your pension our world

London Pensions Fund Authority

Data Protection Policy

June 2022

London Pensions Fund Authority
Data Protection Policy

1. Introduction

Purpose of the data protection policy

The purpose of the Data Protection Policy is to set out London Pensions Fund Authority (**LPFA**) position in how it meets its legal obligations under the United Kingdom General Data Protection Regulation (**UK GDPR**) and Data Protection Act (**DPA**) 2018.

Data protection introduces rules around how an organisation manages, processes and protects the data that it holds regarding individuals. It also gives individuals rights related to the information that is held by LPFA and its third party service providers.

The context

From 8 April 2016, LPFA partnered with Lancashire County Pension Fund (LCPF) to establish Local Pensions Partnership Ltd (LPP Group), as a pensions services company. Subsequently the delivery of most of LPFA's functions have been outsourced to LPP Group through its pension administration subsidiary (Local Pensions Partnership Administration Ltd (LPPA)) and its FCA registered investment subsidiary (Local Pensions Partnership Investments Ltd (LPPI)).

These subsidiaries act as data processors in regard to LPFA's data. LPPA processes LPFA's pension fund member data and LPPI processes small amounts of personal data relating to LPFA staff accessing IT services which are provided by LPPI.

LPFA remains responsible for this Data Protection Policy (the "**Policy**") and for ensuring that LPFA, as the Administering Authority and its key suppliers, operate effective data protection measures. It is an expectation that such measures are achieved through effective internal controls and procedures in the collection, processing, and storage of data in line with regulatory requirements.

This Policy sets out LPFA's approach and commitment to data protection under the DPA and the UK GDPR.

LPFA recognises that its reputation for the protection of data must be maintained through the application of, and compliance with robust policies and processes.

2. Purpose and scope of the policy

LPFA is seen as a Public Body under Schedule 1, Part IV of the Freedom of Information Act (FOIA) 2000 and this is recognised in its ICO Registration.

ICO Registration Number: ZB080843.

LPFA as a data controller, is subject to the UK data protection regime, set out in the DPA, which includes the UK GDPR, with responsibility to gather and use certain information about individuals and members as part of its everyday functioning.

This can include data about members, employers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy sets out how personal data must be collected, processed and stored to meet LPFA's data protection standards – and in doing so comply with the law.

This policy supplements and supports the training, provided to all staff via e-learning systems and which can be audited to evidence compliance.

This policy applies to all LPFA staff including contractors, along with members of the LPFA Board and Local Pensions Board.

It applies to all personal data that LPFA holds relating to identifiable individuals. Personal data is defined in the UK GDPR as:

"personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

Personal data includes:

- names of individuals
- date of birth
- national insurance number
- bank account details
- postal and email addresses
- any other personal information relating to individuals

The UK GDPR refers to 'special categories of personal data' which is personal data that is more sensitive in nature and requires a higher level of application.

These are:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

Personal data can include information relating to criminal convictions and offences which also require a higher level of protection.

3. Risk appetite statement

The LPFA Board's Risk Appetite for material breach of the UK GDPR and DPA 2018 is "Minimalist" as set out in the LPFA Risk Appetite Statement.

The LPFA Board has identified that personal data breaches, failing to uphold data subjects rights and reputational damage, as key risks.

4. LPFA's general approach to data protection

All processing activities shall be carried out in accordance with the 7 Principles set out in the UK GDPR:

Principles

1. **Lawfulness, fairness, and transparency:** data is processed lawfully, fairly and in a transparent manner in relation to individuals
2. **Purpose Limitation:** data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. **Data Minimisation:** data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
4. **Accuracy:** data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. **Storage limitation:** data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
6. **Integrity and confidentiality (security):** data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures
7. A**ccountability:** the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1, a to f above.

5. Processing data

5.1 LPFA itself processes only small amounts of personal data, mainly in relation to employees and responding to member issues referred by LPPA, as the pensions administration provider. LPPA acts as a data processor relating to pensions administration.

5.2 Any internal processing is carried out under one of the 6 specified Lawful Basis as set out in Article 6 of the UK GDPR;

1) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
2) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
4) Vital interests: the processing is necessary to protect someone's life.
5) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

5.3 Where no lawful basis exists for the processing of data, processing will immediately cease, except for storage of the data in line with any retention schedule, policy, or legal requirement.

