

## External Privacy Notice for LPPI

**1. Introduction**

Welcome to the privacy notice for Local Pensions Partnership Investments Ltd (“LPPI”).

LPPI respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how LPPI and other entities in its group of companies look after your personal data and tell you about your privacy rights and how the law protects you.

It is important that you read this privacy notice together with any other notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements other notices and is not intended to override them.

LPPI is an FCA-regulated UK investment management firm which invests and manages the pension fund assets of its Local Government Pension Schemes clients on a discretionary basis. It is a wholly owned subsidiary of LPPI Holdings Ltd.

In most cases LPPI is the controller and responsible for your personal data where you, as an individual, have a relationship with LPPI, or with one of the funds we manage.

This privacy notice is likely to apply to you if:

- (i) You visit our website; or,
- (ii) if you are an individual who represents or is employed by:
  - a. a client or prospective client of LPPI;
  - b. one of LPPI’s service providers;
  - c. an investee company or investment fund in which an LPPI fund or an LPPI client is invested; or,
  - d. any other business partner of LPPI.

If your relationship with LPPI is that of an employee or other worker, please refer to our employee privacy notice located on the LPPI Intranet page, or request printed copy by writing to us at the addresses below. If you are a job applicant, you can access the relevant Privacy Statement through the WebRecruit application platform. .

**2. Our contact details**

LPPI has appointed a data privacy manager who is responsible for overseeing questions in relation to our handling of personal data. If you have any questions about our activities and practices relating to data processing, this privacy notice, or if you wish to exercise your legal rights, please contact the data privacy manager using the details set out as follows:

Email address:           dataprotection@lppi.co.uk

Postal address:           1 Finsbury Avenue, London EC2M 2PF

For the avoidance of doubt, we are not required, and have not appointed, a statutory data protection officer.

### 3. Your right to complain

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. However, we would appreciate the opportunity to address your concerns before you approach the ICO, so please contact us in the first instance.

The ICO's address and contact details are:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number:       0303 123 1113

ICO website:           <https://www.ico.org.uk>

### 4. Changes to this privacy notice and to your details

We keep our privacy notice under regular review. When we update it, we will publish the updated version on our website.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your business relationship with us.

### 5. The data we collect about you

Personal data, or personal information, means any information about an individual from which a person can be identified. It does not include data where the identity has been irreversibly removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity data** includes first name, last name, username or similar identifier, marital status, title, job title, date of birth and gender.
- **Contact data** includes billing address, delivery address, email address and telephone numbers.

- **Financial data** includes bank account and payment card details.
- **Transaction data** includes details about payments to and from you.

Other than as specified in LPPI's employee privacy notice and job applicant privacy statement, we do not collect any **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

## 6. How we collect your personal data

We will obtain some of your information directly and indirectly when we act as a service provider to our clients and where you represent or are employed by such a client.

We also obtain information about you from our service providers and business partners where you work with us.

We obtain information directly and indirectly in the course of our investment activity on behalf of our clients where you represent or are employed by an investee company or investment fund manager in connection with an LPPI fund or LPPI client investment.

This includes collecting information from you when you send us emails or otherwise communicate with us.

We will also collect some information from you when you interact with the website, visit our premises or attend our events.

## 7. How we use your personal data lawfully

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation.

**Legitimate interest** means the interest of our business in conducting and managing our business to enable us to give the best service to our clients and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights and freedoms before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

**Performance of contract** means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

**Compliance with a legal obligation** means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

With the exception of cookies deployed on our websites, generally, we do not rely on consent as a legal basis for processing your personal data. You can withdraw your consent to cookies on the cookies management tool available on our websites.

## 8. Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose / Activity	Lawful basis for processing including basis of legitimate interest
<p><b>Managing and administering our relationship</b></p> <p>Managing our relationship with you and the client you represent, updating and maintaining client records including for billing purposes</p>	<p>Legitimate interests in understanding and developing our relationship with you or the client you represent</p> <p>Contractual obligations</p>
<p><b>Managing and operating our business</b></p> <p>Day to day administration and management of our business; disclosing information to third parties, such as service providers, auditors, regulatory authorities and technology providers; processing in the event of a merger, reorganisation or disposal of, or a proposed merger, reorganisation or disposal</p>	<p>Legitimate interests in carrying out, improving and developing services and products</p> <p>Legitimate interests in connection with mergers, reorganisations or disposals</p>
<p><b>Preventing and detecting crime</b></p> <p>LPPI itself (or through a third party e.g. credit reference agency) processes certain information about client /service provider / investee company or fund/fund manager directors, officers and employees and beneficial owners in order to carry out anti-money laundering (AML) checks</p>	<p>Legitimate interests relating to the prevention of fraud, money laundering, terrorist financing, bribery, corruption, tax evasion and to prevent the provision of financial services to persons who may be subject to economic or trade sanctions, on an on-going basis, relating to making or</p>

and related actions which LPPI considers appropriate; monitoring and recording calls and electronic communications for investigation and fraud prevention purposes, crime detection, prevention, investigation	defending against legal claims, Legal and regulatory obligations
<b>Protecting and administering our premises and electronic infrastructure</b>  Access control measures; monitoring use of website for technical improvement and cybersecurity	Legitimate interests in administering and securing LPPI premises and electronic infrastructure
<b>Handling online queries</b>  Processing media enquiries, Freedom of Information requests, complaints, and corporate enquiries transmitted through our website	Legitimate interests in understanding and developing our relationship with you or the client you represent
<b>Publishing our websites and facilitating website navigation</b>  If you visit our website, we may deploy <i>cookies</i> and similar technologies to ensure core functionalities, including security and network management, to analyse how you use and interact with it, and to remember your preferences.	As set out in the relevant Cookie Notice, available at [ <a href="http://www.lppi.co.uk/your-privacy/">http://www.lppi.co.uk/your-privacy/</a> ]
<b>Processing job applications</b>  If you submit a job application to us	As set out in the relevant Job Applicant Privacy Statement, available through the WebRecruit application platform
<b>Managing your work relationship</b>  If you are employed or have another work relationship with us	As set out in the relevant Employee Privacy Notice, available on the LPPI Intranet.

## 9. Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Exceptionally, and where required or permitted by law, we may process your personal data without your knowledge or consent, in compliance with the above rules.

## 10. Sharing your personal data

We may share your personal data with the parties set out below for the purposes set out above.

- Other group entities acting as a joint controller, controller or processor.
- External Third Parties including:
  - service providers acting as processors (e.g. our IT service providers):
    - O2 / Telefonica – mobile phone recording;
    - ASC Technologies – call recording of certain MS Teams calls including chat and Teams ‘landline’;
    - Bloomberg L.P. – Bloomberg Vault stores information which includes personal data, including emails, mobile phone recordings, Bloomberg Mail and Instant Bloomberg messaging;
    - KeepIT – cloud data storage solution;
    - DocuSign – document execution platform;
    - HireRight – background screening provider;
    - Microsoft 365 – software provider for word document, presentation, email, cloud-based services and online calls;
    - WebRecruit – applicant tracking system;
    - Google – website analytics.
  - Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services
  - HM Revenue & Customs, regulators including the Financial Conduct Authority, and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of processing activities in certain circumstances
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

### **11. Transferring your data overseas**

Whenever we transfer your personal data outside of the UK, we ensure a similar degree of protection is afforded to it by implementing at least one of the following safeguards:

- the country to which we transfer your personal data has been deemed to provide an adequate level of protection for personal data;
- standard data protection clauses such as the UK IDTA which are deemed to give personal data the same protection it has in the UK.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

### **12. Protecting your personal data**

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

### **13. Retention of your personal data**

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

In some circumstances you can ask us to delete your data: see your legal rights, below, for further information.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

## **14. Exercising your rights under privacy laws**

### **14.1 Your rights**

Under certain circumstances, you have rights under data protection laws in relation to your personal data, as follows:

- Request **access** to your personal information (commonly known as a data subject access request). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request **correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request **erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- Request the **restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the **transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Privacy Manager in writing (which may be by email). Please refer to the Contact Details above

### **14.2 No fee usually required**

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

### **14.3 What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

### **14.4 Time limit to respond**

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

#### **15. Consequences of not providing your data**

Generally, the provision of your personal data to us does not arise from a statutory or contractual obligation with you. The notable exception is when you are employed, or want to be employed, by us. The potential consequences of your refusal to provide your personal data in these circumstances are addressed in the Employee Privacy Notice, or in the Job Applicant Privacy Statement, available at <https://lppi.co.uk/careers/>.

#### **16. Automated decision making**

We do not use your personal data to make any decisions solely by automated means (i.e. without human involvement) that could have a legal or similarly significant effect on you. Nor do we undertake profiling as defined under data protection laws.