



## GDPR - Pensions & Pegasus Data Record Summary

- The Law Debenture Pension Trust Corporation p.l.c.
- Pegasus Pensions plc

Date of version:	May 2021
Created by:	Risk & Control Consultant
Reviewed by:	Law Debenture Pensions Risk Committee
Approved by:	Law Debenture Pensions Risk Committee
Next review date	January 2023
Document classification:	PUBLIC

**PUBLIC** - The contents of this document may be shared with external parties such as clients and prospective clients without permission from the Statement creator.

## Document Control

This is a CONTROLLED document and updates or changes to this document are authorised and then made available on Law Debenture's intranet.

It is UNCONTROLLED when printed. You should verify that you have the most current version.

Review Date:	Review Completed by:	Reason for change:
February 2020	Pensions Executive	Creation
May 2021	Risk & Control Consultant	Regular refresh
January 2022	Risk & Control Consultant	Regular refresh

## Overview

The UK Data Protection Act 2018 (“**GDPR**”) requires organisations to maintain a record of the personal data processing activities under their responsibility (the “**Data Record**”).

The Data Record is intended to be a living document which should be reviewed and updated as processing activities change and develop. Its content will depend entirely on how the relevant personal data is processed - which will always be a matter of fact.

The GDPR specifies that the Data Record for controllers shall include:

- the name and contact details of the controller, the controller's representative and the person responsible for Data Protection
- the purposes of the processing
- a description of the categories of data subjects (i.e. the people identified by the relevant personal data) and of the categories of personal data
- the categories of recipients to whom the personal data have been or will be disclosed including recipients outside of the UK in third countries or international organisations
- where applicable, transfers of personal data outside of the UK to a third country or an international organisation, including the identification of that third country or international organisation and, the documentation of suitable safeguards taken in respect of exceptional transfers undertaken by the controller (i.e. those which are not based on an adequacy decision or other appropriate safeguard prescribed by the GDPR).
- where possible, the envisaged time limits for erasure of the different categories of data
- where possible, a general description of the technical and organisational security measures taken to protect the personal data

## Controller Name and Contact Details

This Data Controller Record applies to The Law Debenture Pension’s corporate entities. The controller names and contact details are;

- The Law Debenture Pension Trust Corporation p.l.c.  
8th Floor, 100 Bishopsgate, London, EC2N 4AG
- Pegasus Pensions plc  
8th Floor, 100 Bishopsgate, London, EC2N 4AG

## Data Protection Officer Details (If Applicable)

N/A – Colleague responsible for GDPR and Data Protection is the Chief Operating Officer.

## Joint Data Controllers

Where Law Debenture are acting as a Trustee, they may be acting as a Joint Controller with other Trustees. In which case, Law Debenture will process Personal Data in accordance with this Data Record.

## Categories of Data Subjects

- Active members
- Deferred members
- Pensioners (including those in receipt of a dependant's or a spouse's pension)
- Prospective members or those named on a member's expression of wishes form who will or may receive benefits from the scheme (for example on the death of a member)
- Former members (for example members who have transferred out of the scheme)
- Ex-spouses of members (for example following a pension sharing order)
- Persons who claim to be any of the above.
- Trustees (e.g. where Law Debenture are acting as one of a number of Trustees and not a Professional Corporate Sole Trustee).
- Trustees' professional advisers and service providers (for example legal advisers, auditors, actuaries, communication consultants, investment consultants, administrators).

## Categories of Personal Data

- Employment and pension scheme membership data including dates of joining and leaving employment, periods of pensionable service, earnings and details of other benefits.
- Personal data including name, date of birth, gender, contact details (e.g. home address, telephone numbers and e-mail address), identifiers such as National Insurance number, member or system identifiers.
- Pension contribution and benefit data, including compulsory and voluntary contributions, actual or potential defined benefits, defined contribution account information (e.g. investment allocation and account balance).
- Other financial data such as National Insurance contributions, bank sort code and account number, tax code, Lifetime Allowance and other tax protections.
- Family data and data regarding personal and financial circumstances including current marriage or civil partnership, details of financial dependency, any previous relationships and dependants, death benefit expression of wishes and distribution information.

- Data provided in connection with dispute resolution, including details in support of a claim for financial or non-financial loss
- Identification documents including birth, marriage, civil partnership and death certificates, passport identity pages, decree absolute, pension sharing and earmarking orders, wills.
- Special Category Data including personal health data in connection with eligibility for ill-health and death benefits and payment of ill-health benefits.

