Tax Return Adviser Limited

DATA Privacy & Retention Policy

Last updated: 03/12/2018

Tax Return Adviser Limited (the firm) act as a Data Controller in respect of personal data for the purposes of the Data Protection Act 1988 and also the requirements of the EU General Data Protection Regulation (GDPR) which came into effect on 25th May 2018.
This policy sets out what systems and controls we have implemented to process client data in accordance with the requirements of the Information Commissioners Office (ICO) and also ensure that we mitigate the risks of data being lost / stolen. In addition to this the following outlines who has access to your personal data and what your rights are. We take your privacy seriously, please review it carefully.

This Policy covers the following key areas:

What is Personal Data?

1. Personal data is any information relating to a natural person or 'Data Subject' which identifies you personally whether directly (for example, your name) or indirectly (for example, information about your use of our products and services). Examples can be but not limited to; a name, date of birth, address, an ID number, a photo, an email address, bank details, NI number etc.

Why we collect personal data?

2. In order to carry out our role as both accountants and tax advisers, we need to store and act on (process) a large amount of personal data for the people we provide advice and bookkeeping services to, which would be held in paper and/or electronic format.

   With your consent we may collect the following data about you (but not limited to):

a. **Contact details:** your name, email address, and telephone number so that we can contact you in response to an enquiry you make in relation to the products and services that we have agreed to provide to you;
b. **Correspondence:** we may collect any additional personal data you may provide to us from time to time if you contact us by email, letter or telephone, or by any other means;

c. **Transaction details:** we or our third party providers will collect information relating to transactions you carry out through online services and for the purposes of fulfilling our terms of business.

Use of Data

3. Processing includes but not limited to obtaining, recording or holding information or data. Transferring it to other companies associated with us, our third party suppliers, the Chartered Institute of Taxation (CIOT) or any other statutory, governmental or regulatory body for legitimate purposes including, where relevant, to solicitors and/or H M Revenue & Customs.

   We may use your personal data for the following purposes:

a. To provide you with the products and services within our terms of business

We use your personal data to accept you as a new or returning client to provide you with the products and services you have requested in accordance with the Terms of Business.

b. To send you service communications, including in relation to changes to Terms of Business

We use the contact details you have provided to us so that we can communicate with you about the products and services that we provide, including to let you know about major changes to those products and services or to the Terms of Business between us or to any related information.

c. Direct marketing (including by third parties)

Tax Return Adviser Ltd distributes emails and newsletters via MailChimp, a third party supplier which stores data in the USA. We will seek your permission to add your name to our distribution list and will only transfer your name, email address and company name to MailChimp and store this data in order to send you emails and track interactions. We are satisfied that MailChimp comply with data protection regulation. You can update your preferences or unsubscribe from our direct marketing at any time by clicking the "Unsubscribe"/ “Update my preferences” link at the bottom of any of our emails or by contacting us.

d. To maintain our records and improve data accuracy

Like any business, we process personal data in the course of maintaining and administering our internal records. This includes processing your personal data to ensure that the information we hold about you is kept up to date and accurate.

e. To respond to enquiries, complaints and disputes

We use the personal data we hold about you to help us respond to any enquiries or complaints you have made, or deal with any dispute which may arise in the course of us providing our products and services to you, in the most effective manner.

f. To investigate, detect and prevent fraud and comply with our legal obligations

In certain circumstances, we use your personal data only to the extent required in order to enable us to comply with our legal obligations, including for fraud detection, investigation and prevention purposes. This may require us to provide your personal data to law enforcement agencies if they request it.

4. Legal grounds for processing

Data protection law requires us to only process your personal data if we satisfy one or more legal grounds. These are set out in data protection law of the Data Protection Act 1988 and also the requirements of the EU General Data Protection Regulation (GDPR) which came into effect on 25th May 2018. We rely on a number of different grounds for the processing we carry out. These are as follows:

5. Consent

In certain circumstances, we process your personal data after obtaining your consent to do so for the purposes of:

a. Necessary for the performance of a contract and to comply with our legal obligations

It is necessary for us to process your personal details, payment details and information about the business you represent for the performance of the Terms of Business between us. In particular, we rely on this legal ground to:

- provide you with products and services;
- communicate with you about products and services that we provide to you, including to let you know about major changes to those products and services or to the Terms of Business between us or to any related information;
- provide and improve client support;
- sending you marketing communications about our products and services;
- sharing your personal information with our trusted business partners;
- conducting marketing research;
- obtaining an identity/address check on you or your company for Anti Money Laundering purposes;
- obtaining your credit score so that we can establish the best possible payment terms we are able to offer to you.

If you choose not to give some or all of the aforementioned information to us, this may affect our ability to provide our products and services to you.

