

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

The personal data will be processed by FIL Investment Management (Luxembourg) S. A., a société anonyme having its registered office at 2a, rue Albert Borschette, L-1246 Luxembourg.

(hereinafter referred to as “FIMLUX” or the “Manager”).

You may contact the Manager at the following address:

Data Protection Office
FIL Investment Management (Luxembourg) S.A.
2a, rue Albert Borschette, B.P. 217,
L-1246 Luxembourg

In addition, other entities involved in the management of your investment may process personal data in their capacity as data controllers (for instance the fund, the management company, the depository bank etc.). These processing activities are done under the sole responsibility of these independent data controllers and are governed by separate privacy notices.

The Manager is the management company of the following common contractual funds (the “CCFs”):

- Fidelity Common Contractual Fund
- Fidelity Common Contractual Fund II

The Manager has also been appointed as management company / AIFM to each of the following investment funds (each a “Fund”, and together with the Manager, “we” or “us”):

- Fidelity Institutional Liquidity Fund plc
- Fidelity Institutional Variable Capital Company Fund plc
- Fidelity Qualifying Investor Funds plc
- Fidelity UCITS ICAV
- Fidelity UCITS II ICAV

The Manager is the controller of your personal data in connection with investments in the CCFs, and a processor (for the relevant Fund, which is the controller) of your personal data in connection with investments in a Fund. You can find out more about the Manager, the CCFs and the Funds here:

<https://www.fidelityinternational.com>

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. This statement will apply to you if you are a natural person who is a registered unitholder/shareholder, an applicant for units/shares, a beneficial owner of a registered unitholder/shareholder or applicant for units/shares, or a personal representative, financial advisor, director, officer, employee, agent, trustee and / or authorised signatory of a registered unitholder/shareholder or applicant for units/shares in a CCF or Fund, or director, officer, employee, agent or authorised signatory of a service provider to the Manager, a CCF or a Fund.

It is your responsibility to ensure that any third parties whose personal data you provide to us are aware of their rights in this regard and are provided with a copy of this statement.

Where we need to process personal data in connection with a registered unitholder/shareholder's contract with a Fund, or the Manager in respect of a CCF, or in anticipation of an applicant for units/shares becoming a registered unitholder/shareholder, or where we have a legal obligation to collect certain personal data relating to an individual (for example, in order to comply with anti-money laundering obligations), we will not be able to deal with you (or the registered unitholder/shareholder or applicant for units/shares which you represent) if you do not provide the necessary personal data and other information we require.

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

The basis we rely upon will depend on the purposes for which we are processing your personal data. These 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.

When you provide personal data to us, we will use that personal data so we can provide our services to you and to administer the investment in a CCF or Fund by you (or the registered unitholder/shareholder you represent).

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
- For board reporting and management purposes
- To market to you if you are a business
- To send you information about our products and services where appropriate
- To take advice from external legal and other advisors
- In the event of a merger or proposed merger of a Fund or CCF, or any sub-fund of a Fund or CCF, or any other restructuring or reorganisation of a Fund or CCF, or any sub-fund of a Fund or CCF, or relating to the assets of a Fund or CCF or any sub-fund of a Fund or CCF
- In the event of a merger, reorganisation or disposal of, or a proposed merger, reorganisation or disposal of all or part of the business of the Manager or the Group
- Where use or sharing of your personal data is for a legitimate purpose of another company in the Group, or of a third party to which the Manager or a Fund provides the Personal Data

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. This includes for the purposes of anti-money laundering and anti-terrorist financing (collectively “AML”) and fraud prevention purposes, including OFAC and PEP screening for these purposes, and / or to comply with UN, EU and other applicable sanctions regimes, as well as compliance with applicable tax and regulatory reporting obligations. Sometimes this involves personal data. We will never transfer more personal data than is necessary to discharge our legal obligations.

4. Your consent

We may use your personal data for purposes to which you have consented. If you give consent for particular purposes, you have the right at any time to withdraw consent to the future use of your personal data for some or all of those purposes by writing to the address specified below.

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.

We may, in limited circumstances, collect and process “special purpose” personal data, such as data revealing racial or ethnic origin, political opinions, or trade union membership in connection with our obligations under applicable AML laws. Any personal data of this nature will only be used and disclosed, as necessary, for such purpose.

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 may share your personal data with third party controllers, such as the depositary to a Fund or CCF, where it needs the personal data in order to enable it to discharge its legal and regulatory obligations (including AML obligations), or in limited circumstances, where the administrator to a Fund or CCF is subject to a separate legal obligation requiring it to act as controller of the personal data, including where it is required to use the personal data for the discharge of its own AML obligations, or where you may have otherwise consented to your personal data being shared with the administrator for specific purposes. We shall also share your personal data as required with the Irish Revenue Commissioner, the Central Bank of Ireland, the Commission de Surveillance du Secteur Financier (CSSF), the Data Protection Commissioner, the National Commission for Data Protection in Luxembourg and our other relevant regulators.

We will disclose your personal data to the relevant Fund or CCF administrator for the purposes of carrying out the services of administrator and registrar of the Fund or CCF and to comply with legal obligations, including under company law and AML legislation or regulatory requirements.

