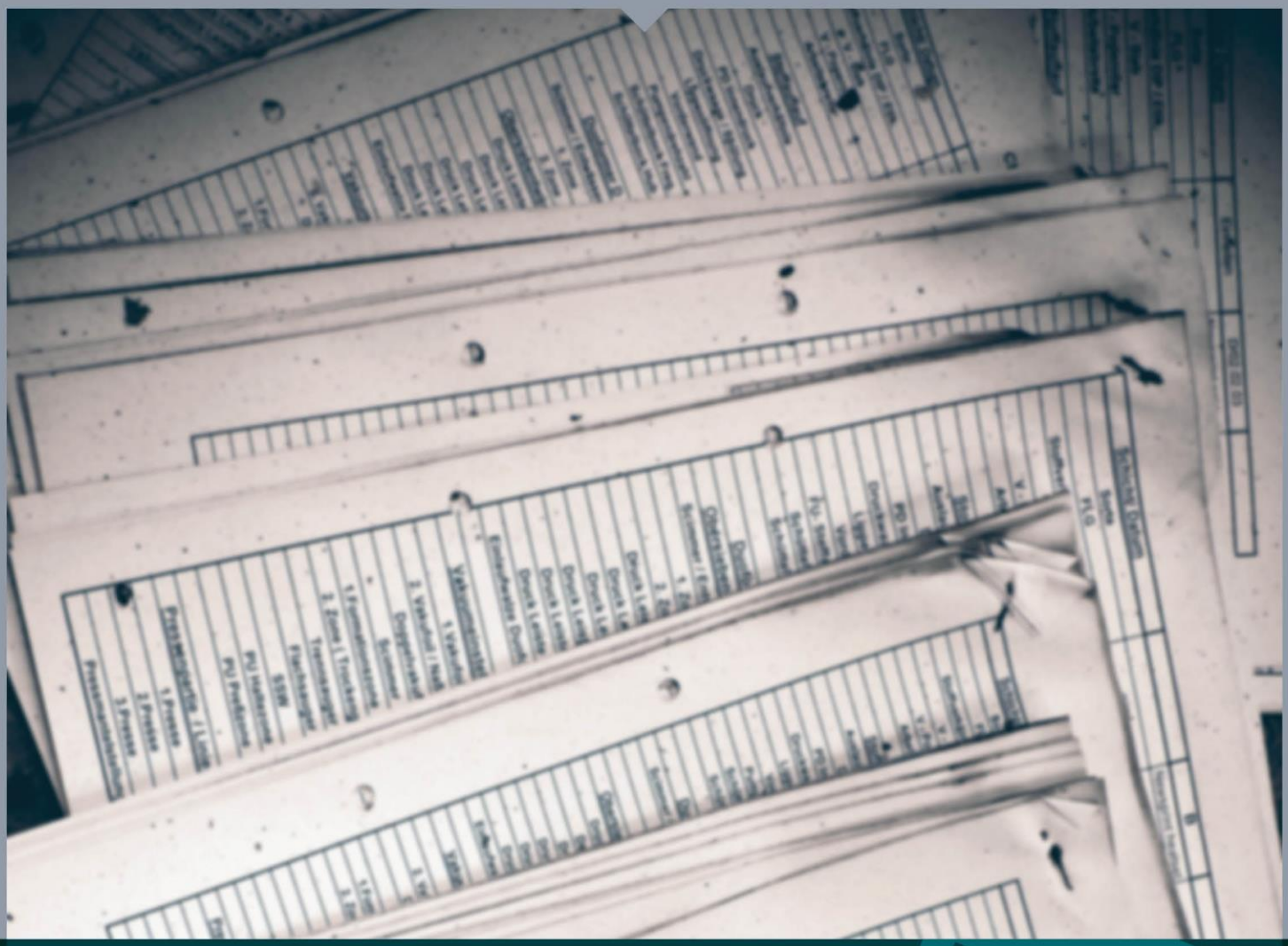
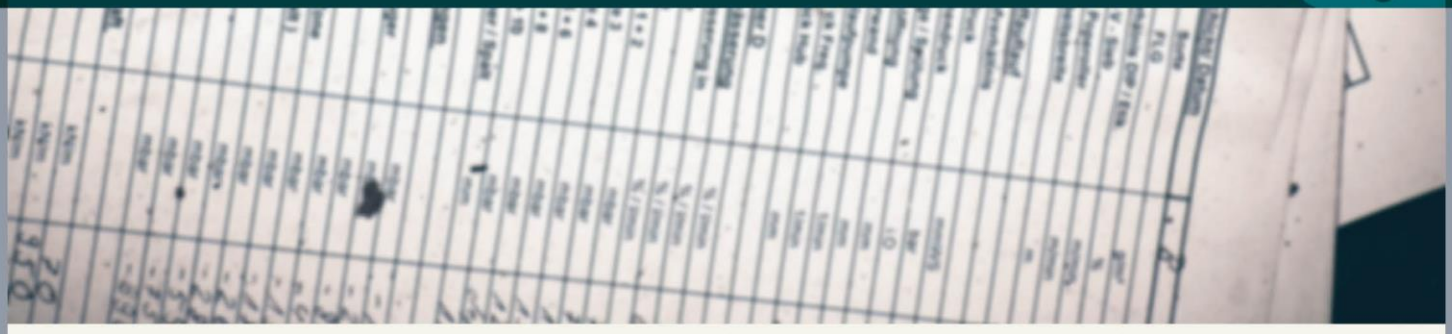