In certain circumstances, we also use your personal data only to the extent required in order to enable us to comply with our legal obligations, including to detect, investigate and prevent fraud.

b. Necessary for the purposes of our legitimate business interests or those of a third party

It is sometimes necessary to collect and use your personal data for the purposes of our legitimate interests as a business, which are to:

- provide you with products and services that are as useful and beneficial as possible, including by personalising our contact with you and making sure we tell you about all the services that are relevant to you;
- better understand our client base so that we can improve our products and services and marketing activities (which could also benefit you);
- comply with our contractual obligations to third parties;
- train our staff so that we can provide you with a better customer service;
- respond to any enquiries or complaints you have made, or deal with any dispute which may arise in the course of us providing our products and services to you; and

- ensure effective operational management and internal administration of our business, document retention, compliance with regulatory guidance and exercise or defence of legal claims.

Where we think there is a risk that one of your interests or fundamental rights and freedoms may be affected we will not process your personal data unless there is another legal ground for us to do so (either that we have obtained your consent to the processing or it is necessary for us to perform our contract with you or to comply with our legal obligations).

Who we share your personal data with

6. With your prior consent, we may provide your personal data to our suppliers and service providers, who provide certain business services for us and act as "processors" of your personal data on our behalf. We do not pass personal data onto any unrelated third party firms. In addition, we may disclose your personal data if we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to protect the rights, property, or safety, of our business, our clients or others. This includes, in specific cases, exchanging information with other organisations for the purposes of fraud protection.

7. In some cases, the personal data we collect from you may, for the purposes set out above, may be transferred outside the European Economic Area (EEA) and such destinations may not have laws which protect your personal data to the same extent as in the EEA. We are required by data protection law to ensure that where we or our "processors" transfer your personal data outside of the EEA, it is treated securely and is protected against unauthorised access, loss or destruction, unlawful processing and any processing which is inconsistent with the purposes set out in this Privacy Policy.

Retention and Disposal of Client Data

8. We retain your personal data for no longer than is necessary for the purposes(s) for which it was provided. What this means in practice will vary between different types of data. When determining the relevant retention periods, we take into account factors including:

- legal obligation(s) under applicable law to retain data for a certain period of time;
- statute of limitations under applicable law;
- potential or actual disputes;
- guidelines issued by relevant data protection authorities.

We will keep personal data for longer than the 7 years stated if we have justification for doing so; this could be but not limited to a situation where we have given advice that could be subject to investigation from HMRC or another authoritive body. HMRC can investigate over 20 years later and therefore all information needed to assist with this is required to be retained. However, after the initial 7 year period we will archive the data with an encrypted password which is only accessible to Simone Freedman.

Otherwise, we securely erase your personal data from our systems when it is no longer needed.

- In respect of retaining client data, Principle 5 set out by the Information Commissioner's Office of the Data Protection Act 1988 states that personal data shouldn't be kept for longer than necessary. With the introduction of the GDPR, this also introduces the right for someone to ask for their data to be deleted – the right to be forgotten. Some client data might be kept

for a few weeks in paper format whilst it is being used, for example in the preparation of a tax return. However, this information will be returned to the client once the necessary processing of the data has been completed. The calculations, and in some cases corroborating bank statements or breakdowns will then be held on file. These, must be retained for 7 years for tax purposes.

- If we obtain personal data, and they no longer require our services we will archive the data for a minimum of 7 years for our own taxation purposes. This data will only be available to be accessed by the data controller via an encrypted password.
- In respect of any paper correspondence received, Tax Return Adviser Limited has clear procedures for the disposal of customer data and all staff are aware that any documents that are sensitive must be shredded once they have been scanned and are no longer required and not placed in the normal waste bins within the office.
- All client data, once it has been scanned, is shredded and disposed of accordingly.

Data Subject Requests

9.

a. All individuals who are the subject of data held by Tax Return Adviser Limited are entitled to ask what information we hold about them and why, how to gain access to it, and to ask how Tax Return Adviser Limited meets its data protection obligations. If someone requests a copy of the data we store on them, this is called a "subject access request".
c. Any request should be referred to the Compliance Officer who will verify the identity of anyone making such a request before releasing any data, which will usually be provided within 14 days, but within the maximum 30 days allowed.
d. No charge is made for any release of data.
e. The Data Protection Act also allows personal data to be disclosed to law enforcement agencies without the consent of the data subject, and similarly the regulator, the Chartered Institute of Taxation (CIOT) would also be able to see any client data on request.