## Third Parties with Whom Data May be Shared

- Trustees' professional advisers (for example legal advisers, auditors, actuaries, communication consultants, investment consultants)
- Service providers (for example administrators, payroll providers, printing agencies, banks and tracing agencies, financial advisers appointed to support members)
- Participating employers and their advisers
- Insurance providers
- Regulatory authorities (for example the Pensions Regulator and HM Revenue & Customs)
- Intra-group Law Debenture entities for the purpose of group infrastructure and support services, for example IT infrastructure and software support.

## Purpose of Processing and Other Information

- To confirm a member's identity and establish the eligibility for benefits.
- To calculate and pay pension benefits and deal with any questions about these.
- To calculate and pay tax charges, monitor whether allowances are exceeded and report to HM Revenue & Customs.
- To meet the compliance requirements with regulatory legal obligations, such as governance requirements, reporting to relevant authorities and government bodies.
- For risk management purposes, including the insurance or management of longevity risks and obtaining quotations for annuities or other insurance products.
- To communicate with pension scheme members about their benefits and the pension scheme in general.
- To trace members and other beneficiaries.
- To meet "Know Your Customer" and anti-money laundering regulatory requirements of trustees and other service providers.

## **Names of third countries or international organisations that personal data are transferred to (if applicable)**

Personal data will only be transferred to third countries for the purposes of processing, to the third parties identified above where those parties are in a third country. For example, a member may have relocated to a third country from where the participating employer and scheme is operated.

Law Debenture will not transfer data outside the United Kingdom unless such transfer is:

- to a recipient in an Adequate Territory;
- to a recipient that has entered into the Model Clauses;
- to a recipient in circumstances where Law Debenture is entitled to rely on a permitted derogation under Data Protection Law, which may include circumstances where (among other things) the transfer is necessary for the establishment, exercise or defence of legal claims

## **Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable)**

Our clear preference is to work with our clients to ensure that member data is anonymised or pseudonymised before it is shared with us so that a higher level of data protection is automatically built into our processes. However, even if such policies are put in place, there may still be instances when identifiable individual data is made available to us. Accordingly, we will maintain organisational and technological measures to protect any personal and sensitive personal data to which we have access.

For example, secure SharePoint share sites are set up where personal data is to be shared with multiple parties such as multiple trustees.

Third party processors and sub-processors are subject to data processor agreements and due diligence.

## **Retention schedule**

Our policy is to retain data only for as long as it is necessary to cover our and our clients' legal, professional and regulatory obligations. In many cases, data will be retained indefinitely as pension schemes are inherently long-term arrangements and questions/issues can arise many years after our appointment has ceased or the scheme has been wound up. Data in paper form is disposed of using our locked shredding bins which are emptied by our approved shredding contractor.

We engage specialist suppliers to safely remove all data and systems from redundant computer hardware and mobile phones. We are in the process of developing an enhanced policy to address GDPR requirements in respect of subject access requests.

## **General description of technical and organisational security measures**

## Information Security and Data Protection

The Law Debenture process personal data as per the Group Data Protection Policy and Group Information Security Policies which are available on request.

No data security incidents have been reported to the ICO by Law Debenture and we have not been the subject of any enforcement action or investigations by the ICO.

## Employment Contracts and Screening

All colleagues undergo pre-employment screening prior to joining which includes;

- Identity Check including right to work
- Adverse Financial History (Credit Check)
- Employment history
- Academic history
- Professional qualifications
- Criminal records (unspent convictions)
- Directorships
- Sanctions

We also contact previous employers for a professional reference.

Colleagues are rescreened on a periodic basis for the following;

- Adverse Financial History (Credit Check)
- Criminal records (unspent convictions)
- Directorships
- Sanctions

Each colleague is contractually required to comply with Law Debenture's security regulations including our Information Security Policy as a condition of employment in order to protect any information accessed as part of their work with Law Debenture. Misuse of IT systems and unauthorised use of personal data are both treated as gross misconduct offences which will involve instant dismissal.

## Training

All colleagues undergo risk and compliance training as part of onboarding and annual refresher training across a range topics including Data Protection and Information Security.

## Business Continuity

Law Debenture has in place a Business Continuity and Disaster Recovery (BCDR) Plan. Particular elements of these plans are subject to testing throughout the year. The BCDR plan aims to ensure that, in the event of a major incident, Law Debenture can continue to operate with the minimum of disruption to client and business activities.

Further details are available on request.

## External Accreditation

LDPTC has an AAF 02/07 Assurance Report in place for the year ended 31<sup>st</sup> March 2021. The reporting accountant is Crowe Clark Whitehill LLP.