, registration or insurance evidence where actually held; and
- anonymised project examples, quantified outcomes and authorised references.

Credentials, private addresses, detailed firewall rules, exact recovery locations, exploit information, full risk registers, other clients' information and unredacted incident evidence may be withheld or redacted even under an NDA.

7. Claims we do not make

- ISO/IEC 27001, ISO 22301, Cyber Essentials or another certification that is not held;
- universal or guaranteed legal, UK GDPR or PECR compliance;
- ICO approval or endorsement;
- full WCAG 2.2 AA conformance before testing supports that conclusion;
- independent penetration testing where none has been completed;
- guaranteed security, zero vulnerabilities, uninterrupted availability or zero data loss;
- encrypted, immutable, air-gapped or geographically separate backups without verified evidence;
- staffed 24/7 support, continuous monitoring, a SOC or an SLA unless agreed in writing;
- formal vendor partnership or organisational ownership of an individual qualification; or
- insurance coverage that has not been evidenced.

8. Shared responsibility

Consulting outcomes depend on agreed scope, accurate client information, client decisions, third-party products, licensing, operational ownership and continued maintenance. Technology alone does not create compliance with a law, standard or contract. Each engagement should define responsibilities, assumptions, exclusions, acceptance criteria and required evidence.

Contact

Route	Details
Compliance and assurance	compliance@paulioskos.com
Privacy	privacy@paulioskos.com
Legal and contracts	legal@paulioskos.com

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 - UK GDPR guidance and resources](#)
- [NCSC - 10 Steps to Cyber Security](#)
- [NCSC - Cyber Essentials overview](#)
- [ISO/IEC 27001](#)
- [ISO 22301](#)
- [W3C - WCAG 2.2](#)

[← Back to the Trust Centre](#)