Your rights

10. You have the following rights regarding your personal data:

Your Rights	What does this mean?
a. Rights to be informed	You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data and your rights. This is why we are providing you with the information in this Privacy Policy.
b. Right of access	You have the right to obtain access to your personal data (if we are processing it) and certain other information (similar to that provided in this Privacy Policy). This is so you are aware and can check that we are using your personal data in accordance with the law.
c. Right to rectification	You are entitled to have your personal data corrected if it is inaccurate or incomplete.
d. Right to erasure	This is also known as 'the right to be forgotten' and, in simple terms, enable you to request the deletion or removal of your personal data where there is no compelling reason for us to keep using it. This is not a general right to erasure; there are exceptions.
e. Right to restrict processing	You have the right to 'block' or supress further use of your personal data in certain circumstances. When processing is restricted, we can still store your personal data, but may not use it further in accordance with the law.
f. Right of data portability	You have the right to obtain and reuse your personal data in a structured, commonly used and machine-readable format in certain circumstances. In addition, where certain conditions apply and with consent, you have the right to have such information transferred directly to a third party.

Governance

11. A data security breach can happen for a number of reasons:-

- Loss or theft of data and/or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences - information is obtained by deceiving the organisation which holds it.
- We act on an email request which later transpires to be fraudulent

12. Our Security procedures are:

- Tax Return Adviser Limited acknowledges that data security is a key specific risk to the firm.
- The Compliance Officer has overall responsible for the data security within the firm.
- Each member of staff is made fully aware that they are equally responsible for the data security within the firm.
- The firm has an open and honest culture to encourage staff to report any data security concerns.
- If data loss occurs, we will contact our clients within 48 hours (either via email or phone) and provide free guidance as to what actions they should take. The ICO will also be notified.

Systems and Controls

13. The firm has identified that the two main ways of data being accessed incorrectly are either due to a third party using passwords to access the client data, or due to a security breach meaning data is provided to a third party posing as a client.

a. The majority of client data is stored on computer systems with only current work in progress held in paper format. The main administrative back office system and client records (which are scanned) are not held on the firm's premises but are held on separate servers hosted by a third party, as a cloud service. Full due diligence has been carried on the cloud service provider in respect of their data security procedures meaning only Tax Return Adviser Limited employees have specific access to the data.
b. To access the cloud service, employees are allocated a unique login specific to each employee, each login requires a password, including at least 1 number, 1 capital letter. To then access the administrative back office system actually hosted on the cloud service, a different password is required. Passwords have to be changed periodically.
c. No client data is permanently stored on employees' computers.
d. The identity of a client is always confirmed / checked by staff before providing any personal data over the telephone. In addition, due to the fact that the majority of our business is transacted with regular clients, close relationships have been built up with them, meaning we are in regular contact with them by post, phone and in person, and so are generally aware of their particular circumstances. If circumstances change or a clients' employee leaves it is the responsibility of the client to inform us immediately by phone and then followed in writing to ensure no security is breached.
e. Anti-virus protection is installed on the cloud service as well as all PC's held onsite, which provides daily protection against viruses, which are updated regularly. All laptops used for business use have been encrypted and require strong passwords to be booted up.
f. Once any computer equipment reaches the end of their useful life, any hard disk(s) are removed and physically destroyed by the Compliance Officer including smashing the drive platters to ensure the data can't be accessed.
g. Individual printers used in the office do not have hard drives and therefore no data is stored on them.

14. Physical Security

a. Although the vast majority of client data is held electronically, some is held in paper format whilst it is being processed. The firm has implemented a "clear desk" policy, meaning that at the end of each day, all staff desks are cleared of any work in progress, and the records are locked in the desk.
b. The main office location is in a home environment and therefore is rarely unoccupied at any given time.
c. A security system, including an alarm is installed at the property. All external doors and windows are lockable and remained locked when premises are not occupied.
d. All visitors are supervised throughout their visit.

15. Compliance and Monitoring

a. We carry out a risk assessment of our data security arrangements annually.
b. The risk assessments are carried out by the Compliance Officer
c. Any issues identified by a risk assessment are reviewed by the Compliance Officer and any actions required are addressed within 2 months from the date the assessments are conducted.
d. In the event of any form of data loss to an unauthorised party, in all instances, staff are required to notify the Compliance Officer immediately who will then carry out the appropriate actions. This will consist of identifying what happened, the severity of the event, how to prevent a re-

occurrence, additional staff training, and contacting the Information Commissioner's Office within 72 hours of any breach being detected, as well as if appropriate, contacting the police.

Training and Staff Awareness

16.

a. Data security training is given to all new recruits by the Compliance Officer.
b. Until data security training is delivered and understood, members of staff are not allowed unsupervised access to client data.
c. Regular and on-going data security training is delivered to all existing staff to maintain their awareness.