WRIGLEYS
— SOLICITORS —

GDPR MAY 2018

Pension Scheme Trustees: How to Comply with the General Data Protection Regulation in 10 Steps



HR response from WRIGLEYS

The Legal 500 United Kingdom Top Tier 2016

Top Ranked UK Chambers 2017 Wrigleys Solicitors LLP

Lexcel Practice Management Standard Law Society Accredited

Working to become Dementia Friendly

We are a Living Wage Employer

Contents

This guide is for guidance only and does not constitute definitive advice.

Introduction

The General Data Protection Regulation (**GDPR**) comes into force in the UK on 25 May 2018, bringing with it a tougher data protection regime.

Although trustees may not often be in physical possession of a scheme member's personal data, as legal administrator of the pension scheme, they nevertheless control the processing of the personal data of hundreds (if not thousands) of scheme members and beneficiaries through their agreements with third party processors, most notably, the scheme administrator. As controllers under the GDPR, therefore, trustees will be responsible for both their own and their processors' compliance with the six data protection principles governing the processing of personal data. These principles are similar to those found in the Data Protection Act 1998, although one significant addition under the GDPR is a new accountability principle which requires trustees to show how they comply with the six principles.

This guide provides an overview of the main requirements of the GDPR and describes the ten steps that trustees should be taking now to achieve compliance ahead of 25 May 2018. In light of the accountability principle, we also highlight the documents that trustees will need to prepare in order to evidence their compliance with the new regime. A useful key documents table with drafting notes and a suggested timeframe for completion is included in the appendix.

Note on Brexit: At the time of writing it is intended that the Data Protection Bill will replace the Data Protection Act 1998 to provide a comprehensive legal framework for data protection in the UK supplemented by the GDPR until the UK leaves the EU. When the UK leaves the EU, the GDPR will be incorporated into UK domestic law under the European Union (Withdrawal) Bill currently before Parliament.

What should trustees be doing now?

Before embarking on the 10 steps described in this guide, trustees should:

1. Add data protection / GDPR as a standing item on the agenda for trustee meetings.

   Initially the agenda item will give trustees the opportunity to agree a strategy for achieving compliance with the GDPR, to monitor progress against that strategy and any agreed timescales, and to approve data protection policies, privacy notices and other documents (as appropriate). After 25 May 2018 trustees should retain data protection as an item on the agenda to monitor ongoing compliance with the regime, to discuss any personal data breaches that may occur, and to review and update periodically the data protection documents.

2. Form a data protection trustee sub-committee / allocate responsibility for data protection to an existing trustee sub-committee or nominated trustees.

