

Dorset County Pension Fund
Dorset County Council as Administering Authority of the Local Government Pension
Scheme
(the "Scheme")

Data Protection Policy

1. Why we have this policy

As the Administering Authority of the Scheme, we need to Process Personal Data about people who are joining the Scheme, people who are members of the Scheme and (in some cases) people who used to be members of the Scheme. We also need to Process Personal Data about certain other people (for example, the spouses, civil partners, partners or dependants of members).

A lot of this information is collected by service providers on our behalf. Some of those service providers will be Data Controllers in their own right. However, for many purposes, we will be the Data Controller for the purposes of data protection law, and our service providers will be Processing Personal Data on our behalf. There will also be instances where we ourselves collect, receive, access or otherwise Process Personal Data.

Our contracts with service providers govern our relationship with them and the responsibilities those service providers have to us and to others.

The purpose of this policy is to set out how we comply with our obligations as Data Controllers when Processing Personal Data.

2. Why data protection is important

Protecting the confidentiality and integrity of Personal Data is a key responsibility.

The correct and lawful treatment of Personal Data supports our relationship with members. It also helps to ensure that the Personal Data we hold is accurate and up to date. This helps us to meet our duties as Administering Authority, including the key duty to pay the right benefit to the right person at the right time.

In addition, as Data Controller we are responsible for complying with data protection law and must be able to demonstrate compliance with it.

If we do not protect the confidentiality and integrity of Personal Data or otherwise fail to comply with (or demonstrate compliance with) data protection laws, this could result in any or all of the following:

- regulatory intervention;
- regulatory fine (up to a maximum of 20 million euros or 4% of annual worldwide turnover);
- claims for compensation from Data Subjects or bodies acting on their behalf; and

- reputational damage for us, the Scheme and the Employers.

3. **Who this policy applies to**

This policy applies to the Administering Authority, its staff and employees. It is an internal document.

4. **Key terms used in this policy**

In this policy:

Data Controller means anyone who, alone or jointly with others, decides the purposes and means of the Processing of Personal Data. We are a Data Controller. There can be more than one Data Controller in respect of the same Personal Data; some of our service providers may also be Data Controllers.

Data Processor means anyone who Processes Personal Data on behalf of a Data Controller. Some of our service providers are Data Processors.

Data Subject means an identified or identifiable natural person. In the context of the Scheme, this will usually be a person who is joining the Scheme, a person who is a member of the Scheme, a person who used to be a member of the Scheme, or someone else who is, might be, or used to be eligible to receive benefits from the Scheme (for example, a spouse, civil partner, partner or dependant).

Personal Data means any information (in any format, including in electronic or hard copy) relating to a Data Subject who is directly or indirectly identifiable from that information. Personal Data may or may not name the Data Subject. However, if, taken together with other information that the Scheme has, a Data Subject is identifiable, that information will be deemed to be Personal Data. It can be factual (for example, a name, address or date of birth), or a decision or opinion about a person, their actions and behaviour.

Special Categories of Personal Data means Personal Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of uniquely identifying an individual, data concerning health, sex life or sexual orientation. Special Categories of Personal Data are subject to additional protection, as set out in this policy.

Processing means any activity that involves use of Personal Data. It includes collecting, recording, holding, transferring, organising, amending, retrieving, viewing information on a screen, storing it on a back-up server or printing or carrying out any other operation on the data. Even the act of destroying or erasing data will be Processing. **Process, Processes and Processed** shall be construed accordingly.

5. **Data protection law**

When we Process Personal Data, we will comply with data protection law. By 'data protection law', we mean The General Data Protection Regulation ("**GDPR**") and the Data Protection Act 2018 when it comes into force.

The GDPR is based on a set of core principles. The principles are that Personal Data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and only Processed in ways that are consistent with those purposes;
- Adequate, relevant and limited to what is necessary for the purposes for which the Personal Data is being Processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which does not allow individuals to be identified for any longer than is necessary for the purposes for which the Personal Data is being Processed;
- Processed in a way that ensures the security, integrity and confidentiality of the Personal Data by using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage; and
- Not transferred to another country without appropriate safeguards being put in place.

We will comply with these principles and the requirements that support them.

6. **Lawful Processing**

We will Process Personal Data lawfully. By this we mean that we will only Process Personal Data on grounds that are permitted by data protection law.

For Personal Data other than Special Categories of Personal Data, the grounds permitted by data protection law include the grounds that the Processing is necessary for us to comply with our legal obligations to operate and administer the Scheme as the Administering Authority.

