

Privacy Notice

T4 Tax Limited

Version: T4-DPN-05-2026-v3 | Last updated: May 2026

This Privacy Notice explains how T4 Tax Limited collects, uses, stores and shares personal data. It replaces our previous Data Privacy Policy dated May 2018.

We handle a large amount of personal, financial, tax and business information. We aim to keep that information confidential, secure and used only for appropriate purposes connected with our services, legal obligations and the management of our business.

Please read this notice and bring it to the attention of anyone whose personal data you provide to us, such as your spouse or partner, directors, shareholders, employees, contractors, beneficiaries, trustees, executors, family members or other connected individuals.

Controller details

Organisation	Details
Data controller	T4 Tax Limited
Company number	05134077
Registered office	24 St Marys Way, Burghfield Common, Berkshire RG7 3YR
Data Protection Point of Contact	John Cotter
Email	data.protection@t4tax.com
Telephone	0118 449 2404

Unless a service-specific agreement says otherwise, T4 Tax Limited acts as an independent data controller for personal data processed in connection with its professional tax, accounting and advisory services.

In limited cases, for example some outsourced or bureau-style work, we may act as a processor on your instructions. If that applies, the relevant service-specific agreement or data processing terms will explain this.

Who this Privacy Notice applies to

This notice applies to clients, prospective clients, former clients, business contacts, suppliers, professional contacts, website users and other people whose personal data we process in connection with our services and business activities.

Where our client is a business, company, trust, estate, partnership or other organisation, we may process personal data about directors, officers, shareholders, persons with significant control, beneficial owners, partners, trustees, executors, beneficiaries, employees, workers, contractors, customers, suppliers, family members and other connected individuals.

Personal data we collect and use

Category	Examples
Contact and identity data	Name, address, email address, telephone number, date of birth, signature, client reference, passport, driving licence, proof of address, identity verification results.
Tax and accounting data	Tax returns, UTR, National Insurance number, HMRC records, income, gains, reliefs, allowances, pensions, dividends, benefits, expenses, VAT, payroll, accounts, bookkeeping records and Companies House information.
Financial and transactional data	Bank statements, bank feeds, credit card records, invoices, receipts, payment details, loan information, asset details, investment information where relevant to tax/accounting work.
Business and entity data	Company or business details, ownership and control, directors, shareholders, PSCs, partners, trustees, executors, beneficiaries, management information and business records.
Family and personal circumstances	Marital or civil partnership status, spouse or partner details, dependants, household information, residence and domicile information, employment status, lifestyle or personal circumstances

	where relevant to tax or accounting work.
Communications data	Emails, letters, phone notes, video call notes, WhatsApp/text messages, portal messages, website form submissions, engagement confirmations, instructions, approvals and complaints.
Technical and website data	IP addresses, device and browser information, website logs, cookies or similar technologies, form metadata, submission dates/times and interaction data.
Special category data	Health or medical information, disability information, religious or similar information, biometric or other sensitive data if it appears in documents or is relevant to a service, tax relief, payroll matter, legal obligation or claim.
Criminal offence or sanctions data	Information relating to criminal offences, allegations, sanctions, politically exposed person checks, fraud prevention or anti-money laundering checks where relevant and lawful.

Where we get personal data from

- you directly, including through meetings, calls, emails, website forms, checklists, engagement agreements, secure portals, WhatsApp/text messages and document uploads;
- HMRC, Companies House, the Government Gateway and other public bodies;
- banks, bookkeeping software, payroll software, cloud accounting platforms, pension providers and other financial or software providers;
- previous or new accountants, tax advisers, solicitors, financial advisers, banks, lenders, insurers or other professional advisers;
- directors, employees, family members, trustees, executors, beneficiaries, shareholders, partners or other people connected with you or your business;
- publicly available sources such as Companies House, the Land Registry, the electoral register, sanctions lists, insolvency registers and publicly available internet sources; and
- our own systems, including website logs, form submissions, CRM/client records, email systems, workflow tools and file notes.

