PUBLIC TRUST & ASSURANCE · PT-FIN-PRIV-001

Paulioskos Finance Privacy Notice

Explains how Paulioskos processes, protects, shares and retains personal information within the internal Paulioskos Finance platform, including HMRC Making Tax Digital data.

Version	Effective	Last reviewed	Owner
1.0	13 September 2026	13 September 2026	HR & Compliance Director

CURRENT IMPLEMENTATION POSITION

Paulioskos Finance is an internal Paulioskos business system. The v0.7.5 HMRC integration is read-only and uses HMRC sandbox/test services during development. It does not submit VAT returns and is not described as HMRC approved, accredited, certified or recognised.

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

This notice explains how Paulioskos Tech Consulting Ltd ("Paulioskos", "we", "us") processes personal information within **Paulioskos Finance**, our internally operated finance, accounting, evidence and tax-management platform.

Paulioskos Finance is currently an internal business system for Paulioskos. It is not offered as an accountancy, bookkeeping, tax-agent or software service to customers or other organisations.

This notice should be read alongside the Paulioskos Website Privacy Notice, Information Security Statement, Data Protection Complaints Policy and other controlled material published in the Paulioskos Trust Centre.

1. Who is responsible for the information

Paulioskos Tech Consulting Ltd is the controller for personal information processed through Paulioskos Finance where Paulioskos determines why and how that information is used.

Company	Paulioskos Tech Consulting Ltd
Company number	17354568
Registered in	England and Wales
Registered office	Unit A, 82 James Carter Road, Mildenhall, IP28 7DE

Privacy and compliance enquiries should use the current compliance contact route published in the Paulioskos Trust Centre.

2. What Paulioskos Finance is used for

Paulioskos Finance supports controlled internal financial administration, including:

- customer, supplier and business-contact records;
- quotations, invoices and associated commercial records;
- transaction, payment and reconciliation records;
- receipts, invoices and other supporting evidence;
- accounting and VAT records;
- audit, approval and operational evidence;
- secure integration with HM Revenue & Customs ("HMRC") where enabled; and
- business reporting, backup, recovery and compliance activities.

The platform is designed so that application code and release artefacts are separated from production data, credentials, secrets and environment-specific configuration.

3. Personal information we may process

Depending on the record or workflow, Paulioskos Finance may process:

Identity and contact information

- names;
- business names and trading names;
- business postal addresses;
- business email addresses and telephone numbers;
- job titles, roles and other business-contact information.

Financial and commercial information

- quotations and accepted commercial records;
- invoices, credit information and payment status;
- transaction descriptions and references;
- bank or payment references where required for reconciliation;
- VAT treatment, rates and amounts;
- supporting receipts, invoices and evidence; and
- correspondence or notes required to explain a financial record.

User and access information

For authorised Paulioskos users, the platform may process:

- name and business identity;
- corporate email address;
- application role and permissions;
- Microsoft Entra identity information;
- authentication and session metadata; and
- security and audit events.

Paulioskos Finance does not need to store a user’s Microsoft password.

HMRC and Making Tax Digital information

Where HMRC integration is enabled, the platform may process:

- Paulioskos VAT registration information;
- VAT obligation periods, period keys, due dates and status;
- VAT return values and submission evidence if a future approved submission capability is enabled;
- HMRC receipt, correlation or processing references;
- HMRC API request and response metadata required for safe audit and troubleshooting; and
- OAuth authorisation metadata and encrypted access/refresh tokens.

Paulioskos Finance does **not** store HMRC sign-in usernames or passwords. HMRC authentication is performed through HMRC’s own OAuth authorisation service.

Fraud-prevention and technical information

Where required by HMRC, the platform may derive and transmit fraud-prevention information such as browser/user-agent information, connection method, user identifiers, device identifiers, screen information, timezone, window size, public network information and vendor/application identifiers.

Only information required for the relevant HMRC fraud-prevention specification should be sent. Paulioskos does not intentionally invent unavailable header values.

Audit and security information

The platform may record:

- timestamps;
- actor/user identifiers;
- application actions;
- safe request/result metadata;
- change reasons;
- delivery and notification state; and
- error or correlation references.

