Client Privacy Policy

Overview

This policy sets out how and why LPFI Limited collects and processes personal data in accordance with the requirements of the data protection legislation below, specifically:

- The UK Data Protection Act 2018
- the UK GDPR (as defined in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419
- To the extent relevant, the EU's General Data Protection Regulation 2016/679

Information which LPFI collects

'Personal data' is formally defined in the data protection legislation as "any information relating to an identified or identifiable natural person ('data subject')".

As a data controller, LPFI collects personal data from data subjects associated with its clients (such as officers or authorised signatories) in connection with the services it provides. This can include names, dates of birth, contact details such as email address, telephone numbers and residential addresses. LPFI uses client on-boarding questionnaires, and annual AML and suitability confirmations which require copies of passports and driving licences to be provided, to collect this information, or it may directly request specific information from data subjects on an ad-hoc basis.

When clients are in contact with LPFI by phone, LPFI will collect and store the client's phone number and a recording of the call.

It may be necessary for LPFI to collect certain personal data, which is sensitive in nature, for example, to allow LPFI to comply with anti-money laundering laws or other laws, regulations or policies that apply to the organisation. However, this information is kept to a minimum and any information that is not relevant will be deleted.

How personal data is used

LPFI may use personal data relating to the data subjects associated with its clients for the following purposes:

- To communicate with the client's Pensions Committee, officers and employees in relation to the services
- To process identification details of the data subjects associated with the client (such as officers or authorised signatories) in order to confirm their identities to confirm their authority to sign legal documents (including but not limited to any subscription deed, partnership agreements and side letters, powers of attorney or sale and purchase agreements); and/or confirm the client's source of funds in order to comply with applicable anti-money laundering, anti-terrorist financing and similar laws, regulations and policies
- To comply with "know your client", anti-money laundering, anti-terrorist financing, creditworthiness, eligibility and any other checks carried out by: (a) any fund manager or service provider relevant to any of the client's investments; (b) any person from which, or alongside which LPFI intends to purchase fund interests on the secondary market; and (c) any person who provides services to LPFI or any member of LPFI's group
- To check such personal data against databases of individuals who are subject to sanctions, classified as "politically exposed persons" or have committed crimes and to follow up any

suspicions to ensure that LPFI complies with its anti-money laundering and terrorism obligations and to avoid fraud itself
- To record or monitor communications issued by LPFI to the client;
- To comply with agreements, legislation, treaties, instructions or guidance on the collection and/or sharing or exchange of tax(-related) information
- To make legal, regulatory, tax or other filings in relation to a client's investments, or LPFI itself
- To meet LPFI's legal, tax, compliance and regulatory duties
- To facilitate, support and/or enhance LPFI's operations and functions
- To liaise with any regulatory authority, tax authority or other body with jurisdiction over LPFI, any member of LPFI's group as required or deemed appropriate by LPFI in its discretion, notwithstanding that such processing may be undertaken by a party who is located in a territory which does not offer a level of protection for the rights and freedoms of data subjects which is equivalent to the data protection standards afforded within the United Kingdom
- To disclose to anti-fraud organisations and law enforcement or regulatory agencies anywhere in the world (and LPFI will be acting as a data controller in respect of such processing)
- For any other purpose that LPFI reasonably determines is necessary or desirable in connection with the services it is appointed to provide to a client.

Disclosure of Personal Data

LPFI may disclose personal data to any service provider to provide administration, legal or other services, in connection with its services to clients.

LPFI and/or its service providers may also disclose and/or transfer personal data to other members of its group, or its employees, officers, agents, delegates, sub-processors, sub-contractors, tax, legal and other advisors, auditors, administrators, brokers, accountants, custodians, investors and/or potential investors, placement agents, vendors or purchasers of investments, banks or other financial institutions or finance providers, registrars, tax authorities and/or other competent regulatory or governmental authorities or bodies, or any of the aforementioned persons' service providers, agents or advisers.

In most cases, LPFI's lawful basis for processing the personal data is because it needs to in order to meet its contractual obligations to clients in relation to the service it provides (for example, as part of its letter of engagement to arrange club deals in the private markets), or to take steps, at the client's request, before entering into a contract. On occasion, the reason LPFI processes personal data is because it needs to do so to satisfy its legal obligations (e.g. under anti-money laundering regulations).

LPFI is committed to doing all that it can to keep personal data secure. It has set up systems and processes to prevent unauthorised access or disclosure of such personal data. LPFI also makes sure that any third parties that it deals with keep all personal data they process secure.

During the course of the processing and disclosure described above, and in accordance with client instructions, certain personal data may be transferred to entities situated or operating in territories outside the UK. Where personal data is transferred outside the UK, LPFI reviews whether the relevant jurisdictions offer an adequate level of protection to personal data to ensure such transfers will be in full compliance with data protection legislation. To the extent required by the data protection legislation to legitimise any cross-border transfers of personal data, additional safeguards may be implemented. Please contact us if you want more information about the safeguards that are currently in place.

Information collected from other sources

LPFI and/or its service providers may collect personal data from the client, directly from the data subject, from any other person to which LPFI and/or service providers reasonably believe the data subject has given its consent to share such data with LPFI and/or such service providers, and from publicly accessible websites. LPFI will ensure that all information is kept up to date to accurately reflect the client's situation and details.

Retention

Personal data will be retained for as long as required or permitted by data protection legislation and/or as required for LPFI and any other person to whom the personal data may be provided for the purposes set out in paragraph headed 'Lawful Basis of Processing', including as required by the Markets in Financial Instruments Directive 2004/39/EC (as subsequently amended from time to time). The precise length of time we retain personal data depends on the purpose for which we collect and use it and what we are required to do to comply with applicable laws and to establish or defend our legal rights.

Personal data will be securely stored in accordance with LPF's Records Retention Schedule. Some records may be hosted on LPF's corporate network. Paper and electronic records will be disposed of in a secure way.

Access and Control

A data subject may, under certain circumstances:

- Withdraw its consent to processing of personal data (where applicable)
- Access its personal data and transfer its personal data to another controller
- Rectify its personal data
- Restrict the use of its personal data
- Request that its personal data is erased
- Object to the processing of its personal data.

The circumstances in which a data subject may take any of the above actions are set out in data protection legislation.

A data subject has the right to lodge a complaint with the ICO and, where LPFI has relied on consent to process the personal data, to withdraw consent at any time by contacting the client's LPFI client contact. Please note that where consent is withdrawn, this may impact the service which LPFI can provide to the client.

If you have concerns about the processing and use of your personal data, you can contact UK Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, Tel: 08456 30 60 60.

Communication to Clients

A copy of this policy is provided to LPFI's clients prior to the launch of services and is available at https://www.lpf.org.uk/about-us/lpfi/. LPFI will inform clients of any material changes to the policy and upon request, LPFI will provide further explanation about it to clients. Chief Risk Officer, Kerry

Thirkell, is responsible for the implementation of and compliance with this policy. Any complaints or enquiries about the operation of this policy should be addressed to Thi85K23@lpf.org.uk in the first instance.