Privacy Statement

July 2023

Why we collect your data

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. We collect and use your personal data to enable us to conduct our business with you and to comply with the law. The basis we rely upon for lawfully collecting and using your personal data will depend on the purposes for which we are processing your personal data. These are detailed below:

(a) Performing our contract with you

When we do business with you, we do so under the Client Terms. For us to meet our obligations to you under the Client Terms we must process your personal data. We will only process your personal data in line with the Client Terms. When you provide personal data to us, we will use that personal data so we can:

- provide our services to you in the provision, administration and servicing of your account
- enable the conduct of security operations, such as using your IP address to help identify you when you log on to your account online
- identifying you when you contact us
- 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.

(b) Our legitimate interests

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

- developing new services and products
- internal research and analysis
- to help us to run our business; this includes financial management, risk management, planning, corporate governance, audit and research

(c) Our legal obligations

In some circumstances, we have a legal obligation to process and share your personal data. We must provide a wide range of data to regulators or other entities in order to prevent or detect crime. Sometimes this involves personal data. We will never transfer more personal data than is necessary to discharge our legal obligations.

(d) 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 and how

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 National Insurance number, banking account details, date of birth, voice biometrics & voice recordings, location information, employment information, gender, IP address, language, and marital status, dependants and beneficiaries and shareholders.

This information is typically provided to us by your adviser if you have one or by you through the course of your relationship with us. We hold your personal information relating to your account on paper and on computer systems.

Fidelity may also need to hold and process sensitive information about you and/or your dependants and beneficiaries (known as "special category data"). Under legislation, details relating to health, racial or ethnic origin, religious or other similar beliefs, sexual orientation political affiliations and biometric data are regarded as "special category data". Except where the legislation allows it, this information cannot be processed or passed to a third party without your explicit consent. If we need your consent to process or pass your special category data to a third party, we will ask you to provide it at the relevant time.

Where you tell us about any additional needs you have (for example relating to an illness or challenges you're facing in life), we will record this information to provide you with appropriate additional support. Where this includes your special category data, we will ask for your consent to do so. We will hold this information for as long as you need extra support from us, or until you or your adviser asks us to remove it (whichever is shorter).

Who we share your personal data with

Like most businesses, we use third parties, including other entities in the Fidelity Group, to help 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. We operate a regular and strict regime of third party checks on how your personal data is protected.

Your personal data will be held in confidence by us but may be passed to other companies as detailed below:

- Fidelity Group companies, their agents or any third parties we appoint for the administration and servicing of your account, which may include the transfer of your information outside the UK and European Economic Area (EEA). Where we send the data of your dependants, beneficiaries or shareholders to such third parties you agree to inform and gain consent from the relevant persons.
- We, or other Fidelity Group companies, are provided with updated address details or other information by either you or your employer, in which case we will update the information kept for any other accounts for which we hold records on our database.
- If applicable to you, your adviser or intermediary - this would include any other party to the business relationship with your adviser or intermediary that you have told us about;
- HM Revenue & Customs, the Financial Conduct Authority and other statutory bodies (such as the Financial Ombudsman) – we can be fined and subject to other action if we fail to provide certain information to these authorities.

Fidelity INTERNATIONAL

- The Unclaimed Assets Register to help you with the recovery (for example) of unclaimed distribution payments.
- Companies who facilitate payments to you, for example tracing agents, and to allow regulatory money laundering checks to be made and BACS and Western Union payments to be made.
- Other organisations to take action if we consider your levels of trading to be short-term, excessive or disruptive.
- Other organisations to help prevent and detect fraudulent behaviour and to authenticate customers using our online services.
- 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**.

  We and other organisations may access and use from other countries the information recorded by fraud prevention agencies.
- Our affiliated and associated companies for marketing purposes where you have provided your specific consent.
- Other Fidelity Group companies in order to provide improved servicing of the accounts you hold with Fidelity Group, including reporting to you. This is at your request only.

Any transfer of information will usually be by electronic means, including the internet.

Transferring your personal data to other countries

As part of delivery of 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 UK and 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 UK and EEA, that data subsequently receives the same degree of protection as it would in the UK and 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, The Netherlands, Germany, Ireland, USA and India.

In some circumstances we transfer your personal data to companies for whom it is necessary to provide their services from a multitude of countries across the globe. The details of these transfers may be found on the websites of those companies, they are:

1. Barclaycard - As our payment provider, we transfer your personal data to Barclaycard so that you may complete your transactions. The Barclaycard Privacy Statement can be found at **www.barclaycard.co.uk/personal/privacy-policy**;
2. Experian Limited - To comply with our Anti-Money Laundering obligations we may transfer your personal data to Experian Limited as part of the background checks we are obligated to conduct. The Experian Privacy Statement may be found at **www.experian.co.uk/legal/privacy-statement.html**; and
3. GB Group - To comply with our Anti-Money Laundering obligations we may transfer your personal data to GB Group as part of the background checks we are obligated to conduct. The GB Group Privacy Statement may be found at **https://www.gbgplc.com/privacy-policy/**.

Security of your personal data

Ensuring the confidentiality, integrity and availability of your personal data defines our approach to information security. We ensure that the security risks to your personal data are managed in a way that makes sure we meet our legal and regulatory obligations. 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

The law places robust obligations on entities in the protection of personal data. The way we protect your personal data reflects our legal 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:

(a) Requesting a copy of your personal data

You can access the personal data we hold about you and exercise your right to have a copy provided to you, or someone else on your behalf, in a digital format by emailing or writing to us using the contact details set out in the Client Terms.

(b) 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 us. We will check the accuracy of the information and take steps to correct it if necessary.

(c) 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. If we are still providing services to you we will need to continue using your information to deliver those services. In some circumstances we are obligated to keep processing your information for a set period of time.

Information will generally be provided to you free of charge, although we can charge a reasonable fee in certain circumstances.

How long do we keep your personal data?

We keep all personal data safe and only hold it for as long as necessary. To meet the requirements of UK tax law, we must keep your personal information for a minimum of 7 years.

How to complain

If you are unhappy with how we have used your personal data you can complain by contacting us, Fidelity International, Beech Gate, Millfield Lane, Tadworth, 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.**

UKM0723/65499-11/QC/0724

FNW-GEN-36 [WF 1284983]