Where your personal data is held in connection with Fidelity UCITS ICAV, Fidelity UCITS II ICAV, Fidelity Institutional Variable Capital Company Fund plc, Fidelity Qualifying Investor Funds plc, Fidelity Common Contractual Fund and/or Fidelity Common Contractual Fund II, your personal data will be disclosed to, and processed by, Brown Brothers Harriman Fund Administration Services (Ireland) Limited ("BBH Administrator"), which is the administrator of these funds. BBH Administrator may in turn disclose your personal data to agents or other third parties where necessary to carry out the administration services, including to: Brown Brothers Harriman & Co., Brown Brothers Harriman (Luxembourg) S.C.A., Brown Brothers Harriman (Poland) Sp. Z.o.o., Brown Brothers Harriman (Hong Kong) Limited and/or Infosys BPO Limited.

Where your personal data is held in connection with Fidelity Institutional Liquidity Fund plc and, your personal data will be disclosed to, and processed by, J.P. Morgan Administration Services (Ireland) Limited ("JPM Administrator"), which is the administrator of this fund. JPM Administrator may in turn disclose your personal data to agents or other third parties where necessary to carry out the administration services, including to other JP Morgan affiliated entities located in the European Union and outside of the EEA.

In certain circumstances, each of BBH Administrator and JPM Administrator may use your personal data for the purposes of complying with any law or regulation applicable to it, its sub-processors or affiliates or for complying with any request made by any financial services regulator or other public authority or government body having jurisdiction over BBH Administrator or JPM Administrator (as relevant), its sub-processors or affiliates, in which case it will be considered to be a data controller of such personal data.

In any case where we share personal data with a third party data controller (including, as appropriate, other members of the Group, or BBH Administrator or JPM Administrator in the circumstances described above), the use by that third party of the personal data will be subject to the third party's own privacy policies.

We will never share your personal data with third parties for a purpose not described in this 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.

Transferring your personal data to other countries

In today's global market, it is necessary for us to transfer your personal data across national borders. On the most part, these transfers will involve at least one of our 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 our Group agree to process your personal data in line with our high global standards. Where we transfer your personal data within our Group but outside of the EEA, that data subsequently receives the same degree of protection as it would in the EEA through the implementation of EU Commission approved standard contractual clauses.

Where it is necessary to transfer personal data to a third party, we operate stringent reviews of those with whom we share the data and we will only transfer that data in line with the purpose for which it was collected and where the transfer is permitted under European data protection rules and / or there is an appropriate safeguarding mechanism in place. The third parties who help us process your data are located in the following countries: Argentina, Australia, Austria, Belgium, Bermuda, Brazil, Canada, Chile, China, Croatia, Czech Republic, Denmark, Finland, France, Germany, Greece, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Kuwait, Liechtenstein, Luxembourg, Malaysia, Malta, Mauritius, Mexico, Monaco, The Netherlands, New Zealand, Norway, Pakistan, Philippines, Poland, Portugal, Saudi Arabia, Singapore, Slovakia, South Africa, Spain, Sweden, Switzerland, Taiwan, Thailand, United Arab Emirates, United States and the United Kingdom.

Details of the transfers of your personal data to other countries by BBH Administrator and JPM Administrator are set out above.

Please contact us if you wish to obtain more information concerning these safeguards.

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.

Updates to Personal Data

We will use reasonable efforts to keep your personal data up to date. However, you will need to notify us without delay in the event of any change in your personal circumstances, or those of the others mentioned above, so that we can keep the personal data up to date.

Your Rights

European law places robust obligations on businesses in the protection of personal data. Globally, the way the Group protects 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 in some circumstances. 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 below, in some circumstances we are obligated to keep processing your information for a set period of time.

4. Other Rights

In limited circumstances, you may also have the right to data portability in respect of certain of your Personal Data, which means you can request that the Manager and the Fund via the Manager provide it to you in a structured, commonly used and machine-readable format, or transmit it to your third party nominee where this is technically feasible.

If you are unhappy with how we have used your personal data, you can complain to us by contacting us at the contact details set out below.

Finally, you also have the right to complain to your national data protection authority or to National Commission for Data Protection in Luxembourg, which can be contacted at:

Commission nationale pour la protection des données
1, avenue du Rock'n'Roll
L - 4361 Esch-sur-Alzette
Tel.: (+352) 26 10 60-1
<https://cnpd.public.lu>

How long do we keep your personal data?

We will keep your personal data for as long as you are a client of the Manager or are an investor (or you represent an investor) in one of the Funds or CCFs. We will not retain your data for longer than is necessary for us to meet our legal obligations or to ensure our security and business continuity procedures are effective.

We are obliged by law to retain AML related identification and transaction records for six years from the end of the relevant investor relationship or the date of the relevant transaction. In general, we (or our service providers on our behalf) will hold your personal data for a period of seven years, unless we are obliged to hold it for a longer period under law or applicable regulations.

How to contact us

Any queries or complaints regarding our use of your Personal Data and / or the exercise of individual rights should be addressed to:

Data Protection Office
FIL Investment Management (Luxembourg) S.A.
2a, rue Albert Borschette/B.P. 2174
L-1246 Luxembourg

Last updated 1 June 2022