Why we use personal data and our lawful bases

We only use personal data where we have a lawful basis to do so. The lawful basis may vary depending on the purpose. The main purposes and lawful bases are set out below.

Purpose	What this covers	Likely lawful basis
Providing professional services	To provide tax, accounting, bookkeeping, payroll, VAT, company secretarial, advisory and related services; to prepare returns, accounts, reports and filings; to communicate with you and act on your instructions.	Contract; legitimate interests; legal obligation.
Legal, tax and regulatory compliance	To comply with tax law, accounting rules, anti-money laundering obligations, professional standards, regulatory requirements, court orders, HMRC enquiries and Companies House requirements.	Legal obligation; legitimate interests.
Client identification and AML checks	To verify identity, address, ownership/control, sanctions, politically exposed person status, source of funds/wealth and money laundering or terrorist financing risk.	Legal obligation; legitimate interests; substantial public interest where relevant.
Client administration and communications	To manage engagements, send service updates, request information, chase records, provide timetable updates, update engagement agreements, manage deadlines and maintain client records.	Contract; legitimate interests; legal obligation.
Website forms and online systems	To receive engagement agreements, checklists, client information forms, uploads and requests; to update client records and client communication systems such as	Contract; legitimate interests; legal obligation.

	Mailchimp or similar providers.	
AI, automation and technology tools	To assist with internal planning, document review, summarising, data extraction, spreadsheet or bank-record analysis, drafting, checking, workflow management, quality control and process improvement.	Contract; legitimate interests; legal obligation where connected with compliance work.
Quality control and professional compliance	To review files, manage quality, obtain insurance, deal with professional body reviews, respond to regulators and maintain standards.	Legitimate interests; legal obligation.
Security, fraud prevention and risk management	To protect our systems, prevent fraud, monitor security, recover debts, deal with disputes and protect legal rights.	Legitimate interests; legal obligation.
Marketing	We do not currently send general marketing newsletters. If we send marketing in future, we will do so only where lawful and with any required consent or opt-out rights.	Consent or legitimate interests where permitted; PECR compliance where applicable.

Where we rely on legitimate interests, we consider our interests and your rights and freedoms. You may object to processing based on legitimate interests in certain circumstances.

Special category and criminal offence data

Some information needs extra protection under data protection law. This includes special category data, such as health information, racial or ethnic origin, religious or philosophical beliefs, trade union membership, genetic or biometric data, sex life or sexual orientation. It also includes criminal offence data and related security measures.

We do not normally ask for this information unless it is relevant to the services we provide, required by law, included in documents you provide, needed for employment/payroll or tax purposes, relevant to a claim, relief or allowance, or needed for anti-money laundering, fraud prevention, sanctions or legal compliance purposes.

Where we process this type of data, we will only do so where we have a lawful basis under Article 6 UK GDPR and a relevant condition under Article 9 UK GDPR or the Data Protection Act 2018. Where required, we will maintain appropriate policy documentation and safeguards.

Client service communications, Mailchimp and similar platforms

We may use email platforms, client communication systems and similar providers, such as Mailchimp or equivalent systems, to send client service and administration communications to clients or groups of clients.

These communications may include requests to complete forms, updated engagement agreements, tax return process updates, timetable updates, deadline reminders, information requests, practice administration updates and other matters connected with services we provide.

These communications are not intended to be general marketing newsletters. If we decide to send general marketing communications in future, we will deal with this separately where required by law and provide appropriate consent or opt-out options.

When you complete forms, checklists, engagement agreements or information requests through our website or other online systems, the information you provide may be used to update our client records and administration systems. This may include email and client communication systems, such as Mailchimp or similar providers.

Artificial intelligence, automation and technology tools

We may use artificial intelligence, automation, machine learning, document analysis tools, software assistants and similar technology tools to help us provide our services and manage our business.

These tools may include systems provided by OpenAI, Microsoft Copilot and other AI or software providers. We may also use software supplied by third parties that includes AI-enabled features. Some AI features may be built into software we already use, and the design, operation or updating of those features may be controlled by the relevant software provider.