   Implementing the steps identified below will require regular input from the trustee board, and progress will be quicker if day to day decision making is delegated to a sub-committee/nominated trustees that is able to meet at short notice.

3. Prepare a timeline for taking key decisions and drafting / negotiating / approving the various documents identified in the documents table. Where appropriate, make provision in the timetable for documents to be approved at a full trustee meeting.

   Key to complying with the GDPR is identifying personal data and understanding how it is processed. From this starting point, decisions can be taken regarding the legal basis for processing, the requirement (if any) for consent, the measures which need to be taken to keep personal data secure, and the content of privacy notices, data protection policies etc. The step which kick starts all others is the completion of a data protection questionnaire / data mapping exercise so this should be the priority in any timeline.

4. Arrange trustee training on data protection for the full trustee board to equip trustees with the knowledge and understanding necessary to bring the pension scheme into compliance with the GDPR. Training should cover the key concepts underpinning the new regime including the accountability principle and data protection by design and by default, as well as providing information about the penalties for non-compliance.

Step one: carry out an audit of the scheme's personal data

In order to understand how the GDPR applies to them, trustees will first need to identify:

- the personal data held by and on behalf of trustees, and
- the types of processing carried out in relation to that personal data.

This exercise is sometimes referred to as data mapping and gives trustees a useful overview of how personal data is collected and used for the purposes of the scheme. From this vantage point, trustees will be in the best position to consider, for example, which lawful basis for processing applies (step three), and to identify where member consent is required for the processing of certain data (step five).

ACTION: trustees and scheme advisers should complete **the data protection questionnaire** prepared by Wrigleys (see Appendix 1 to this guide). Scheme advisers for these purposes include the Scheme's administrators, legal advisers, investment consultants and the scheme actuary. If an adviser issues a more generic response to the questionnaire (some advisers may do this where they have received a high volume of questionnaires from clients), trustees should check the information provided carefully to make sure it is sufficient for the purposes of completing the steps identified below. For example, information gathered from the questionnaire will be used to draft privacy statements (step four) and so it is important that a complete set of information is obtained from advisers.

Step two: identify gaps in compliance and fill them!

Pursuant to the provisions of the GDPR, trustees are responsible for and must be able to demonstrate compliance with six principles relating to the processing of personal data.

The principles provide that personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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; and
- 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.

ACTION: **the data protection questionnaire** is designed to identify personal data held by the trustees and their advisers, and the extent to which personal data is collected / processed / stored in accordance with the six data protection principles. Where a response to the questionnaire reveals a gap in compliance, the trustees will need to address it. Compliance with all six data protection principles should be recorded in a trustee **data protection policy** which is subject to periodic review and updating. The data protection policy should take account of any **codes of conduct** issued by the Information Commissioner's Office (**ICO**); adherence to which may demonstrate compliance with one or more principles.

Step three: identify the trustees' lawful basis for processing personal data

Personal data must be processed "lawfully". This means the processing must fall within one of the prescribed legal bases under the GDPR, including where processing is carried out with the consent of the data subject.

There are likely to be significant practical difficulties in obtaining each and every member's written consent to processing. Also, consent can be withdrawn at any time under the new "right to be forgotten". Accordingly, trustees may wish to explore alternative lawful bases for processing including "the pursuit of legitimate interests". This basis applies where processing is necessary for the purposes of the legitimate interests pursued by the controller.

Given that the processing of personal data is integral to the day-to-day administration of pension schemes, we anticipate trustees will be able to rely on this lawful basis in most cases. However, given the significant fines that can be imposed in relation to any breaches of the GDPR, we strongly advise trustees to take legal advice on this point.

ACTION: Trustees should analyse the categories of personal data and processing activities revealed by the responses to the questionnaire and decide, in each case, the legal basis for processing the personal data (taking legal advice as appropriate). The legal basis or bases should be recorded in the **data protection policy** and members should be informed in an updated **privacy notice** (required by the GDPR).

