PRIVACY & DATA PROTECTION POLICY

Introduction

The purpose of this Policy is to document our data protection procedures in relation to the forthcoming GDPR. Our understanding of this legislation means that The Adviser Support Hub Limited (TASH) and our subsidiary company The Admin Pod Limited (TAP), are data processors on behalf of your clients personal data. This document aims to provide clarity on our role and the steps we take to protect personal data.

The General Data Protection Regulation (GDPR) comes into effect on 25 May 2018. It is a complex and wide-ranging piece of legislation but the key points are that the GDPR will give people greater control over how their personal data is used and provide them with the much-publicised 'right to be forgotten' (erasure).

Our management team are fully aware of the requirements of GDPR and have undertaken a full review of our systems and procedures to ensure that we comply with the requirements, and remain so beyond the effective date.

Up to the effective date we remain registered with the Information Commissioner's Office (ICO) under registration numbers **Z1930307** (TASH) and **ZA272611** (TAP) and comply with current regulations.

TASH and TAP are not regulated by the FCA. However, we directly support IFA firms who are, and rely on our service. The responsibility for any outsourced business activities and compliance with the FCA rules, remain with the IFA firms we support, as the regulated firm. This is why it is important that together, we are able to provide a data subject with reassurance, in terms of how we handle their personal data.

In order to carry out our work for you, we need to collect and use certain types of personal data about your clients. Under Article 4 of the EU GDPR definitions, 'personal data'', means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Under the Data Protection Legislation, all organisations which handle personal data must comply with a number of important principles regarding the privacy and disclosure of this information. We are committed to compliance with these principles.

We believe that the lawful and correct treatment of a data subject's personal data is critical to our successful operation, and to maintaining the confidence of our clients in us. We recognise that, to maintain our reputation and integrity as an open and professional organisation, we must be fully compliant with this legislation.

We believe GDPR is an opportunity for us all to build customer trust through effective management of their personal data.

We have discussed the implications of GDPR with our staff and we are committed to ongoing training on the matter.

GDPR is an ongoing project for us. We will regularly review our procedures and continuously look at ways of improving how we do things.

You can read more about GDPR here - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Data Protection Legislation

In the United Kingdom and the European Economic Area (EEA), "Data Protection Legislation" means all applicable data protection and privacy legislation or regulations including The Privacy and Electronic Communications (EC Directive) Regulations 2003 (also known as PECR) and any guidance or codes of practice issued by the European Data Protection Board or the Information Commissioner, together with:

- prior to 25 May 2018, the UK Data Protection Act 1998; and
- from 25 May 2018 onwards Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR"), as amended by the UK Data Protection Bill.

Outside of the EEA, "Data Protection Legislation" means local, territorial data protection and privacy legislation that governs the processing of Personal Data.

We fully endorse and adhere to the principles of data protection set out in the Data Protection Legislation and will:

- fully observe the conditions regarding the fair collection and use of personal data;
- meet our legal obligations to specify the purposes for which we use personal data;
- only collect and process the personal data needed to carry out our business or to comply with any legal requirements;
- ensure that the personal data we use is as accurate as possible;
- ensure that we don't hold personal data any longer than is necessary for legitimate business interests or as required by law;
- take appropriate technical and organisational security measures to safeguard personal data;
- ensure that personal data is not transferred outside the EU without suitable safeguards.

We are reviewing our systems, data processes and procedures to identify how we manage personal data – how we got it, who can access it, where it is stored and how long it should be kept. We will also be addressing key areas including breach reporting, subject access and data retention so that you can ensure your clients' personal data is safe with us.

Accountability and Governance

The GDPR applies to **'controllers' and 'processors'**:

- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.

Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees'* that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.

**This document and the information contained on our website, is aimed at helping you consider this. Please also refer to the section below headed 'About our role as a data processor. If you have any specific questions, please contact us using the details provided at the end of this document.*

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

We access and use data supplied by regulated IFA firms with their permission, during the period of a Contract for Service. **We have identified ourselves as a 'processor'.** Though we may act as co-intermediaries, **we believe that the regulated IFA firm appointed by the data subject to advise is classed as the 'data controller'**. The regulated IFA firm retains control of the personal data, subject to its own Client Agreement and Privacy Policy and retains control in terms of access rights granted to all third party processors (such as TASH and TAP). In most circumstances we have no direct data subject consent to process personal data so TASH and TAP rely mostly on a contractual right to process that data.

You can read about controllers and processors in more detail here - https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

With regard to an individual data subject, we encourage all our IFA firms to recognise the following data subject rights under GDPR:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

In addition, TASH and TAP will endeavour to ensure that:

- there is someone with specific responsibility for data protection in our organisation. Currently, the nominated Data Protection Officer (DPO) within TASH and TAP is Daniel Galbally; email dan@advisersupporthub.co.uk;
- we will regularly review and audit how we handle personal data;
- the ways we handle personal data are clearly understood;
- everyone handling personal data understands that they are responsible for following good practice;
- everyone handling personal data is appropriately trained and properly supervised;
- anybody wanting to make enquiries about handling personal data knows what to do; and
- queries about handling personal data are dealt with promptly and courteously.

As a data controller, the IFA firm has the right to request a copy of the data subjects' (your Client) personal data that we hold about them. We may charge a fee for this service, which will be dependent on the required level of data requested.

About our role as a data processor

When we use the data our IFA firms provide us with (with their permission), we have a duty of care in terms of how we handle that data. There are specific responsibilities under GDPR that provide sufficient guarantees that the requirement of the GDPR will be met and the rights of the data subjects protected.

As a data processor, TASH and TAP will:

- Only act on written instructions of the data controller (unless required by law to act without such instruction).
- Take appropriate measures to ensure the security of processing.
- Look to assist the data controller in providing subject access and allowing data subjects to exercise their rights under GDPR.
- Look to assist the data controller in meeting its GDPR obligations in relation to the security of processing, notification of personal data breaches and data protection impact assessments.
- Consider a request to delete or return all personal data to the data controller at the end or during the termination period of any contract, **unless retention of such data is required by law or for legitimate business interests**, in which case the data processor shall inform the data controller of such requirement(s).
- From time to time sub-contract work to a sub-processor (self-employed contactor). In the event that a sub-processor fails to meet its obligations under any sub-processing Agreement, the data processor (TASH) shall remain fully liable to the data controller for failing to meet its obligations.
- Not process or make any use of any personal data supplied to it by the data controller otherwise than in connection with the provision of the Services to the data controller.

- As a matter of good practice, ensure that our contracts state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR and in return we expect the same from the data controller.
- Strive for anonymity when producing data subject documentation as far as reasonably possible and sensible to do so.
- Ensure that documentation containing personal data is password protected when sent outside of our own organisation.
- Co-operate with supervisory authorities (such as the ICO) in accordance with Article 31.

Contracts

Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. Similarly, if a processor employs another processor (known as a sub-processor) it needs to have a written contract in place.

All of our existing IFA firms have in place a Client Agreement (a contract), which will remain in force. However, some IFA firms are asking TASH to sign separate a Data Protection Agreements (DPA). We believe this is good practice, and we encourage all IFA firms to provide us with a separate DPA – as the data controller, it is your responsibility to provide a DPA and it should cover the responsibilities of TASH and TAP as the data processor and the IFA firm as the data controller. Where you do not have a DPA, we can provide you with a draft DPA of our own.

Why are contracts between controllers and processors important?
Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

What needs to be included in the contract?
Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

How long will we keep Personal Data

We will not keep a data subjects personal data for any longer than is necessary in light of the reason(s) for which it was first collected. A data subject's personal data will therefore be kept for the following periods (or, where there is no fixed period, the following factors will be used to determine how long it is kept):

- Until when it is no longer in our **legitimate business interests** to keep it. We reserve the right to retain data for longer than this due to the possibility that it may be required to defend a future claim against us. Please note that in the event of a pension transfer, a regulated IFA firm is required to hold client records indefinitely and if we believe we are part

of this intermediary process, we may choose to also hold records indefinitely.