5.4 Where processing involves the data of children, parental consent must be sought, provided, and documented. Third-party processors must be able to provide evidence of this.

5.5 LPFA will obtain assurance of adherence to the requirements under the DPA regime from its data processors, through contractual obligations and oversight.

5.6 LPFA will seek documentary assurance that any other party acting as a data processor or joint controller has robust policies and processes in accordance with current regulations.

5.7 Where LPFA is engaging a third-party processor for LPFA data, it will seek documentary assurance that the processor has robust policies and processes in accordance with current regulations.

6. Rights of individuals

The UK GDPR provides the following rights for individuals:

- **The right to be informed:** Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.
- **The right of access:** Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
- **The right to rectification:** The UK GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- **The right to erasure:** The UK GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. It is not an absolute right and only applies in certain circumstances.
- **The right to restrict processing:** Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.
- **The right to data portability:** The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- **The right to object:** The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- **Rights in relation to automated decision making and profiling:** The UK GDPR applies to all automated individual decision-making and profiling. Article 22 of the UK GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

7. Subject access requests

All individuals who are the subject of personal data held by LPFA or its third party service providers are entitled to:

- Ask what information is held about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

An individual can make a Data Subject Access Request regarding the data held.

How will they ask?

A request must be made in writing (hard copy or email). If any individual makes contact using the phone, then they must be asked to put their request in writing. This is vital for LPFAs obligation in maintaining a register of the requests.

A typical data request could be:

- "Please send me a copy of my staff records"
- "Please could you send me all email correspondence wherever I am mentioned"

When a request is received it should be forwarded to the Compliance and Regulation Manager by sending an email to legal@lpfa.org.uk as soon as possible and within 24 hours of receipt.

Under the UK GDPR individuals can request this information free of charge.

It is important that before discussing personal information, security questions are asked to confirm the identity of an individual following any normal processes in place.

If contacted by a third party, ordinarily an individual may only speak to LPFA about their own data. In the case of a third-party request – the correspondent should provide a written authority signed by the individual in question. This can then be verified with the individual or records held.

Important note.

If there is any doubt on the authenticity of the request or the individual making the request, then information should not be provided, and the request should be flagged to the Data Protection Officer (DPO).

Requests for personal information relating to police investigations:

If contacted in relation to an on-going police investigation any such requests should be sent to the DPO immediately for action.

8. Data Protection Officer role and responsibilities

8.1 LPFA as a public body is required to have an appointed Data Protection Officer (DPO) who by nature of the role reports directly to the Board.

8.2 Details of the DPO and their contact details are made publicly available on the LPFA website.

8.3 The DPO or their delegated representatives:

8.3.1 will support LPFA in upholding the rights of data subjects in line with the regulatory principles outlined in this document.

8.3.2 will establish and maintain a programme to monitor compliance with this policy.

8.3.3 will provide advice and guidance on the requirements of this policy.

8.3.4 shall ensure that LPFA data protection training is in place for those within scope of this policy.

8.3.5 shall ensure that LPFA provides timely and appropriate access to information and information systems in the discharge of its duties.

8.3.6 will review, take appropriate action and report personal data breaches in line with current regulatory requirements and the LPFA data breach processes as shown at the end of this policy.

8.3.7 will review the policy at least biennially and lead on improvements in data protection risk management and monitoring audit recommendations.

8.3.8 will maintain the following registers:

i) Register of LPFA data processing activities in its Information Asset Register and Record of Processing Activity

ii) Register of data subject requests

iii) Register of data protection breaches

iv) Register of DPO contacts for joint controllers and processors.

9. Responsibilities of the Principal Officers

While the LPFA Board have oversight responsibility for this policy, the Principal Officers have the powers set out in the Scheme of Delegation and overall responsibility for:

- The design and implementation of LPFA's Data Protection risk management system.
- Ensuring that a sound system of internal control is maintained, including responsibility for the Record of Processing Activity (RoPA) for the relevant business function as information asset owners.
- Business is conducted in accordance with the law and proper standards; and
- That personal data is safeguarded and properly accounted for, used efficiently, and effectively in line with the UK GDPR and DPA regime.
- Participate in risk reviews and identify new data protection risks.

10. The key elements of the internal control environment:

- Setting the tone at the top for the rest of LPFA. Principal Officers create a culture through words and actions, where failing to uphold data subjects' rights and reputational damage due to data loss is not tolerated, that any such behaviour is dealt with swiftly and decisively, and that whistle-blowers will not suffer retribution.
- The establishment of a Compliance Monitoring Programme which ensures compliance with established policies, procedures, laws, and regulations through compliance monitoring activities.
- Implementing adequate internal controls — including documenting Data Protection risk management policies and procedures and evaluating their effectiveness.
- Reporting to the LPFA Board and Local Pension Board (LPB) on actions taken to manage DPA risks and the effectiveness of the data protection risk management program. This includes reporting any remedial steps that are needed, as well as reporting actual Data Breach instances.
- The various functions within LPFA will be responsible for keeping and maintaining a Risk register that will include data protection and information asset security. This will be supported and audited by the Compliance function in line with the LPFA Compliance Monitoring Programme.

11. Responsibilities of all employees and officers

LPFA has, and maintains, effective controls against data protection breaches, which are the responsibility of everyone in LPFA.

LPFA is responsible for gaining assurance that providers of services such as LPP Group, LPPA, LPPI and any other third-party providers have and maintain their own policies and procedures to satisfy DPA and GDPR regulations.

All levels of employees, including Principal Officers, excluding LPFA Board members and LPB members should:

- Have a basic understanding of Data Protection and information security protocols and how to identify a Data Subject Access Request.
- Undertake the mandatory training in line with this policy.
- Understand how their job procedures/processes are designed to manage data protection risks and understand when non-compliance may create an opportunity for a breach to occur or go undetected.
- Comply with established procedures, policies, delegations, and codes of practice, including other operational policies and procedures, such as procurement manuals.
- As required, participate in the process of creating a strong controlled environment, including monitoring, designing, and implementing data protection control activities.
- Consider the risk of data protection breaches when reviewing LPFA's risk registers.
- Co-operate in data protection investigations
- Deploy the aim of "Data protection by design and default" in all system, processes and activities undertaken within day-to-day work.
- Report any data protection breaches promptly and within a maximum timeframe of 24 hours using the Data Protection Breach Reporting Form shown at the end of this policy.

12. Record keeping requirements

LPFA functions are responsible for recording the risks and mitigation actions of all data collection, processing and storage that takes place.

This should include information and evidence of:

- Processing activities, including the lawful basis for the activity, which can be evidenced via a Record of Processing Activity (RoPA) which is contained in the Information Asset Register
- Any third-party service or systems providers Data Protection and Information Security policies and procedures, along with the RoPA, Information Asset Registers (IAR) or other registers containing information deemed as a minimum by the ICO. For example, data retention periods, purpose and whether it is key data. This should be reviewed on a regular basis and at least annually.
- Contractual agreements with joint controllers, processors and other third-party service providers including data processing agreements.
- All functions should use the LPFA Data Breach Reporting Form to ensure a consistent approach to data breach reporting.
- A central Data Breach Log will be maintained by the DPO or delegated team members.

13. Independent audit and the Audit and Risk Committee

Independent Audit

Independent audit will be carried out at prescribed intervals as part of the LPFA audit programme providing reassurance to the LPFA board and ARC of compliance standards.

Audit and Risk Committee

The Audit and Risk Committee reviews the internal (management) reports and should satisfy themselves that the integrity of the information presented is robust and reflects best practice and compliance.

The Audit and Risk Committee may request assurance statements on the internal control environment of key suppliers such as LPP Group's subsidiaries. This could be in the form of direct reports from LPP Group itself, or via internal or external auditors who have reviewed a particular area of LPP Group's operations.

Compliance monitoring programme

The Compliance and Regulation manager, within the Legal, Governance and Compliance Team is responsible for creating, maintaining, and undertaking the Compliance Monitoring Programme.

This will audit systems, processes, and guidance to capture and report on what is happening against what should be happening. A report will be shared periodically with ARC, the LPFA Board and LPB.

Learning from experience and minimisation of losses

LPFA seeks to ensure that where it suffers or causes a data breach, that loss is minimised, a review is carried out to ensure the causal act is not repeated. The review may be localised, or if serious enough involve independent audit.

The following steps should be taken:

- Investigate whether there are more cases of a similar nature.
- Investigate all areas of activity of any person(s) implicated.
- Identify whether there was an absence or lapse of internal control and recommend improvements.
- Ensure that there are controls to either prevent or detect data losses, protecting LPFA from being vulnerable to data losses, the risk to reputation and the possibility of being fined.

To meet the above requirements, LPFA will ensure that actions are carried out, (with the support of LPP Group subsidiaries relating to personal data processed within the group), that:

- Ensure that areas at risk are identified and action is taken to mitigate the risk.
- Develop a robust and vigilant DPA culture - monitoring DPA risk within our control, with a view to reducing the risk where possible.
- Hold managers accountable for performance of their areas of responsibility.
- Prevent data breaches through good practices and encourage best practice.
- Verify the identity of members and third parties where necessary, keeping records. Maintaining sufficient documentation to demonstrate compliance with the DPA requirements.
- Comply with all applicable legislation and other relevant requirements that may be relevant.
- Assess, in advance where possible, DPA impact resulting from business operations and the effects of any significant business development and adjust the plans accordingly.
- Ensure that all DPA incidents are reported, recorded and root causes identified where the incident occurs or could have occurred and ensure that corrective and preventive actions are implemented.
- Communicate any necessary information and training to enable all internal/external stakeholders, affected by the LPFA's undertakings, to carry out their duties.

This policy will be made available to LPFA employees, LPFA Board members and LPB members, and those working for or on behalf of the LPFA.

An individual's failure to comply with some of the DPA legal responsibilities may constitute a criminal offence which could lead to a personal criminal prosecution. Additionally, LPFA may be at risk of incurring penalty fines and reputational damage if LPFA and its employees, officers and contractor fail to comply with legal requirements of the DPA. Therefore, it is vital that individuals are familiar with their responsibilities under the DPA and this policy.

Failure to comply with the DPA, this policy or any related guidance may lead to disciplinary action.

This policy will be reviewed every two years.

Data Breach Process

Data Protection Breach identified, evidence gathered and any further losses prevented

DPA report form completed fully and submitted to legal@lpfa.org.uk within 24 hours of breach

DPO will direct investigation and decisions on notifying Board, CEO and officers, data subjects and ICO

DPO may request root cause analysis (RCA) from business function as part of investigation process

Compliance monitoring may carry out a deep dive review of practices and any required remedial actions as part of the RCA

Important information

When a data breach is identified, it is important to act quickly to gather information on the breach, note the time and date of the breach, what data has been lost and by who, whose data has been lost and can restriction be put in place to stop any further loss or breach of data.

The breach must be reported within 24 hours maximum to the data protection officer (DPO) via the LPFA Data breach reporting form. This must have the first section completed as fully as possible and be sent to legal@lpfa.org.uk

The DPO will;

- review the breach information and carry out the investigation with the assistance of the reporting individual and team
- notify the CEO and Board as appropriate
- notify the affected individuals as appropriate
- notify the ICO as appropriate
- direct any further actions as deemed appropriate during or following the investigation

LPFA data security breach reporting form

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is Stored, Inappropriate access controls allowing unauthorised use, Equipment failure, Human error, Unforeseen circumstances such as a fire or flood, hacking attack, 'Blagging' offences where information is obtained by deceiving the organization who holds it.

This form must be completed and sent to legal@lpfa.org.uk within 24 hours of identification of the breach. Please ensure you complete all sections that apply.

Date and time of Notification of Breach	
Notification of Breach to Data Protection Officer by: Name Contact Details	
Details of Breach – what information, when, how.	
Nature and content of Data Involved – personal, sensitive, commercial.	
Number of individuals affected:	
Business Entity where breach occurred	
Name of individual investigating breach Job Title Contact details Email Phone number	
Assessment of ongoing risk and likelihood of other occurrences.	
Containment Actions: technical and organisational security measures applied (or to be applied) to the affected data. When were they or when will they be done? Who is responsible for taking actions? Who is responsible for authorising and checking completion of actions?	
Recovery Plan outline and link to detail document, if required.	

Data Protection Officer actions record of actions	
Information Commissioner informed - Time and method of contact	
Other authorities informed as appropriate (please list) Time and method of contact Name of person contacted Contact details	
Individuals impacted by Breach contacted? How many individuals contacted? Method of contact used to contact? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Relevant Staff briefed (CEO, Board etc) as required.	
Evaluation and response if any required.	
Are all actions completed and the data breach case closed? If so when and by whom?	