Passwords, OAuth access tokens, refresh tokens, encryption keys and client secrets must not be written into normal application audit logs.

4. Why we use personal information

Paulioskos processes information in Paulioskos Finance for the following purposes:

- operating and administering the company;
- creating and maintaining accurate financial and accounting records;
- managing customer and supplier transactions;
- issuing, receiving and reconciling financial documents;
- complying with VAT, tax, accounting and statutory record-keeping obligations;
- communicating with HMRC through authorised digital services;
- maintaining evidence of financial decisions and transactions;
- detecting, investigating and preventing misuse, fraud or security incidents;
- managing access, audit, backup, resilience and disaster recovery;
- establishing, exercising or defending legal rights; and

- improving the reliability, security and maintainability of the platform.

5. Lawful bases

The lawful basis depends on the information and purpose. Paulioskos may rely on:

- **Legal obligation** - for tax, VAT, accounting, company and statutory record-keeping requirements.
- **Legitimate interests** - for proportionate internal financial administration, security, audit, resilience, fraud prevention and business operations.
- **Contract** - where processing is necessary to enter into or perform a contract with a customer, supplier or other business contact.
- **Legal claims and related statutory provisions** - where records need to be retained or used to establish, exercise or defend legal rights.

Consent is not normally the lawful basis for core accounting, VAT or statutory financial records.

6. HMRC Making Tax Digital

Paulioskos Finance is being developed to support HMRC Making Tax Digital for VAT for **Paulioskos's own VAT account**. Paulioskos is not presenting the platform as an agent or accountancy platform for third parties.

HMRC remains authoritative for HMRC-supplied obligation status, period keys and filing status.

At version 0.7.5, the HMRC integration is deliberately read-only: it can authorise securely and retrieve VAT obligation information, but it does not provide a VAT-return submission function. Any future write/submission capability must be separately developed, tested, approved and released before use.

When HMRC authorisation is used:

- the user is redirected to HMRC for sign-in and consent;
- HMRC returns an authorisation code to the registered callback;
- Paulioskos exchanges that code server-side;
- resulting OAuth tokens are encrypted before database storage;
- refresh-token rotation and expiry are controlled by the application; and
- removing local authorisation removes usable local token material without requiring HMRC credentials to be stored.

7. Who we may share information with

Information may be shared only where reasonably necessary with:

- **HM Revenue & Customs**, for authorised VAT/MTD functions and associated fraud-prevention requirements;
- **Microsoft**, where Microsoft Entra ID, Microsoft 365 or related business services provide identity, authentication or authorised communication functions;
- approved infrastructure, backup or security providers supporting Paulioskos systems;
- accountants, auditors, legal advisers or other professional advisers where required;
- banks or payment providers where an authorised financial workflow requires it; and
- regulators, courts, law-enforcement bodies or other authorities where disclosure is required or legally permitted.

Paulioskos does not sell personal information.

Access to Paulioskos Finance is restricted to authorised users and is not made available to advertisers.

8. Where information is processed

Current implementation position: the v0.7.5 HMRC integration is being validated in a segregated development/sandbox environment and does not use HMRC production access. When Finance is operated in production, its application and database are intended to run on Paulioskos-controlled infrastructure in the United Kingdom with controlled backup and recovery arrangements.

Some supporting service providers, including Microsoft and other infrastructure or security providers, may process information in other countries. Where UK personal information is transferred internationally, Paulioskos will use an applicable lawful transfer mechanism and proportionate supplier/security assessment.

Development and production environments are separated. Production credentials, live databases, evidence and HMRC secrets are not intended to be copied into the development environment through source-control deployment.

9. Security

Paulioskos applies proportionate technical and organisational controls to Paulioskos Finance, including:

- authenticated access and role-based permissions;
- Microsoft Entra identity controls where configured;
- multi-factor authentication through the relevant identity service where enabled;

- TLS for production network transport;
- encryption of stored HMRC OAuth token material using AES-256-GCM;
- separation of secrets and environment-specific configuration from Git/source control;
- controlled database migrations and release/version management;
- audit logging with secret/token redaction;
- controlled backup and recovery procedures;
- protection of production databases, uploads, evidence, certificates and encryption material;
- least-privilege administrative access; and
- security testing and dependency/configuration review as part of controlled releases.