Step four: update privacy notices

The GDPR requires trustees to provide members (known as data subjects under the GDPR) with certain prescribed information at the point at which personal data is obtained. In the trustees' case, we recommend that updated **privacy notices** (covering all the items required by the Regulation) are issued to members no later than 25 May 2018.

ACTION: Draft and issue **privacy notices** to members (and anyone else in relation to whom the trustees or advisers hold personal data) covering:

- the identity and the contact details of the controller (the trustees for these purposes),
- the contact details of the data protection officer (if applicable),
- the purposes of the processing for which the personal data are intended as well as the legal basis for processing,
- where the processing is based on legitimate interests, the legitimate interests pursued by the controller,
- the recipients of the personal data, if any,
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation,
- the period for which personal data will be stored, or if that is not possible, the criteria used to determine that period,
- the existence of the right to request from the controller access to and rectification or erasure of personal data,
- where lawful processing is based on consent, the right to withdraw consent at any time,
- the right to lodge a complaint with a supervisory authority,
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data, and
- the existence of automated decision-making.

Information gathered from responses to the **data protection questionnaire / the data mapping exercise** will help trustees to draft the **privacy notices**.

Step five: obtain consent for the processing of special categories of personal data

The processing of special categories of personal data can only be carried out with the consent of the data subject. Special categories of personal data processed by pension schemes include data concerning health and/or a person's sexual orientation. Trustees should ensure they have appropriate consent before processing such data (which is likely to arise in the context of ill health early retirement applications and / the distribution of death benefits (where the member was married or in a civil partnership).

ACTION: the **data protection questionnaire** should identify any special categories of personal data currently held by or on behalf of the trustees. In relation to each item of data, the trustees should decide whether to destroy / return / retain it. If it is retained, the trustees must obtain the written consent of the data subject to the processing of that personal data.

Trustees should further liaise with advisers (1) to determine at what point in the "membership cycle" these special categories of personal data could be obtained, and (2) to put in place processes to ensure consent is obtained at an appropriate stage in accordance with the requirements of the GDPR. This process should be recorded in the **data protection policy**. The **ill health early retirement application form** should be updated to include a consent provision whereby the applicant consents to the processing of his sensitive personal data. N.B. Consent has its own definition under the GDPR (see the Glossary of key terms included at the end of this document) and therefore trustees should ensure any consent given by a member GDPR compliant (taking legal advice as appropriate).

Step six: know your members' rights

Data subjects (the members and beneficiaries in the context of a pension scheme) have various rights in connection with their personal data including a right of access and a right to erasure. Some of these rights must be communicated to data subjects and, where they are enforced by the data subject, certain time limits apply.

ACTION: trustees should arrange trustee training on the GDPR to learn about members' rights and the trustees' role in relation to the enforcement of those rights. Further, information about data subjects' rights (and how to enforce them) should be included in the **privacy notice**. **Agreements with advisers** should be amended where necessary to require the adviser to notify the trustees where a data subject seeks to enforce one of his rights under the GDPR and to require the advisers to assist the trustees in responding to any request of the data subject. The **data protection policy** should set out a process for dealing with a request from a data subject to enforce any of his rights under the GDPR including a timetable for responding / taking action, where appropriate.

Step seven: update adviser contracts to reflect GDPR requirements

Where personal data is processed by a third party (as processors) on behalf of the trustees (as controllers), the trustees must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Furthermore, processing must be governed by a legally binding agreement that sets out certain prescribed matters.

ACTION: the trustees will need to enter into **data protection agreements** with all advisers that process personal data relating to the scheme (or amend **existing agreements with advisers** to incorporate new provisions on data processing). These agreements should require, amongst other things, the processor:

- to process data only on the instructions of the trustees,
- to ensure confidentiality,
- to assist with subject access requests,
- to assist the trustees in meeting certain compliance obligations including safeguarding the security of personal data, and notifying and communicating personal data breaches,
- to pass on obligations to delegates, and
- to delete or return data following the termination of services.

