Dorset County Pension Fund
Actions to be taken for GDPR compliance

	Action	Additional Information	Target Met?	Date Target Met	Notes
Section A: Legal Basis for Processing					
A1	The Administering Authority should document in a data protection policy its legal basis under the GDPR for Processing Personal Data (other than Special Categories of Personal Data) and for Processing Special Categories of Personal Data.	For Processing Personal Data (other than Special Categories of Personal Data) the legal basis is to comply with its legal obligation to administer the LGPS to which the Administering Authority as a Data Controller is subject. For Processing Special Categories of Personal Data there are two legal bases. The first is the same as for Processing Personal Data (other than Special Categories of Personal Data) and is to comply with its legal obligation to administer the LGPS to which the Administering Authority as a Data Controller is subject, and the Administering Authority will also need to rely on a second ground for Processing this type of data by relying on explicit consent.	Target Met		The DCPF has a Data Protection Policy in place as of 25/05/2018
A2	The Administering Authority should agree new member consent wording for the purposes of Processing of Special Categories of Personal Data for use in member event forms such as expression of wish forms and application for ill-health early retirement.	Requests for consent must be clearly distinguishable from other matters, clear and easy to understand, accompanied by an explanation that the Data Subject has the right to withdraw their consent at any time. It must be as easy for the Data Subject to withdraw their consent as it is to give it, and consent must be freely given, specific, informed and unambiguous.	Not Met		
Section B: Providing information to Data Subjects					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
B1	The Administering Authority needs to prepare a bespoke privacy notice containing all of the information required by the GDPR.	To include information about circumstances in which the Administering Authority receives Personal Data from third parties such as the Employer or a tracing agent.	Target Met	25/05/2018	The Privacy notice is published on the DCPF website. https://www.yourpension.org.uk/Dorset/Accessibility/Privacy-and-Cookie-Policy.aspx
B2	The Administering Authority should amend all forms and other communications asking for Personal Data which it (or the Service Providers on their behalf) sends to Scheme members or beneficiaries.	To include a statement that signposts the member / beneficiary to the central privacy notice	On-going		
Section C: Purpose of Processing Personal Data					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
C1	The Administering Authority should ensure that its new privacy notice clearly states that Personal Data is being collected and Processed by (or on behalf of) The Administering Authority for the legitimate, specified and explicit purposes of operating the Scheme to ensure that the correct benefits are paid to Scheme members and beneficiaries at the correct time.	Must also specify all other purposes for which it is collected and processed. (For example, complying with laws and regulations that apply to the Scheme).	Target Met	25/05/2018	The Privacy notice is published on the DCPF website. https://www.yourpension.org.uk/Dorset/Accessibility/Privacy-and-Cookie-Policy.aspx
Section D: Quality of Personal Data					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
D1	The Administering Authority should continue to contact Scheme members on a regular basis, we suggest annually, inviting them to submit an up to date Expression of Wish form.	Scheme members should also be regularly reminded of the need to contact the Administering Authority if any of their personal details change	On-going		This will be done through the Annual Benefit Illustration each year, and upon the award of benefits, for example, at retirement.
D2	The Administering Authority should continue to try to improve its common and conditional data scores in line with the Pension Regulator's guidance on record keeping.	It should also continue to conduct pensioner existence checks and to instruct a tracing agent to locate scheme members for whom there is no current address.	Target Met	Continuous	The Fund conducts monthly mortality checks on its UK pensioners, and tri-annual existence checks on pensioners living abroad.
D3	The Administering Authority should document in an internal data protection policy details of its approach to data quality	This should be separate from Employer's own data protection policy.	Target Met		DCPF has completed its Data Protection Policy
Section E: Storage and Retention of Personal Data					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
E1	The Administering Authority should consider introducing a basic data retention policy, with agreed intervals for reviewing the data they store and agreed procedures for securely destroying records that are no longer needed.		Not Met		Some further advice and clarity will be needed.
