Privacy Statement

At Fidelity we are committed to protecting your personal data. This statement explains how we do that. It sets out what we do with your personal data, how we protect it, and explains your pertinent privacy rights.

Who We Are

FIL Life Insurance Ltd (Fidelity) is part of the Fidelity International Group. You can find out more about us here www.fidelitypensions.co.uk. Fidelity Life Insurance Ltd operates in United Kingdom, Ireland and India. Fidelity can be contacted at the following address:

UK Data Protection Officer, Fidelity International, Beech Gate, Millfield Lane, Surrey, KT20 6RP

Email: **pensions.service@fil.com**

Telephone: **0800 3 68 68 68**

Your Personal Data

We collect and use your personal data to enable us to conduct our business with you and to comply with the law.

Why we collect it

The law requires us to tell you why we collect and use your personal data – this is known as the lawful basis for processing. The basis we rely upon will depend on the purposes for which we are processing your personal data and are detailed below.

1. ### Performing our Contract with You

When we do business with you, we do so under a contract. For us to meet our obligations to you under that contract we must process your personal data. We will only process your personal data in line with the terms of that contract. Once you become a member of a pension administered by Fidelity the relevant privacy policy conditions will be sent to you.

When you provide personal data to us, we will use that personal data so we can provide our services to you or send you information about our products and services where appropriate.

We will only process that data for the purposes for which it was collected or to meet our legal obligations.

2. ### Our Legitimate Interests

We process your information for the following reasons, which we define as our **legitimate interests**:

- To conduct our security operations such as using your IP address to help us to identify you when you log in to our systems
- To help us to run our business; this includes financial management, risk management, planning, corporate governance, audit and research
- To market to you if you are a business

3. ### Our Legal Obligations

In some circumstances, we have a **legal obligation** to process and share your personal data. As a financial services business, we must provide a wide range of data to regulators. Sometimes this involves personal data. We will never transfer more personal data than is necessary to discharge our legal obligations.

4. ### Your Consent

We will ask you for your preferences in terms of how you would like us to communicate with you and what information you would like to receive from us. You can always adjust your communications preferences, and can opt not to receive information from us unless we are obliged to provide it.

What we collect

The personal data you provide to us will include combinations of any of the following: Your name, email address, telephone number, address, identification numbers such as social security number, banking account details, date of birth, voice biometrics & voice recordings, location information, employment information, gender, IP address, language, and marital status.

Who we share your personal data with

Like most businesses, we use third parties to help us deliver our services. This will often involve a third party processing your personal data but that will only be in line with the purposes set out above.

The third parties with whom we share your personal data will only be permitted to use that data in line with the instructions we provide them and we operate a regular and strict regime of third party checks on how your personal data is protected.

We will never share your personal data with third parties for a purpose not described in our Privacy Statement; but remember, in some cases, we are obligated to share your personal data with a third party in relation to matters such as countering identity theft and fraud as well as schemes such as the Unclaimed Assets Register.

We will share your personal data with fraud prevention and law enforcement agencies if false or inaccurate information is provided and fraud is identified. Fidelity Group companies and other organisations may also access and use this information to prevent fraud and money laundering, for example, when: checking details on applications for credit and credit related or other facilities; managing credit and credit related accounts or facilities; recovering debt; checking details on proposals and claims for all types of insurance; and checking details of job applicants and employees. If fraud is detected, you could be refused certain services, finance, or employment. Please contact us if you wish to receive details of the relevant fraud prevention agencies, further details can be found regarding data protection rights and fraud prevention agencies at **https://www.cifas.org.uk/fpn**.

Fidelity™ INTERNATIONAL

Transferring your personal data to other countries

As part of delivery our service to you it is necessary to transfer your personal data across national borders. These transfers may involve at least one of Fidelity's Group entities operating in the EEA and as such will apply the European standard of protections to the personal data we process. In practice, this means that all the entities in the Fidelity Group agree to process your personal data in line with high global standards. Where your personal data is transferred within the Fidelity Group but outside of the EEA, that data subsequently receives the same degree of protection as it would in the EEA.

Where it is necessary to transfer personal data to a third party, stringent reviews of those with whom we share the data are carried out and that data will only be transferred in line with the purpose for which it was collected. The third parties to whom we transfer your data are located in the following countries: UK, Ireland and India.

Security of Your Personal Data

Ensuring the confidentiality, integrity and availability of your personal data defines our approach to information security. We manage the security risks to your personal data in a way that makes sure we meet our legal and regulatory obligations. In order to protect the continuity of the business we do with you, we produce, maintain and regularly test our business continuity plans. We utilise the internationally recognised information security best practices, ISO27001 and PCI-DSS. Our Information Security Policy & Standards are regularly reviewed, adhered to and tested for compliance. Information Security training is mandatory for all staff and breaches of information security, actual or suspected, are reported and investigated.

Your Rights

European law places robust obligations on businesses in the protection of personal data. Globally, the way we protect your personal data reflects our European obligations. A number of rights in relation to the use of your personal information empowers you to make certain requests of us, detailed as follows:

1. Requesting a copy of your personal data

You can access the personal data we hold about you by emailing or writing to us using the contact details at the end of this Statement.

2. Letting us know if your personal data is incorrect

If you think any of the personal data we hold about you is wrong please let us know by contacting your local client services team. We will check the accuracy of the information and take steps to correct it if necessary.

3. Asking us to stop using or to erase your personal data

You have the right to object to our use of your personal data. You can ask us to delete it, to restrict its use, or to object to our use of your personal data for certain purposes such as marketing. If you would like us to stop using your data in any way, please get in touch. Of course, if we are still providing services to you we will need to continue using your information to deliver those services. As detailed above, in some circumstances we are obligated to keep processing your information for a set period of time.

How long do we keep your personal data?

We will keep your personal data safe as a client of Fidelity and will hold it for as long as necessary. To meet the requirements of both UK tax and pensions law, we must keep certain personal information for a minimum of 6 years. However, given the nature of pension schemes, for us to meet our legal obligations we need to keep some of your personal information for the rest of your life even if you have closed your account with Fidelity.

How to complain

If you are unhappy with how we have used your personal data you can complain to us by contacting us at:

UK Data Protection Officer, Fidelity International, Beech Gate, Millfield Lane, Surrey, KT20 6RP

Finally, you also have the right to complain to your national data protection authority: Information Commissioner's Office whose helpline number is: **0303 123 1113**.

UKM0719/24433(WI)/QC/0520

WI-GEN-36