For Special Categories of Personal Data, the grounds permitted by data protection law include that the Data Subject has given their explicit consent to Processing for one or more specified purposes.

7. **Fairness and transparency**

We will Process Personal Data in a **fair** and **transparent** manner. To achieve this, we will provide Data Subjects with a detailed privacy notice that meets the requirements of data protection law.

If we (or one of our Data Processors) collect Personal Data directly from a Data Subject, we (or the Data Processor on our behalf) will provide them with the detailed privacy notice. The notice will be provided before or at the same time as we ask for the Personal Data. If the

Data Subject has already received a detailed privacy notice, we will remind them of it and where they can find it.

If we (or one of our Data Processors) receive Personal Data about Data Subjects from another source (for example, from an employer, or from a mortality screening or tracing agent), then we need to make sure that this is addressed in our privacy notice.

8. **Processing for specified, explicit and legitimate purposes**

We will only collect Personal Data for specified, explicit and legitimate purposes and we will not Process it in any way that is incompatible with those purposes.

The purposes for which we currently Process Personal Data are set out in the "**How do we use your personal data**" section of our separate privacy notice.

If we think we will need to Process Personal Data in a new way or for a new purpose (for example, if the Employers asks us to share some Personal Data), then we will take legal advice.

9. **Data that is adequate, relevant and non-excessive**

We will only collect Personal Data that is adequate, relevant and limited to what is necessary for the purposes for which the data is being Processed.

The types of Personal Data that we currently Process are listed in the "**Personal data we Process**" and "**What personal data do we collect about you and how?**" sections of our separate privacy notice.

We will seek legal advice if we are going to need to Process any other types of Personal Data.

10. **Data that is accurate and up to date**

We will make sure that the Personal Data we hold is accurate and, where necessary, kept up to date. We will also take steps to correct or delete data without delay when we find it is inaccurate.

For example:

- We have taken and continue to take steps to improve data quality, and common and conditional data scores, in response to the Pensions Regulator's guidance on record keeping.
- We are in the process of reconciling the Scheme's records of member's guaranteed minimum pensions with the records held by HMRC.

- We engage a mortality screening agent and undertake annual pensioner existence checks to reduce the risk of us continuing to contact, or pay benefits to, any pensioner member who has died.
- We engage a tracing agent to locate a current address for members where we do not hold one.
- We remind members on a regular basis of the importance of telling us if any of their personal details change and regularly invite members to submit an up to date expression of wishes form.
- We ensure that, following appropriate security checks, member records are updated to reflect any change or remove any inaccuracy that a member tells us about or of which we otherwise become aware.

11. **Data retention**

We will not keep Personal Data in an identifiable form for longer than is necessary for the purposes for which the data is Processed. We will also take all reasonable steps to securely destroy or erase any Personal Data which is no longer required.

The section of our privacy notice titled "**how long do we retain your personal data**" sets out how long the Scheme expects to retain Personal Data.

12. **Data security and accountability**

We will take appropriate technical and organisational measures against the unauthorised or unlawful Processing, and against the accidental loss, destruction or damage of Personal Data by us as the Administering Authority when we personally collect, access and otherwise Process Personal Data.

We will keep these measures under review to make sure they are appropriate given available technology, the costs of implementation and the nature, scope, context and purposes of Processing as well as the potential severity and likelihood of risk to a Data Subjects' rights and freedoms if certain measures are not in place or are inadequate.

We will also:

- ensure that we receive suitable training or undertake learning on our duties under data protection law; and
- ensure that our internal controls procedures and risk register reflect data protection and cyber security risk.

In terms of the Processing of Personal Data by service providers, we will ensure that:

- Our contracts with those service providers contain terms requiring them to implement and maintain appropriate technical and organisational measures to ensure that Personal Data is Processed and protected in accordance with data protection law (as

well as any other mandatory terms required by data protection law to be included in our contracts with them); and

- Where appropriate, we request and consider evidence of technical and organisation measures to ensure that Personal Data is Processed and protected in accordance with data protection law on an annual basis and otherwise as a part of any tendering or adviser review exercise; for example, we might ask whether they have any relevant certifications or accreditations (such as ISO 27001).

13. Transferring Personal Data to another country

We will only transfer or agree to the transfer of Personal Data to a country outside of the United Kingdom and the European Economic Area if we can satisfy the requirements of data protection law, which (broadly) require us to ensure an adequate level of protection for that Personal Data.