E2	In terms of Personal Data stored by the Service Providers for and on behalf of the Administering Authority, the Administering Authority will need to agree with the relevant Service Providers how long Personal Data should be retained by the Service Provider.	This decision should be reflected in the data retention policy (E1) and in the Administering Authority's new privacy notice.	Not Met		
E3	The GDPR requires the Administering Authority to include certain provisions in its contracts with Service Providers that are Data Processors including an obligation to delete or return all Personal Data after the end of the provision of the services.	If the administering authority agrees with the Service Provider that the Service Provider may keep any Personal Data after this time, the Service Provider is likely to do so for its own purposes, as Data Controller (and not on the Administering Authority's behalf).	Partially Met		Contracts with service providers are being reviewed.
Section F: Security of Personal Data					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
F1	The Administering Authority needs to assess existing security measures compliance with the GDPR. Assessment of existing measures and choosing what new measures to implement will involve a risk assessment based on the GDPR threshold test for assessment of appropriate security. A higher standard of security should apply to Special Categories of Data, such as medical reports received from medical practitioners or other items relating to ill health retirement.	In particular, we suggest password protecting / encrypting documents containing Personal Data and use of pseudonymisation and / or redaction as a technique for minimising the risk to Data Subjects	Not Met		
F2	The Administering Authority should also try to circulate and access Personal Data by a secure upload to an information portal, with a link included in any relevant emails, rather than circulating Personal Data by email at all.		On-going		This measure is already part of our standard data protection processes.
F3	The Administering Authority should ensure access to Personal Data is restricted to those who need access to it.		Target Met		Processes are already in place to ensure access to data is only granted to current staff, access is further controlled by position based access levels incorporated into our systems.
F4	To reduce the risk of a security breach, the Administering Authority should delete or securely destroy Personal Data when it is no longer needed and not keep unnecessary copies of Personal Data.		Not Met		A review of our processes will be needed to catagorise data to ensure that, where appropriate data can be kept, or where personal data should be destroyed. This will form part of our data retention policy.

F5	The Administering Authority should put in place an internal Data Protection policy specific to the Fund, documenting what measures the Administering Authority has in place to ensure and to be able to demonstrate compliance with the GDPR.	It should cover, in broad terms, the topics highlighted in this report.	Target Met		The DCPF has a data protection policy in place.
F6	The Administering Authority should put in place a risk register including a section on compliance with the GDPR		Partially Met		A risk register has been completed and will be passed for approval by the Local Pensions Bpard and PFC in September 2018.
Section G: Privacy by Design and Privacy Impact Assessments					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
G1	The Administering Authority should carry out a PIA to assess the data protection and privacy risk of any new high risk Processing activities such as when considering: A) Changing a service provider (for example, changing insurers or scheme administrators with the result that large volumes of data will need to be transferred); B) Setting up a member portal (or similar) for Data Subjects to access information about their Pensions, and; C) A process that involves automated Processing or profiling or considering Processing Special Categories of Personal Data on a large scale.	The Fund should keep such PIA under continuous review and assessment as part of the Administering Authority's accountability obligations (it may be that the assessment does not change but it should be subject to a review to establish that this is the case).	Not Met		
Section H: Record Keeping and Accountability					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
H1	The administering Authority needs to prepare a record of the Data Processing activities that it and Service Providers who are Data Processors undertake.	This should name the Administering Authority as a Data Controller, identify the operation of the Scheme as the purpose of the Processing, describe the Scheme members and beneficiaries (including former members if relevant) as the categories of Data Subjects, and, as good practice for accountability, describe the categories of people from whom the Administering Authority received Personal Data (including members, the Employer and third part providers). It should also list the following: the categories of Personal Data processed; the categories of recipients of Personal Data; the circumstances if any in which Personal Data is transferred to a third country (for example by sending emails or other correspondence containing data to individuals based outside of the EU, or overseas processors accessing data), the periods for which Personal Data is retained (where possible) and a general description of technical and organisational security measures taken by the Administering Authority (where possible).	Not Met		
Section I: Breach Notification					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
I1	The Administering Authority should establish a data breach management process documented in the Data Protection Policy to ensure they will be able to comply with the duty to report any data breach of which it becomes aware, including a breach reported to it by any of the Service Providers, without undue delay, and within 72 hours		Partially Met		Staff will be using the policy and process provided by Dorset County Council which is already in place. Further guidance for staff to enable them to easily and swiftly recognise a breach will additionally be provided to cover our specific service area.
Section J: Sharing of Personal Data					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
J1	The Administering Authority should prepare new GDPR-compliant data Processing clauses / an addendum and work to have the new GDPR-compliant clauses included in their contracts with each of the Service Providers as soon as possible, and ensure that these only permit sub-Processing with the Administering Authority's consent (which may be a specific or general authorisation) and conditional on compliance with the Administering Authority's GDPR addendum or any addendum suggested by the Service Provider(if acceptable).		On-going		A record of Service Providers has been established to enable contracts to be reviewed. In most cases contract ammendments are already in place
J2	The Administering Authority should ensure it has controls and processes in place to undertake due diligence on any new third parties who may collect and use Personal Data as Data Processors (and for putting in place appropriate contractual arrangements with those third parties).	This is particularly important when engaging a new portal service provider as online processing is higher risk from a security perspective and portal providers sometimes offer inadequate protections for Personal Data (which should be negotiated). It is best practice to undertake regular reviews of the technical and organisational security measures Service Providers have in place. (Most should have a policy or factsheet)	Not Met		
J3	The Administering Authority should consider establishing a protocol for sharing Special Categories of Data (e.g. ill health Data) to ensure GDPR-compliant data sharing		Not Met		
Section K: Transfers of Data Outside the EEA					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
K1	The Administering Authority should include a provision in all contracts with all Service Providers confirming that the provider (as Data Processor) may only transfer Personal Data overseas with the documented (written) consent of the Administering Authority or in particular prescribed circumstances where the Service Provider contractually commits to compliance with the GDPR for the transfer.	Where a transfer is to be made, the Administering Authority will need to put in place model contracts (or require a Service Provider to put them in place on the Administering Authority's behalf) or identify another appropriate data transfer solution to ensure the transfer is compliant with the GDPR.	Not Met		
K2	The Administering Authority should establish a process to determine whether a potential provider is based outside of the EEA and will be receiving Personal Data from the Administering Authority.	The Administering Authority should also ensure that pre-contract due diligence looks not just at the immediate provider, but also their own provider chain.	Not Met		
K3	The Administering Authority should consider establishing a protocol for sharing Special Categories of Data (e.g. ill health Data) to ensure GDPR-compliant data sharing.		Not Met		
Section L: Data Subject's Rights					
	Action	**Additional Information**	**Target Met?**	**Date Target Met**	**Notes**
L1	The Administering Authority needs to decide how it would respond to a Data Subject request and document this in its internal Data Protection Policy.	It may be that the response will be to immediately refer the request to the person responsible for data protection, who will then seek legal advice.	Not Met		
Section M: Data Protection Officer					

	Action	Additional Information	Target Met?	Date Target Met	Notes
M1	As a public authority, the Administering Authority will be required to a appoint a DPO to assist it as Data Controller to monitor internal compliance with the GDPR.	The Administering Authority should be able to continue to share the DPO appointed by Dorset County Council assuming that the DPO is a standalone function and is not involved in or response for Processing any Personal Data of the Administering Authority or Dorset County Council. This is in order to avoid any conflict of interest between the role of the DPO and the functions of the Administering Authority and Dorset County Council.	Target Met		Dorset CC has fulfilled this obligation.
M2	The Administering Authority should record the decision to appoint a DPO together with a (brief) explanation of that decision in its internal data protection policy.		Target Met		This is part of the DCPF Data Protection Policy.
M3	The Administering Authority should ensure that there is always an individual who is internally responsible for GDPR compliance	This person must not be named as DPO, or they will become subject to the full range of responsibilities imposed on DPOs by the GDPR	Partially Met		This person will be the Systems Manager. A review of the relevant Job Description needs to be completed in order to comply.