- We recognise that a data subject has the right to request deletion of their personal data and we will comply with this request, subject to the restrictions of our **legal or regulatory obligations** and legitimate business interests as noted above.

If you specifically request that we delete a data subject's personal data, then you waive the right to any future claim against TASH or TAP for errors and omissions.

How and where do we store or transfer Personal Data

We do not usually transfer any personal data outside of the EU except when we need to perform pre-contractual measures (credit and identity checks) or because the checks we request are necessary for important reasons of public interest.

Where we transfer personal data to a third party based in the US, this may be protected if they are part of the EU-US Privacy Shield. This requires that third party to provide data protection to standards similar levels of data protection to those in Europe. More information is available from the European Commission.

Specifically, we do use software companies such workflowmax (a Xero company) and Dropbox which are U.S. based companies. As part of our responsibilities we will ensure any company based outside of the EEA party to personal data is able to demonstrate compliance with EU privacy regulations. In the case of workflowmax the personal data we store is minimal, i.e. a data subject's name. In the case of Dropbox which we use to store all personal data, we confirm that they conform to the EU Privacy Shield: https://www.dropbox.com/help/security/data-transfers-europe-us

For more information regarding the Privacy Shield Framework please refer to: www.privacyshield.gov.

Security of Personal Data

The security of personal data is essential to us, and to protect personal data, we take a number of important measures, including the following:

- We will ensure that personal data is only accessible to authorised people in our firm (and appropriate sub-processors were required) and will remain confidential at all times.
- If we have a contract with another organisation or sub-processor to provide us with services or a service on our behalf to process personal data, we'll make sure they give reassurances regarding appropriate security measures in place and only process information in the way we've authorised them to. These organisations or sub-processors won't be entitled to use personal data for their own purposes. We also insist that a sub-processor is registered with the ICO in their own right.
- Appropriate security measures will be in place to prevent unauthorised access, alteration, disclosure, loss, damage or destruction of personal data.

- In all circumstances, we will take all steps reasonably necessary to ensure that personal data is treated securely and in accordance with this Privacy Policy.
- TASH and TAP emails are of SSL (Secure Sockets Layer) standard, which is a protocol that helps secure communications over computer networks, and is most often used with email. Our system encrypts at 256-bit key rate which is the standard level of Banking encryption. Our internal emails never leave our host email server (located in a 'bunkered' server in Manchester UK) and are therefore always encrypted at 256-bit key rate. When we send external emails, we cannot be held responsible for the level of security of the receiving server*. However, in order to protect personal data as best we can, as a minimum we will always password protect personal data using in the most part a 'zip' file.
- The PCs which are kept on our premises have two layers of security. Stage 1 is Windows 10 encryption and Stage 2 is Window's user profile password entry.
- All laptops used away from the office have the same two levels of security, but DESlock encryption is used in place of Windows encryption.
- Only management staff uses mobile devices (phones and iPad) for work activities. All devices require either a 6 digit pass-code or fingerprint recognition and automatically lock after 1 minute of inactivity. All devices are Apple products and Apple automatically build in encryption to their products, which you can read about here - https://www.apple.com/privacy/approach-to-privacy/
- Across all our devices (excluding mobile phones and iPad) we have installed ESET end-to-end protection which monitors all our PCs and laptops to ensure that our Firewalls & Anti-Virus software remain up to date. This is monitored by our IT partners www.ahead4.com.

*Please note however, regulated firms are responsible for providing a method for the secure transmission of a data subject's personal data to us, whether that is by email encryption, or through a secure communication portal.

How do we use a Data Subject's Personal Data

Under the GDPR, we must always have a lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, because you have consented to our use of personal data, or because it is in our legitimate business interests to use it. Personal data may be used for one of the following purposes:

- Providing and managing your account.
- Providing financial services and supporting advice.
- Undertaking research.
- Consulting and advisory services.
- Providing basic administration services.

Third Party Sharing

We may sometimes share personal data with other companies or contract with the following third parties to supply products and services to you. In some cases, these third parties may require access to some or all of a data subject's personal data that we hold.