There are several mechanisms for ensuring an adequate level of protection; including where certain countries have been deemed "adequate" by the European Commission or where we transfer Personal Data outside the United Kingdom and the European Economic Area on the basis of the standard data protection clauses approved by the European Commission (for example, where we incorporate those clauses into our contracts with service providers based outside the United Kingdom and the European Economic Area).

We will comply with this when we Process Personal Data as Administering Authority.

Our contracts with Data Processors will require them to obtain our consent before making a transfer to a country outside of the EEA and, before we give that consent, we will seek legal advice as to whether we can give it (that is, whether we can satisfy the requirements of data protection law in respect of that transfer¹).

14. Personal data breach

Except in cases where a personal data breach (that is, any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data) is unlikely to result in a risk to the rights and freedoms of the Data Subjects affected by it, we will report any personal data breach to the Information Commissioner's office without undue delay and, where possible, within 72 hours of becoming aware of it. If we do not report the breach within 72 hours, we will provide reasons for the delay when we submit the report.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will also report the breach to the Data Subjects whose Personal Data has been affected without undue delay.

¹ This to be addressed as part of the review of contracts for GDPR compliance (not included in Pension Secure) if instructed.

Our Data Processors have a duty to report any personal data breach of which they become aware to us without undue delay, so that we can consider the need to report it to the Information Commissioners Office.

If we identify, or are informed that there has been a personal data breach, we will inform the point of contact named in paragraph 17 below, and seek legal advice immediately.

15. **Data subject's rights**

Data Subjects are afforded various rights in relation to their Personal Data; specifically, Data Subjects can:

- Withdraw consent to Processing (where we are relying upon consent);
- Ask for access to and information about the Personal Data that we hold (more widely known as a Data Subject access request);
- Ask us to correct (rectify) inaccurate data and complete incomplete Personal Data;
- Ask us to erase Personal Data (more widely known as the 'right to be forgotten');
- Restrict Processing; and
- Ask for their Personal data to be transferred to a third party in a structured, commonly used and machine readable format.

Those rights are not absolute; some only apply in certain circumstances and even where they do apply, there may be exceptions to them.

If the Administering Authority receives a request of this kind (or any request in relation to Personal Data), or is made aware of such a request by a Data Processor, we will refer it to the point of contact named in section 17 of this policy and (where required) seek legal advice.

16. **Other matters**

We are aware that, subject to specific exceptions, Data Subjects have the right not to be subject to a decision based solely on automated Processing, including profiling, which will have legal consequences or otherwise significantly affect them. We will seek legal advice if we think this situation may arise in relation to Processing carried out by us or at our request.

We are also aware that, where a type of Processing (in particular if it uses a new technology), taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of Data Subjects, we must carry out a privacy impact assessment before we carry out that Processing. The privacy impact assessment will consider the impact of the planned Processing on the protection of the Personal Data. It may be necessary to carry out a privacy impact assessment if, for example:

- we are considering changing a service provider (for example, changing insurers or scheme administrators with the result that large volumes of Personal Data will need to be transferred);
- we, or one of our service providers, is considering setting up a member portal (or similar) for Data Subjects to access information about their pensions; or
- We are considering a process that involves automated Processing or profiling as discussed immediately above, or considering Processing Special Categories of Personal Data on a large scale.

Again, we will seek legal advice if we think this situation may arise.

17. **Point of contact**

Any questions or complaints about our collection, use or other Processing of personal data should be referred to the Systems Manager at Dorset County Pension Fund. However, they are not a data protection officer.

Dorset County Council has a Data Protection Officer to assist with all queries regarding our processing of personal data, who may be contacted if you wish to exercise any of your rights; Gary McCann who can be contacted at gary.mccann@dorsetcc.gov.uk

We will investigate and attempt to resolve any such complaint or dispute regarding the use or disclosure of your personal data.

You may also make a complaint to the UK Information Commissioner's Office (<https://ico.org.uk/>), the UK's data protection regulator, or a different data protection regulator in the country where you usually live or work, or where an alleged infringement has taken place. Alternatively, you may seek a remedy through the courts if you believe your rights have been breached.

18. **How often will this policy be reviewed?**

We will review this policy annually, or in the event of any key changes to data protection law.

Signed on behalf of the Administering Authority:



Karen Gibson

Interim Pensions Manager

Policy approved by the Administering Authority:

Next review date: