Pension Protection Fund

Privacy Notice – PPF Employees

Data Controller

Controller Name: The Board of the Pension Protection Fund (PPF)
Contact: Data Protection Officer
Renaissance House
12 Dingwall Road
Croydon
CR0 2NA

Introduction

Your privacy matters to us, so you can be confident that we take good care of all the personal data we hold about you. One of the ways we do this is by adhering to the requirements and principles of data protection legislation. In this privacy notice we explain the reasons we handle your personal data, what happens to it and your rights in relation to it.

What personal data we collect

We collect the following data about our employees which we've grouped into broad categories:

- Home contact – name, address, telephone number (home/mobile), email address (private)
- Work contact – name, email address, telephone number(s), availability
- Core details – date of birth, marital status, national insurance number, employee number, emergency contact
- Recruitment records – applications, scoring, notes, right to work forms and evidence (e.g. copy of passport), reference outcomes
- Performance records – performance development process (PDP) records, quality assessment (QA) of work (e.g. calls with members), notes of one-to-ones with line managers, assessments, attendance, disciplinary records

Pension Protection Fund

- Sensitive data – racial or ethnic origin, religious or philosophical beliefs, health, sexual orientation
- Security data – logs of access to offices and systems, card use tracking data, level of office access, images for identification, surveillance camera footage, vulnerability (e.g. virus) scanning logs, activity logs for IT systems
- Financial details – pay, expenses, payslips, P60s, bank details, pension contributions, PAYE tax data, deductions, personal account investments
- Benefit details – selected benefits, pension scheme, leave records (annual, parental, compassionate, sickness, etc.), flexible working arrangements
- Interaction records – correspondence, call recordings, survey responses
- Communications materials – images, biographies, interests.

Why we use your personal data

Below we provide details of the different ways that your personal data is used and our lawful basis for using it. Beneath each explanation, we have set out the types of personal data affected and details of when and how we share your data with third parties.

There are specific circumstances where it is necessary for third parties to have access to your data. Where this is the case we ensure that appropriate contractual, technological and other safeguards are in place:

- We will disclose your personal data if required to by law. For example, to Her Majesty's Revenue and Customs (HMRC) for tax purposes or to the police for the prevention or detection of crime. Regulators, such as the Information Commissioner (ICO), also require us to share information on occasion. As a public corporation, we can be required to provide data on our establishment to government departments.
- Like most organisations, we rely on companies to support our services, and in some cases they will need to collect, access or handle your personal data. For example, increasingly our IT infrastructure operates in the cloud, which means that suppliers store data for us. Suppliers and their employees are only allowed to access or handle personal data with our permission and where it is strictly necessary for them to fulfil their contract with us. In some cases they will appoint sub-contractors and where this is the case, suppliers will be expected to ensure they are subject to the same requirements.

Employment administration

Pension Protection Fund

When you are employed by the PPF we need to keep records of our contract with you and how we manage that contract. This includes recording your leave of absence from the PPF. In some cases (sick leave, maternity leave) we will need to record data relating to your health. In order to pay your salary and any expenses you claim, we need to handle personal data such as how much we pay you and your bank details. We also have to know what benefits you have opted in to and how much tax you owe so that we can take the correct deductions. If you are on long-term sick leave we need to ensure we are paying you the correct amount. On rare occasions we need to recover any overpayments made to you.

We need to retain your personal data as it's necessary for the performance of our contract with you.

- Type of personal data: core details; home contact; work contact; recruitment records; sensitive data; benefit details; financial details; performance records; interaction records (such as correspondence with Human Resources staff or your line manager)
- Data sharing: recruitment agencies; recruitment portal; pre-employment checks administrator; auditors; People Matters and employee records system providers; our IT network in the cloud; records storage and confidential waste disposal; digital file sharing tool providers; our bank; our finance system provider; HMRC; pension and other benefits providers where necessary

Managing your performance and development

We need to ensure that our employees are performing their work adequately and where appropriate reward success. This requires us to collect information about your performance. For most PPF employees this is managed by line managers through the personal development process. Some customer facing staff will be subject to additional monitoring through quality assessment processes. Contact Centre and Operational Levy employees will have external telephone calls (out-bound and in-bound) recorded for this purpose. We review security pass data to assess compliance with our hybrid working policy (i.e. the days staff attend the office). We provide a number of development opportunities to our employees including training courses, coaching and mentoring. It will normally be necessary for records of your progress to be maintained by the training provider, coach or mentor. Unless you are told otherwise these records will not be shared with us. We will also need to retain records of your professional development. In some cases it's necessary for us to share information with professional or accreditation bodies.

