GENERAL DATA PROTECTION REGULATION (GDPR) FREQUENTLY ASKED QUESTIONS

How does Aspira integrate Data Protection?

The protection of personal data is controlled by our Compliance Risk Plan. Our Security Policy and Business Continuity Plan covers information security, physical security and business continuity; it also includes data protection and records management. These policies and plans provide a clear structure for an effective internal control system to manage risks to the confidentiality, integrity and availability of information. The policy covers information held, processed and transmitted in electronic form. Further information on cyber security can be found later in this document.

Can you provide an overview of your governance structure for compliance with the Data Protection Act 1998, and provide details of how this will change post 25 May 2018?

We have a Data Protection Officer, supported by a Compliance team, who is responsible for ensuring Aspira can evidence compliance with its data protection obligations. The Data Protection Officer reports directly to the Managing Director and the Board.
Governance is reviewed at our regular Board meetings, and across the various reporting lines to ensure continued oversight of our data management practices and controls.

We will be reviewing our governance structure as we prepare for GDPR and we will continue to retain senior accountability and oversight of our business processes and operational compliance with our data privacy obligations to ensure the ongoing security and privacy of our clients' personal information.

What personal data or sensitive data does Aspira process or hold, and what categories of Data Subjects does this relate to?

Personal Data

We will need to collect personal data about you, when you first become a client and thereafter throughout the course of our relationship with you.

We will only ever collect and use information which is personal to you, your clients where it is necessary, fair and lawful to do so.

Special Categories (Sensitive Data under DPA 1998)

We may collect special categories of data (as defined by the GDPR) about you, including information relating to your physical or mental health. We will normally require your explicit consent for this.

What is the purpose of the processing of the personal data that Aspira does?

We will collect and use your information only where:

- you have given us your permission [consent] to send you information about products and services offered by Aspira and/or selected third parties we have chosen to work with which we believe may be of interest and benefit to you
- it's necessary to provide the product or service you have requested e.g. if you wish to invest in one a pension or savings product, we will require some personal information including your name, address, date of birth and bank account details
- it's necessary for us to meet our legal or regulatory obligations e.g. to send you Annual Statements, tell you about changes to Terms and Conditions, or for the detection and prevention of fraud
- it's in the legitimate interests of Aspira e.g. to deliver appropriate information and guidance so that you are aware of options that will help you get the best outcome from their product or investment; where we need to process your information to better understand you and your needs so we can send more relevant communications about the products and services we provide to you and to develop new products and services; where we use artificial intelligence or computer algorithms to improve products and services offered to you
- it's in the legitimate interests of a third party e.g. sharing information with product providers with whom you hold/will hold an plan

Processing of sensitive personal data (special categories of personal data) and personal data relating to criminal convictions and offences

GDPR maintains the requirement for explicit consent to process sensitive data (subject to some exemptions). GDPR prohibits the processing of personal data relating to criminal convictions unless there is local law to permit such processing.

Who can access sensitive personal data?

Security of all data is of paramount importance to us and we have robust controls in place to ensure this happens. Access to sensitive information is restricted only to those who have a lawful reason to process it.

When does Aspira obtain consent from clients in order to process personal data?

- Where consent is relied upon as the legal basis for processing, this will be captured, stored and used in line with GDPR standards. Individuals will be able to withdraw their consent at any time.
- Where the individual has given us consent to send them information about products or services offered by other companies in the LEBC group plc and/or third parties we have chosen to work with.

How will Aspira provide Privacy Notices to clients?

Organisations must provide privacy notices to the Data Subject so that the Data Subject is aware of how their information will be used, and to ensure transparency of processing.

When collecting personal information from you we will make a Privacy Notice available at that time e.g. when completing a factfind or client agreement.

Our Privacy Policy will be updated whenever we make a change, and if these are important changes such as where data is being processed, we will contact individuals to let them know. You can find a copy of the Privacy Policy online: https://www.aspirafp.co.uk/privacy-policy

Does Aspira have operating procedures, guidance notes and templates to complete to meet the Subject Access Requests requirements?

GDPR grants Data Subjects further rights to access their personal information. Organisations are required to provide this information, where feasible, in an electronic format where the request is made electronically. From 25 May 2018, firms will no longer be able to charge for the provision of a Subject Access Request and must respond within 1 month.

Aspira has established processes in place to respond to Data Subject Access Requests. We are reviewing and (where necessary) enhancing these processes to comply with the GDPR.

Does Aspira have a process for rectifying incorrect information?

Yes. Aspira has established processes in place to respond to requests to correct inaccurate or incomplete information on individuals. We are reviewing and (where necessary) enhancing these processes to comply with the GDPR.

Does Aspira have a process in place for handling any requests to erase data?

The right to erasure is also known as 'the right to be forgotten'. Data Subjects have the right to request the deletion or removal of personal data in certain circumstances. It is not an absolute 'right to be forgotten'.

Aspira has a process for Erasure/Right to be forgotten. We are reviewing and (where necessary) enhancing these processes to comply with the GDPR.

Aspira may not fulfil a request for erasure / right to be forgotten where we are bound by regulations or other laws to retain this personal data.

Does Aspira have a process for handling any requests for restriction of processing?

Yes, we have a process for handling requests to restrict processing of personal information. We are reviewing and (where appropriate) enhancing these processes to comply with the GDPR.

We will contact any third parties/recipients of your personal data to notify of any requests to rectify / erase / restrict processing.

Does Aspira complete any automated profiling or decision-making?

GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements.

Data Subjects have the right not to be subject to a decision based solely on automated processing where it produces a legal effect or significantly affects the Data Subject.