No security measure can provide an absolute guarantee. Controls are reviewed as the platform, suppliers and regulatory requirements change.

10. Retention

Paulioskos keeps financial and tax records for the period required by applicable law and legitimate business need.

VAT records are normally retained for **at least six years**, consistent with HMRC VAT record-keeping requirements. A record may be retained longer where another legal requirement, unresolved dispute, investigation or legitimate evidential need applies.

Supporting financial evidence is retained in line with the record it supports where practical.

OAuth access and refresh tokens are retained only while required to maintain authorised HMRC connectivity, subject to expiry, rotation, revocation and local disconnection.

Security, audit and operational records are retained according to their purpose and internal retention rules. Paulioskos aims not to retain secret values in ordinary logs.

When data reaches the end of its required retention period, it is deleted, anonymised or securely disposed of where reasonably practicable and lawful.

11. Backups and disaster recovery

Backups may contain personal and financial information.

Paulioskos protects backup copies through access controls and recovery procedures appropriate to the underlying data. Production recovery planning covers, where applicable:

- the Finance database;
- uploaded financial evidence;
- environment-specific configuration;
- certificates and cryptographic material;
- HMRC token-encryption material; and
- application/configuration state required for reliable restoration.

Application source code is separately protected through controlled source management. Backup processes are designed so that recovery does not depend solely on source control.

Expired backup copies are removed in accordance with applicable backup-retention rules.

12. Data accuracy

Users of Paulioskos Finance are expected to record information accurately and correct material errors when identified.

Where HMRC provides VAT obligation status, Paulioskos Finance treats HMRC as authoritative for that status. The platform does not create a statutory filing obligation merely because a locally calculated calendar date has passed.

13. Automated decision-making

Paulioskos Finance may calculate status indicators, deadlines, warnings or workflow reminders from stored records.

These operational indicators do not constitute solely automated legal or similarly significant decisions about individuals.

HMRC-derived obligation status remains distinct from Finance presentation or urgency labels.

14. Your data-protection rights

Depending on the circumstances and applicable law, individuals may have rights to:

- request access to their personal information;
- ask for inaccurate information to be corrected;
- request erasure in applicable circumstances;
- request restriction of processing;

- object to certain processing based on legitimate interests;
- request portability where applicable; and
- complain about how their personal information is handled.

Some rights may be limited where Paulioskos must retain records to comply with tax, accounting, legal or evidential obligations.

Requests should use the current privacy/compliance contact route published in the Paulioskos Trust Centre.

Individuals also have the right to complain to the UK Information Commissioner's Office (ICO).

15. Security incidents and breaches

Suspected compromise of Finance data, credentials or HMRC connectivity is handled through Paulioskos security and incident procedures.

Where required, Paulioskos will:

- contain and investigate the incident;
- preserve relevant evidence;
- revoke or rotate affected credentials or tokens;
- assess risk to individuals and statutory obligations;
- notify HMRC, the ICO or other authorities where applicable; and
- document remediation and follow-up actions.

16. Changes to this notice

This notice is reviewed periodically and when there is a material change to:

- Paulioskos Finance functionality;
- HMRC integration or permissions;
- hosting or major suppliers;
- categories of information processed;
- retention requirements;
- security controls; or
- applicable legal/regulatory requirements.

A new controlled version will be published where changes are material.

Contact

Route	Details
Privacy and data-protection enquiries	privacy@paulioskos.com
Trust Centre	Open Trust Centre
Postal correspondence	Unit A, 82 James Carter Road, Mildenhall, IP28 7DE
UK regulator	Information Commissioner's Office (ICO)

Reference framework

These sources describe the legal, regulatory and good-practice framework used when preparing this document. They do not represent certification, accreditation, HMRC approval, regulatory endorsement or legal/tax advice.

Source	Link
HMRC Developer Hub - Terms of Use	Open source
HMRC - VAT (MTD) API 1.0	Open source
HMRC - Test Fraud Prevention Headers API 1.0	Open source
GOV.UK - Keeping VAT records	Open source
ICO - Personal data breaches: a guide	Open source
Paulioskos Trust Centre	Open source

PT-FIN-PRIV-001 · Version 1.0 · Public - Controlled