Pension Protection Fund

We need to monitor your performance to ensure that you are fulfilling your employment contract. Additional performance monitoring is conducted as it is necessary for us to provide a quality service to our members and levy payers in line with our public task set out in the Pensions Act 2004. Records of your training and development need to be kept to meet our legitimate interest in your continuing development, and we also have a legitimate interest in assessing the success of new ways of working.

- Type of personal data: work contact; performance records
- Data sharing: People Matters and employee records system providers; training providers; online training provider

Providing your benefits

In order for the PPF and its benefits administrator and providers to provide benefits to PPF employees, it is necessary for us to collect and process your personal data. Your details are used by our benefits administrator to provide you with access to the benefits portal. Your details are also shared with the providers of the insurance and pension schemes that you have opted in to. When you opt to receive a particular benefit through the portal, you are entering into a contract with the provider of that benefit. Our benefits administrator will need to share relevant personal data with the provider, and the provider will need to process your data in order to provide the requested service. The providers of your benefits and rewards have their own terms and conditions and data processing requirements. You are advised to check these before opting for a particular benefit.

We share your data with our benefit administrator as it is necessary in order to be able to administer our employee benefit and rewards scheme (our legitimate interest). They let us know which benefits employees have signed up to which is necessary for tax purposes. They use your personal data to ensure that you receive the correct rewards and benefits, to improve products and services, and to send you information about the benefits portal and the rewards and benefits that you might be entitled to. This is necessary so that they can administer your benefits, improve their service to you and to keep you informed about changes to the service (their legitimate interests).

- Type of personal data: work contact; core details; benefit details
- Data sharing: benefit portal provider; insurers, pension and other providers (see the benefits portal for details)

Ensuring equality and diversity

Pension Protection Fund

We have obligations to advance equality of opportunity and in order to do this we need to better understand the make-up of the PPF's workforce. For this reason we collect data as part of the recruitment process and then via People Matters on race, sexuality, gender, and long-term health conditions. The data is aggregated and used to produce reports; data about identifiable individuals is not used other than to produce these reports.

We use this data because it is necessary in order to advance equality in line with our public sector duties under the Equality Act.

- Type of personal data: work contact; sensitive data
- Data sharing: recruitment portal; People Matters and employee records system providers

Keeping you and your colleagues safe

We have a duty of care for you and other employees and this means that we need to collect and use data about your health and wellbeing. If you have an accident in the workplace details will be retained. We also retain records of DSE assessments carried out on your workspace. If you call in sick the reason will be recorded on People Matters. Where necessary for public health purposes, the numbers of employees reporting particular symptoms or conditions may be reported to Risk and to Executive Committee.

It is necessary to collect and use this data to meet our legal and contractual requirements to provide a safe workplace for you and other employees.

- Type of personal data: work contact; sensitive data
- Data sharing: HSE (only in case of a RIDDOR reportable accident)

Keeping our premises and infrastructure secure

When you join the PPF you are issued with a security pass which provides access to the PPF's offices. Your work contact details, a photograph and card tracking data is stored on a system provided by our landlords. Card tracking data is used to identify and investigate breaches of physical security and also to produce reports on office attendance to assess compliance with hybrid working policies (see the section on Managing your performance and development above). We have surveillance cameras in place in our offices which are intended to prevent and assist with the investigation and prosecution of crime as well as to ensure the safety of our premises, employees and visitors. It's not just our physical premises that need to be kept secure – we also need to protect our IT infrastructure from threats, intentional or otherwise. We collect data on systems

Pension Protection Fund

activity which includes details of when you log on and off systems, and your geographical location. This remains relevant when remote working using PPF or your own devices. Access to external websites and online resources is monitored to ensure that use is consistent with the Acceptable Use Policy. We also scan for vulnerabilities and security weaknesses across our estate.

It is necessary to process your personal data as part of these activities in order to meet our legitimate interest in securing our premises and infrastructure.

- Type of personal data: work contact; security data
- Data sharing: building management (in Cannon Street and Renaissance); systems vulnerability and activity monitoring providers

Keeping the PPF working

We need to log incident reports (whether operational risk, IT support or Office Services related) and will need to use your details in order to respond. In some cases incident reports will name employees. Your mobile phone number will be used to send you messages where necessary as part of an incident response.

When you book a desk in the PPF's offices, your name and the date and time of your booking will be recorded and will be visible to other PPF employees. The company that provides and administers the PPF's desk booking system publishes a detailed privacy notice explaining how your data is used which can be accessed when you log in to the application.

It is necessary to process your personal data to meet our legitimate interests in responding to incidents, maintaining our services and providing adequate and safe facilities for our employees.

- Type of personal data: home contact; work contact
- Data sharing: emergency messaging; desk booking system

Seeking your views

We collect your views through the annual staff Viewpoint survey. The survey is conducted for us by a company who report the results to us. The process is designed to preserve the anonymity of respondents so we do not receive information about who has provided particular feedback (unless you include identifiable information in a free text box). We also seek to keep you informed about developments throughout the year and to take on board your views. We do this through a number of forums, notably Directorate Stand-Ups, Town Halls and the Employee Liaison Committee. We use video conferencing software to

Pension Protection Fund

facilitate many larger meetings so your image, name and any comments you make will be visible to participants. Some meetings (e.g. Town Halls) are recorded so that they can be shared with staff unable to attend so your image, name and comments will be preserved as part of these recordings. We occasionally conduct research into aspects of our working environment and you may be asked to contribute.

It is necessary to process your data in these circumstances to meet our legitimate interest in communicating with, and understanding the views of, our employees.

- Type of personal data: work contact; interaction records
- Data sharing: staff survey provider; ad hoc surveys; video conferencing

Handling disputes

If someone raises a grievance, is subject to disciplinary action, or reports a concern under the PPF's Whistleblowing Policy, we will need to record the process followed and collect evidence from complainants, witnesses and subjects.

It will be necessary to handle your personal data to ensure that employment contract obligations are fulfilled and to meet legitimate interests in resolving disputes and identifying areas for improvement.

- Type of personal data: work contact; performance records
- Data sharing: People Matters and employee records system providers

Ensuring compliance

We maintain records to demonstrate and facilitate compliance with regulations in relation to potential conflicts of interests, data protection breaches, bribery, fraud, personal account dealing, and gifts and hospitality. External telephone calls (out-bound and in-bound) of Investments employees are recorded to preserve client orders. Messages sent and received by Investments employees on the Bloomberg trading system are retained and monitored by Compliance and Ethics staff. Details and proof of identity of named individuals are shared to meet 'Know your customer' rules. Evidence of entitlement to work in the UK will be collected by Human Resources when you join the PPF.

All of these are necessary for us to meet legal requirements.

Pension Protection Fund

- Type of personal data: work contact; recruitment records; financial details; interaction records
- Data sharing: fund managers and brokers; investments management system

Answering information rights requests

If you exercise your rights under data protection legislation (primarily the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA)) or the Freedom of Information Act 2000 (FOIA) or Environmental Information Regulations 2004 (EIR), we will need to handle your contact details, your request and relevant information.

We need to handle your personal data to help meet our legal obligations under GDPR/DPA and/or FOIA/EIR.

- Type of personal data: basic details; interaction records; other information as relevant to request
- Data sharing: third parties (consultation where they are affected); ICO (in the event of an appeal)

Voluntary activities

If you sign up to social events, the Employee Liaison Committee (ELC) will need to process your details. If the event is being provided by a third party, it may be necessary to share your details with the provider. In this case ELC will either inform you before sharing any data or you will be asked to provide your details directly to the provider. Before providing details to third parties you are advised to check their terms and privacy notice. If you choose to participate in voluntary work with charities organised by the PPF, we will keep records of your involvement and will need to share your details with the charity. For your own safety as well as others, we will occasionally need to share details of relevant medical conditions.

We ask for your consent to handle your personal data in connection with voluntary activities.

- Type of personal data: work contact; (rarely) home contact; sensitive data
- Data sharing: event facilitators/providers; charities you offer to volunteer with

Promoting and reporting on the PPF's work

Pension Protection Fund

Your image and biographical information may be used in PPF publications within the PPF (e.g. on the intranet) or externally.

We have a legitimate interest in promoting the PPF and its activities, and sometimes it will be necessary for us to use your details to do this. However, you will always have the opportunity to opt out. You will be asked to complete a form giving your explicit consent before we use photographs of you. Consent can be withdrawn at any time.

- Type of personal data: communications materials
- Data sharing: publishers; web design; web hosting

Special Category Data

We sometimes need to use special category data about you. Special category data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual orientation or sex life, as well as genetic or biometric data used to identify individuals. We will also need to process criminal conviction data on occasion.

The specific purposes for which we use such data about employees are as follows.

- employment administration (health data, criminal records for pre-employment checks)
- administering leave and flexible working arrangements (health data)
- keeping you and your colleagues safe (health data)
- administering voluntary work (health data)
- ensuring equality and diversity (racial/ethnic origin, religious or philosophical beliefs, health data, sexual orientation)
- ensuring compliance (criminal records).

In addition to the lawful basis set out above for each of these purposes, it is necessary to use special category data to meet our legal obligations as an employer; for health and social care purposes (e.g. occupational health referrals); for statistical purposes; for the purposes of monitoring and promoting equality and diversity; protecting the public against dishonesty; and preventing fraud or money laundering.

Where possible we inform you before handling data of this kind and only collect or use it where necessary. We make it easy for you to check and update your records, and take appropriate security precautions to protect your data. Data is

Pension Protection Fund

retained and then destroyed securely in line with the PPF's Retention and Disposal Schedule.

International transfers of personal data

Most of our service providers are based in, and process personal data in, the UK. There are a small number of circumstances in which your personal data will be handled abroad:

- Human Resources e-filing system: the system, called PeopleDocs, is cloud-based. The data is stored in France and Germany, countries which have the same standard of data protection as the UK.
- Surveys: we occasionally use Survey Monkey, a US-based company, to conduct surveys of our employees. This involves sharing your work email address.
- Video conferencing: when we use Zoom for meetings, your work details, your image and any contributions you make in the meeting are processed by the supplier. Zoom will process your data at data centres outside the UK.
- Online training: our e-learning supplier, KnowB4, is based in the USA and collects information about your completion of training.
- Small businesses: some of our smaller providers rely on sub-contracted services (e.g. Google, Dropbox) that require data to be stored abroad. Examples are training and social event providers.
- Fund managers and brokers: the nature of investment work means that to meet legal requirements KYC data will need to be shared with providers abroad.
- Auditing: where it is necessary for us to share your data with our auditors, this is done using data storage and sharing service Box. Box stores some data on servers outside the UK. Box has approved binding corporate rules (BCRs) in place to ensure that personal data is handled to appropriate standards wherever it is processed.
- Emergency messaging: the current provider (ClickSend) is based in Australia. Only your mobile phone number is shared with them.

Where necessary, we have agreements with these companies which incorporate international data transfer clauses approved by the Information Commissioner's Office. We require companies to comply with the standards set out in data protection legislation and to put in place appropriate security measures before we agree to share your data with them.

Pension Protection Fund

How long will we keep your data?

We'll keep your information in line with our retention policy. The policy is set out in the Retention and Disposal Schedule which is maintained by Information Security and Privacy and can be accessed via their Trunk site.

Exercising your rights

Under data protection legislation you have the right to ask to see the personal data we hold about you and to ask why we hold that information. Other rights you have are to ask us to correct data that you believe to be inaccurate or to ask us to stop using your data if you believe that we no longer need it to carry out our work. Don't forget that you can access and amend many of your records yourself in People Matters.

If you're unable to access or update information using People Matters and would like to exercise any of your rights you should write to:
HRAdmin@ppf.co.uk

We aim to comply with requests made under data protection legislation as quickly as possible and within a month of receipt unless there is a good reason for delay. If there is any reason why we cannot respond this quickly we will let you know when you can expect to hear from us and the reason for the delay.

The PPF's Data Protection Officer and raising concerns

The PPF has a Data Protection Officer (DPO) whose role is to act as a point of contact for individuals and to monitor and provide advice to the PPF in relation to data protection issues. The PPF's DPO is Dana Grey, Interim Chief Risk Officer. If you have any concerns with the way your personal data is being handled you can contact the DPO by emailing compliance@ppf.co.uk.

The Information Commissioner

If you're not satisfied with our response or believe we're not processing your personal data in accordance with the law you can complain to the Information Commissioner's Office (ICO).

Pension Protection Fund

The Information Commissioner can be contacted at:

Address: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Telephone: +44 303 123 1113
Website: www.ico.org.uk

Changes to the privacy notice

We keep our privacy notice under regular review and we will place any updates on the Human Resources and Data Protection and Freedom of Information intranet pages. This privacy notice was last updated in June 2022.

Pension Protection Fund

Annex: main suppliers who process employees' personal data

Supplier	Purpose of processing	Privacy notice
Benefex	Employee benefits administration	You can access this in the Benflex Reward Hub
Bloomberg	Investments management system	https://www.bloomberg.com/notices/privacy/
Box	Document storage and transfer (for audits)	https://www.box.com/en-gb/legal/privacypolicy
Clicksend	Emergency messaging	https://www.clicksend.com/gb/legal/privacy-policy/
Cloudbooking	Desk and room booking	https://ppf.cloudbooking.com/Library/_Generic/CBGDPR.pdf
CVInsights	Pre-employment checks	Ask HR for a copy
Deloitte	Auditing our accounts	https://www2.deloitte.com/uk/en/misc/audit-privacy-statement.html
Employee Feedback Ltd	Viewpoint staff surveys	Not available
KnowBe4	E-learning portal	https://www.knowbe4.com/product-privacy-notice
Lloyds Bank	Banking	https://www.lloydsbank.com/help-guidance/customer-support/privacy-explained/data-privacy-notice.html
Legal & General	Defined contribution pension scheme	https://www.legalandgeneral.com/privacy-policy/
Microsoft	Cloud storage	https://privacy.microsoft.com/en-gb/privacystatement
Midland HR	People Matters system support (occasional access required)	https://mhrglobal.com/uk/en/privacy-policy
Mimecast	Secure email	https://www.mimecast.com/company/mimecast-trust-

Pension Protection Fund

		center/gdpr-center/privacy-statement/
MyCSP	Defined benefit pension scheme	https://www.civilservicepensionscheme.org.uk/privacy/
Networx	Recruitment portal	Ask HR for a copy
Nudge	Website design/hosting	
Oracle	Finance system (expenses administration etc.)	https://www.oracle.com/uk/legal/privacy/services-privacy-policy.html
PeopleDoc/UKG	HR digital filing system	https://privacy.people-doc.com/en/userdata
Pro2Col	GoAnywhere Managed (secure) File Transfer	https://www.goanywheremftexperts.com/privacy-policy/
Restore	Storage and secure destruction	https://www.restoreplc.com/sustainability/policies/
Survey Monkey	Ad hoc staff surveys/quizzes	https://www.surveymonkey.co.uk/mp/legal/privacy/
TSO	Publishing of PPF official documents (e.g. annual report and accounts)	https://www.williamslea.com/privacy-statement
Zoom	Virtual meeting support	https://explore.zoom.us/en/privacy/