We use automated processing where it is in our legitimate interests, focused on understanding you better, helping us communicate with you, and to assist us in improving our products and services:

- Tailoring products and services e.g. placing you in groups with similar customers to make decisions about the products and services we may offer you to help meet your needs
- When designing and enhancing our online services to help meet your requirements for ongoing guidance and support

Has Aspira implemented a Data Protection Impact Assessment/Privacy Impact Assessment (DPIA/PIA) Process?

GDPR requires organisations to consider privacy risks and data protection obligations as part of the implementation of any organisational, technical or systematic change. Data Protection Impact Assessments (DPIAs) (also known as Privacy Impact Assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify risks and fix issues at an early stage.

Aspira already keep the potential impact of processing on an individual's privacy at the forefront. We are developing a DPIA process with standard templates in place for use across the business in our preparation for GDPR.

Does Aspira have a Data Protection Officer in place?

Aspira has a Data Protection Controller and Compliance Officer (vas@aspirafp.co.uk), who is accountable for data protection, security and liaison with the relevant regulators.

Where does Aspira store records and information?

GDPR requires organisations in certain circumstances (either when they have more than 250 employees or the processing could result in a high risk to the rights and freedoms of individuals, or processing involves sensitive data or data relating to criminal convictions and offences) to maintain a record of all their processing activities, with certain prescribed information to include who has access to personal data, what information this includes, and where that information is stored.

The majority of your information is processed in the UK and European Economic Area (EEA).

However, some of your information may be processed by the third parties we work with outside of the EEA, including countries such as the United States, Philippines and India.

Where your information is being processed outside of the EEA, we take additional steps to ensure that their information is protected to at least an equivalent level as would be applied by UK/EEA data privacy laws e.g. we will put in place legal agreements with our third party suppliers and do regular checks to ensure they meet these obligations.

For how long are records retained?

We will keep your personal information only where it is necessary to provide you with our products and services while you are a customer.

We may also keep your information after this period, but only where required to meet our legal or regulatory obligations. The length of time we keep your information for this purpose will vary depending on the obligations we need to meet.

What security measures do Aspira have in place? How does Aspira identify and mitigate cyber vulnerabilities?

The security of your information is always of paramount importance to us and we will always act in your best interests, making robust risk decisions that protect them. Like all financial services companies, we operate in a challenging, constantly evolving cyber-crime environment. We have a strong commitment to our security and IT capabilities, including long-term security programmes, and a dedicated internal IT function. These are designed to protect our customer and corporate assets/information from misuse, the effects of crime and the impact of a significant disruption to our operations.

As a key area of risk for Aspira, cyber security receives significant ongoing focus from our Board and senior management. This is reflected in ongoing investment we make to continually enhance our cyber-related resources and capabilities.

Aspira has invested in a cloud-based client management system to ensure our clients data is a secure as it possibly can. The provider of this software runs regular checks and has processes to fight against crime.

As well as the above investment, Aspira has a robust IT infrastructure setup to try and stop external security breaches. We regularly communicate with all staff to help them identify 'threatening' emails and documentation and what process to follow if they receive an email of this nature.

How is personal data protected within Aspira's Personal Finance Portal (PFP)?

The PFP is uses modern digital security systems just like those used by banks and other financial institutions to make sure your data is in an extremely secure environment. The PFP also offers a secure means of communication between you and Aspira via its messaging function and can be used to send, store and receive documents containing personal information.

If you would like more information about the security on the PFP please visit https://aspirafp.mypfp.co.uk/misc/security.

What is Aspira's internal process for breach reporting, and how does Aspira intend to comply with the GDPR?

GDPR will introduce a new requirement for organisations to report data breaches to the ICO within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the Data Subject. Organisations must also notify the Data Subject of the data breach if there is a high risk to the Data Subject. Processors must notify controllers without undue delay of any data breaches.

Any data protection breaches are managed locally in line with our agreed processes and regular reporting to the Data Protection Controller. If a material breach, this would be escalated immediately to the Board for awareness and actions agreed, as appropriate, including any notification to the regulator(s) and Data Subject where required.

Does Aspira transfer data outside the EU?

Transfers of personal data outside the EU can only be made in certain circumstances, usually by way of appropriate safeguards set out in the GDPR or based on a decision by the Commission. The majority of your information is processed in the UK and European Economic Area (EEA).

However, some of your information may be processed by the third parties we work with outside of the EEA, including countries such as the United States, Philippines and India.

Where your information is being processed outside of the EEA, we take additional steps to ensure that their information is protected to at least an equivalent level as would be applied by UK / EEA data privacy laws e.g. we will put in place legal agreements with our third party suppliers and do regular checks to ensure they meet these obligations.

Is data encrypted/anonymised when being transferred?

All data in transit is protected by TLS encryption which uses the strongest cipher settings available for the source browser.

What training do Aspira staff receive on their data protection and information security obligations in respect of data handling and processing?

GDPR requires all organisations to implement a wide range of technical and organisational measures to demonstrate they have considered and integrated data protection. Privacy by Design requires organisations to embed the GDPR into their systems, process and controls and in the event of any changes.

Staff will be trained and aware of requirements of the GDPR, and how this impacts their work.

A Data Protection e-learning module is mandatory for all staff on an annual basis. All staff are informed of their obligations in their Terms of Employment.

Local education sessions are held and we issue regular communications to staff via our intranet to ensure staff are kept abreast of developments in security processes and potential external threats.

Useful information:

Data Controller - in this case Aspira, determines the purpose and means of processing personal data.

Data Processor - is responsible for processing personal data on behalf of a Controller e.g. a product provider, accountant or bank.

Data Subject - the individual whose personal data is being processed (collected, stored and used).

Information Commissioner's Office - if you'd like more detail you'll find lots of useful information on data protection and the GDPR on the ICO website at https://ico.org.uk.