We may share a data subject's personal data information with:

- Appropriate staff and sub-processors (self-employed contactors) such as those who carry out financial or compliance functions.
- Organisations that need your information because we are required to provide it by law (eg. The FCA, ombudsman services, HMRC etc).
- Organisations that carry out credit references or identity checks.
- Sometimes other companies or individuals, such as technical or research software providers or pension specialists, who assist us in providing our services. Examples of (but not limited to) these types of companies and their main purpose are:
    - O&M Pensions and Selectapension (Pension Research)
    - Morningstar UK and FE Analytics (Fund Research)
    - Synaptic Software (Product Reseearch)
    - Cash-flow planning tools
    - Product Providers, such as:
        - AJ Bell Investcentre
        - Aegon
        - Ascentric
        - Aviva
        - AXA
        - Canada Life
        - Fidelity FundsNetwork
        - James Hay
        - LV=
        - MetLife
        - Novia
        - Nucleus
        - Old Mutual Wealth
        - Prudential
        - Royal London
        - Russell Investment
        - Seven Investment management
        - Scottish Widows
        - Standard Life
        - Transact
        - Zurich
    - Discretionary Fund Managers, such as:
        - Brewin Dolphin
        - Brooks MacDonald

- Cazenove Capital Management
- Charles Stanley Asset Management
- Close Brothers Asset Management
- Investec DFM
- Quilter Cheviot
- Rathbone
- Standard Life Wealth
- Tilney

If any personal data is required by a third party, as described above, we will take steps to ensure as best we can that personal data is handled safely, securely, and in accordance with a data subject's rights, our obligations, and the third party's obligations under the law.

If we know that any personal data is transferred outside of the EEA, we will take suitable steps in order to ensure as best we can that personal data is treated just as safely and securely as it would be within the UK and under the GDPR.

In some limited circumstances, we may be legally required to share certain personal data, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

Third Party Due Diligence & Risk Management

Any third party that we engage with to support it with processing personal data has been contacted to confirm whether they conform to GDPR.

Privacy Policy

We provide services to regulated IFA firm's and as such we are not required to provide a Privacy Policy to the IFA firm's end client (the data subject), which remains the responsibility of the data controller (the IFA firm). This is because we have no authority to contact the data subject. However, in recognition of the fact that a data subject may request details of third parties and where the IFA firm requires it, we do have available on request a Privacy Notice to help the data subject understand our position as a third party.

Website Privacy Policy & Cookie Policy

We've provided a new Website Privacy Policy & Cookie Policy and this can be found on our website, within the Data Protection section www.advisersupporthub.co.uk/dataprotection

Employee Awareness

All our employees and sub-processors will be required to undertake annual training with respect to data protection requirements to demonstrate their understanding of data protection requirements.

Breach Management

In the event of a data breach, we have processes to manage, investigate, and mitigate the impact of data breaches.

Non-Disclosure

Confidentiality forms part of our Client Agreement and also our Contracts of Employment with our own staff and sub-processors. We will always consider signing your own non-disclosure agreement if you ask us to.

Your Responsibilities

- Consider how the GDPR interacts with your business and undertake a self-assessment to understand the action you need to have taken or be taking.
- You are responsible for providing a method for the secure transmission of a data subject's personal data to us, whether that is by email encryption, or through a secure portal.
- Update your websites, your Privacy Policy and other documentation such as considering how you will gather authority for processing sensitive data.
- You are responsible for ensuring that your own Privacy Policy and other appropriate client documentation permits the sharing of a data subject's personal data with third party processors such as us.

Changes to this Privacy Policy

We may change our Policy from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.

Any changes will be made available on our Website or you may request up to date information at any time, by contacting us.

Contact Details

To contact us about anything to do with personal data and data protection, including to make a subject access request, please use the following details (for the attention of Daniel Galbally):

- Email address: dan@advisersupporthub.co.uk
- Telephone number: 01245 200425
- Postal Address: 51 Trinity Row South Woodham Ferrers, Essex CM3 5DE
- Website: www.advisersupporthub.co.uk