We may use these tools for internal planning, administration, workflow management, summarising or reviewing emails and documents, analysing spreadsheets, tax returns, bank records and bookkeeping records, extracting or organising information, drafting or improving wording, identifying possible inconsistencies or missing information, research, training, quality control and process improvement.

These tools may process personal data, tax information, accounting records, financial records, business information, correspondence and other confidential information. We will take reasonable steps to use AI and technology tools in a way that is consistent with our professional, legal, confidentiality and data protection obligations.

We remain responsible for exercising professional judgement. AI-generated output will not be treated as a substitute for professional review, and tax, accounting or advisory work provided to you will be subject to appropriate human review.

We do not use AI to make solely automated decisions about you that have legal or similarly significant effects. If this changes, we will update this notice and provide any information and safeguards required by data protection legislation.

Email, secure portals, WhatsApp, text messages and electronic communications

We may communicate with you by email, secure portal, electronic signature system, telephone, video call, post, text message, WhatsApp, WhatsApp group, website forms or other appropriate methods.

Electronic communication is not completely secure. Emails, text messages, WhatsApp messages and other electronic messages can be delayed, intercepted, misdirected, corrupted, accessed by others using your device, infected by viruses or fail to arrive.

We use email, messaging and other communication systems that provide security and administrative features. These may include encryption, access controls, audit trails, central administration and other risk-management tools. WhatsApp messages are generally end-to-end encrypted, but this does not remove all risks, including device access and group visibility risks.

Where we use WhatsApp groups, other group members may see your name, telephone number, profile details and messages sent within the group. Please tell us if you do not wish to communicate in this way.

You should use any secure portal or secure upload method we make available where practical, especially for identity documents, bank details, passwords, tax documents and confidential records.

Website, forms, cookies and similar technologies

Our website may use online forms, plugins and related tools, such as Formidable Forms or similar systems, to collect engagement agreements, checklists, client information, uploads and other information. Form submissions may be stored in our website systems, emailed to us, attached as PDFs, and used to update client records and communication systems.

Our website may use cookies and similar technologies. Some cookies may be necessary for the website to work. Others may help with security, analytics, form operation, preferences or other website functions. Where the law requires consent or a simple means of objecting, we will aim to provide this through our website or cookie tools.

Please see our Cookie Notice or website cookie settings for further information about the cookies and similar technologies used on our website.

Who we share personal data with

We may share personal data where necessary and lawful with:

- HMRC, Companies House, the Government Gateway, courts, tribunals, public bodies and other authorities;
- professional bodies, regulators, supervisory authorities, the Taxation Disciplinary Board, insurers and external reviewers;
- legal advisers, tax advisers, accountants, auditors, consultants, subcontractors and other professional advisers;
- previous or new advisers, where authorised or required for professional clearance, handover or continuity of service;
- banks, lenders, pension providers, investment platforms or other third parties where you have instructed or authorised us, or where necessary for our services;
- identity verification, anti-money laundering, sanctions, fraud prevention and risk-checking providers;
- cloud storage, email, website hosting, forms, secure portals, e-signature, payment, workflow, practice management, backup, security and software providers;
- client communication platforms such as Mailchimp or similar providers used for service and administration communications;
- AI and AI-enabled technology providers where used in accordance with this notice and our professional obligations;
- buyers, sellers or advisers in connection with a sale, merger, restructure or transfer of our business or assets; and
- law enforcement or fraud prevention agencies where required or permitted by law.

We do not sell your personal data to third parties.

International transfers

Some of our service providers may process personal data outside the UK, or make personal data accessible to support teams or systems outside the UK. Where this involves a restricted transfer under the UK GDPR, we will take steps to ensure the transfer is made lawfully.

These steps may include using UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, supplier contractual safeguards, or another transfer mechanism or exception permitted by data protection law.

How we protect personal data

We take reasonable and appropriate technical and organisational measures to protect personal data. These may include access controls, passwords, multi-factor authentication, encryption where appropriate, secure portals, staff controls, confidentiality obligations, backups, audit trails, anti-virus/security tools, supplier due diligence and internal policies.