Staff Recruitment and Vetting

17.

a. All new recruits, including any temporary staff (if they were to be used) are appropriately vetted prior to being allowed unsupervised access to any client data. The vetting process includes obtaining references from the previous employer for at least the previous 5 years and a credit check. As we are supervised by CIOT for AML our beneficial owner has criminality enhanced checks which are carried out through the Disclosure and Barring Services (DBS).
b. When staff leave, passwords and any electronic access including digital certificates are cancelled at the end of their last day of employment.

Third Party Suppliers

- Chartered Institute of Taxation (CIOT)
- Companies House
- Dropbox
- HIBU Uk (Yell)
- HMRC
- Hosted Desktop
- Indicator
- Iris
- Kashflow
- Mailchimp
- MoneySoft
- Quickbooks
- Ring Central
- Sage
- Saracen Storage
- Tax Filer
- VT Software
- Xero
- insurance companies
- The firm also employs a cleaner who has had sufficient AML checks.

How to contact us

If you would like to exercise your data protection rights or if you are unhappy with how we have handled your personal data, please feel free to contact us by:

- Writing to: Simone Freedman, Nower End, Nower Road, Dorking Surrey RH4 3BX
- Calling: 01306 743 791
- Emailing: simone@taxreturnadviser.com

If you're not satisfied with our response to any enquiries or complaints or believe our processing of your personal data does not comply with data protection law, you can make a complaint to the Information Commissioner's Office (ICO) by:

- writing to: Information Commissioner's Officer, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF;
- calling: 0303 123 1113; or
- submitting a message through the ICO's website at: ico.org.uk

Changes to this Privacy Policy

This Privacy Policy was last updated on 25th September 2018 and may be changed from time to time, please check our website for any changes

Appendix 1

Protecting clients and preventing fraud

Fraudsters are increasingly targeting financial advisers and their clients, to divert funds, by either accessing a client's email account by either guessing the login details or by previously getting the client to unknowingly add software to their PC giving the fraudster access to everything they type in including passwords.

Generally an email will then be sent out requesting a withdrawal of funds. This withdrawal request might be accompanied by new bank account details, along with 'proof of account documents', like bank statements. There may be an excuse as to why the client hasn't rung you, such as them being abroad, or being in hospital and unable to talk. The email might show previous emails, to make you think it's a genuine email. Initial email exchanges may simply request current plan values and other information, in order to build up information.

Other warning signs are:
• Does the email seem uncharacteristically blunt or contain terms or expressions which the client would not normally use?
• Is there a lot of bad grammar, unusual language or poor spelling? Does the tone of the email seem different from normal?
• Are there any mistakes or inconsistencies in terms of the information given?
• Is the email asking for something to be done urgently? Does it set any unrealistic timescales?
• If you try to verify any requests made in the email, do you get a satisfactory answer? Bear in mind that if a customer states they haven't received a particular email or emails, it is possible that fraudsters have intercepted the email and created a new folder for all subsequent emails, making them invisible to the client.
• Is there a time difference which suggests the email was sent from abroad?
• Is the email requesting you to do something which is outside your customer's usual pattern of behaviour, such as making a withdrawal?
• Have they requested a withdrawal that exceeds the current value of funds held?
• Does the email request that you forward on a pre-populated withdrawal form?
• Have they provided new bank details for funds to be sent to? Is this bank anywhere near where the client actually lives?
• Are they suddenly willing to pay a fee, such as a CHAPS payment fee, in order for you to send the funds quickly?

Anything we receive by email could be from a spoofed email address, so not from the client, and any attachments could be fake, as it's very easy to create a genuine looking bank statement, if we're only seeing a copy, not the original.

If you receive any email which asks for a withdrawal, which is unexpected, or not in the usual format, requests payment to a new bank account or raises any other suspicions as covered above, then the following procedure must be followed:

1) Notify the Compliance Officer immediately.
2) Contact the client/Tax Return Adviser Ltd by phone. Check to see if the request is genuine. If not, they will need to change their email password immediately and take steps to notify the police and financial organisations they do online business with. You should encourage clients to consider their online security including the antivirus and spyware software they use
3) Always ask for any original documents to be sent by post.

Similarly, in order to protect client data being sent out, as in theory emails can be intercepted, then personal data should not be provided in the body of any email, and any attachments, such

as those in a Word or pdf format which include a client specific personal data for example a statement or valuation, then the attachment must be encrypted using a password.

In view of the general age of many of our clients, we have to balance the need for client security with respecting their abilities to deal with complex security issues. Therefore a pragmatic approach has been taken to provide a password consisting of the client's first two initials of their first name, the first 2 initials of their surname and their year of birth. For example for Mr Johnathan Stanley Smith, born 1st April 1956, the password would be josm1956.

Word, Excel and Adobe PDF documents can be encrypted by doing File, Protect Document, and Encrypt with Password.