No website, email system, messaging system, cloud service, AI tool or digital service can be guaranteed to be completely secure. If you believe information has been sent to the wrong person, submitted incorrectly, lost, compromised or accessed without authority, please tell us promptly.

How long we keep personal data

We keep personal data and client records for as long as we reasonably need them for the purposes for which they are held. This includes providing services, maintaining tax and accounting records, complying with legal, regulatory, professional and anti-money laundering obligations, dealing with HMRC enquiries, protecting our legal rights, managing insurance and professional indemnity matters, and dealing with complaints or disputes.

Retention periods may vary depending on the type of record, the services provided, the client's circumstances and any legal, regulatory or professional requirements. Many client records may commonly be retained for 6 to 10 years after the end of the relevant tax year, accounting period or client relationship.

Some records may be retained for longer where we consider this reasonably necessary. For example, HMRC may in some circumstances assess tax for periods of up to 20 years, and longer retention may also be appropriate where records relate to ongoing matters, long-term assets, tax claims or elections, HMRC enquiries, professional indemnity, legal claims, complaints, disputes, anti-money laundering obligations or other legitimate business reasons.

Record type	Retention approach
Client records and working papers	Retained for as long as we reasonably need them for tax, accounting, professional, insurance, dispute and business purposes. This may commonly be 6 to 10 years, and may be longer where reasonably necessary.
HMRC enquiry, long-term asset, claim and election records	May be retained for longer periods, including where relevant to potential HMRC enquiry windows of up to 20 years, ongoing matters, long-term assets, claims, elections, disputes or professional indemnity matters.
Anti-money laundering records	Generally retained for 5 years from the end of the business relationship or relevant transaction, unless a longer period is required or permitted.
Company, payroll, VAT and accounting records	Retained according to legal requirements and our professional/business needs, which vary depending on the service and circumstances.
Complaints, disputes and claims	Retained for the duration of the matter and for a reasonable period afterwards to protect legal rights and meet insurance/professional requirements.
Website forms, logs and communication records	Retained according to our operational, security, client record and legal requirements.
Backups and archives	May remain for a limited period until overwritten, deleted or destroyed according to normal backup and archive procedures. Individual records may not always be removable from consolidated backups.

We periodically review the records we hold and may delete, archive, anonymise or reduce records when we consider they are no longer reasonably needed. If you ask us to delete records, we will consider the request in accordance with data protection legislation, but we may need to retain some information where we are required or permitted to do so by law, regulation, professional obligations or legitimate business reasons.

Your data protection rights

Depending on the circumstances, you may have the right to:

- ask for access to your personal data;

- ask us to correct inaccurate or incomplete personal data;
- ask us to erase personal data in certain circumstances;
- ask us to restrict processing in certain circumstances;
- object to processing based on legitimate interests or direct marketing;
- ask for data portability where the right applies;
- withdraw consent where we rely on consent; and
- complain to us and to the Information Commissioner's Office.

These rights are not absolute. For example, we may need to keep or use information to comply with legal obligations, defend legal claims, meet professional obligations, maintain records or complete work you have asked us to do.

We will normally respond to rights requests within one month. We may extend this period where permitted by law, for example if a request is complex or we receive several requests.

Data protection complaints

If you have a concern about how we use personal data, please contact our Data Protection Point of Contact using the details above. We will acknowledge data protection complaints within 30 days and respond without undue delay.

You also have the right to complain to the Information Commissioner's Office. The ICO can be contacted at ico.org.uk or by writing to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Automated decision-making and profiling

We may use software, automation and AI-enabled tools to support our work, improve efficiency and identify matters requiring review. We do not use these tools to make solely automated decisions about individuals that have legal or similarly significant effects.

If this position changes, we will update this notice and provide any required information about the logic involved, the significance and expected consequences, and any safeguards available to you.

Changes to this Privacy Notice

We may update this Privacy Notice from time to time to reflect changes in our services, systems, suppliers, professional requirements, law or regulation. The latest version will be available from our website or on request.

This version is intended to align with our General Terms and Conditions - May 2026.