The GDPR notes the possibility of a supervisory authority adopting **standard contractual clauses** covering the prescribed items. At the time of writing, the ICO had just opened a consultation on draft guidance on contracts and liabilities between controllers and processors under the GDPR. The guidance explains to controllers, what they must include in contracts and sets out what responsibilities and liabilities processors have under the GDPR. The consultation closes on 10 October 2017.

Step eight: prepare a written record of processing

As part of the new principle of accountability, trustees are required to maintain a **written record of the processing activities** under their responsibility. The **written record of processing activities** should be available to ICO on request.

ACTION: trustees will need to prepare and maintain a **written record of processing activities**. The record should contain all of the following information:

- the name and contact details of the controller (trustees);
- the purposes of the processing;
- a description of the categories of data subjects and of categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed;
- where applicable, transfers of personal data to a third country; and
- where possible, the envisaged time limits for erasure of the different categories of data.

Responses to the **data protection questionnaire** should help the trustees to complete their **written record of processing activities**.

Step nine: implement technical and organisational measures to ensure the security of personal data

Trustees (as controllers) and advisers (as processors) must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including where appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

ACTION: the trustees will need to work out (from their own responses to the **data protection questionnaire**) what personal data they actually hold and in what format. They will then need (1) to decide what technical and organisational measures to take in order to protect data and ensure the security of processing, (2) to **implement appropriate technical and organisational measures**, and (3) to record those measures in a **data protection policy** (and keep them under periodic review). The trustees must also incorporate appropriate provisions in bespoke **data protection agreements** or their **existing agreements with advisers** (as applicable) to ensure the processor is also obliged to implement appropriate technical and organisational measures to protect members' personal data against accidental loss, destruction etc.

Step ten: prepare a data breach reporting protocol

The GDPR requires trustees (as controllers) to notify a personal data breach to the ICO without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. A "personal data breach" is a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the trustees should communicate the personal data breach to the data subject without undue delay.

ACTION: the trustees should agree a process and timetable for assessing and reporting (where necessary) personal data breaches and record these in their **data protection policy**. The trustees should also incorporate appropriate provisions in bespoke **data protection agreements** or **existing agreements with advisers** requiring their processors (scheme administrators and other advisers) to notify any personal data breaches to the trustees without delay.

Glossary of key terms

Consent	of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. ***Wrigleys' comment: this is a more rigorous definition than under the Data Protection Act 1998. Consent for the purposes of the GDPR requires some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and there must be a simple way for people to withdraw consent.***
Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determine the purposes and means of the processing of personal data. ***Wrigleys' comment: in the context of pension schemes, trustees and employers will be controllers. Under the terms of the GDPR, controllers are responsible for ensuring that personal data is processed in accordance with the six data protection principles regardless of whether or not the controllers physically process data. Where the processing is undertaken by a third party, the onus is on the controller to ensure that the processor complies with the requirements of the GDPR.***
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. ***Examples of personal data would include a person's name, address, national insurance number and email address but could also capture data such as salary and date of birth where it is possible to identify an individual from that data***

	or combination of data.
Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. ***Wrigleys' comment: in the context of pension schemes, scheme administrators will be processors but other advisers, including the scheme actuary and legal adviser, may also process data.***
Profiling	means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. ***Wrigleys' comment: additional obligations apply in relation to profiling. Trustees must ascertain whether any profiling occurs in relation to scheme members and be aware of any profiling which may occur in the future (for example, in connection with liability management exercises).***
Pseudonymisation	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person. ***Wrigleys' comment: the pseudonymisation of data would be***

	an appropriate technical and organisational measure to take in order to eliminate the security risks associated with the sharing of an individual member's data between trustees and advisers in connection with, for example, an ill health early retirement application. An application could be considered on a no names basis (with the relevant supporting documentation being provided on an anonymous basis by the administrator) at trustee level where the only decision to be taken is whether the individual meets the ill health criteria under the scheme's rules.
Technical and organisational measures	***Wrigleys' comment: There is no definition provided under the GDPR; however, Article 32 requires both the controller and processor to implement technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:*** • ***the pseudonymisation and encryption of personal data;*** • ***the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*** • ***the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and*** • ***a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.***

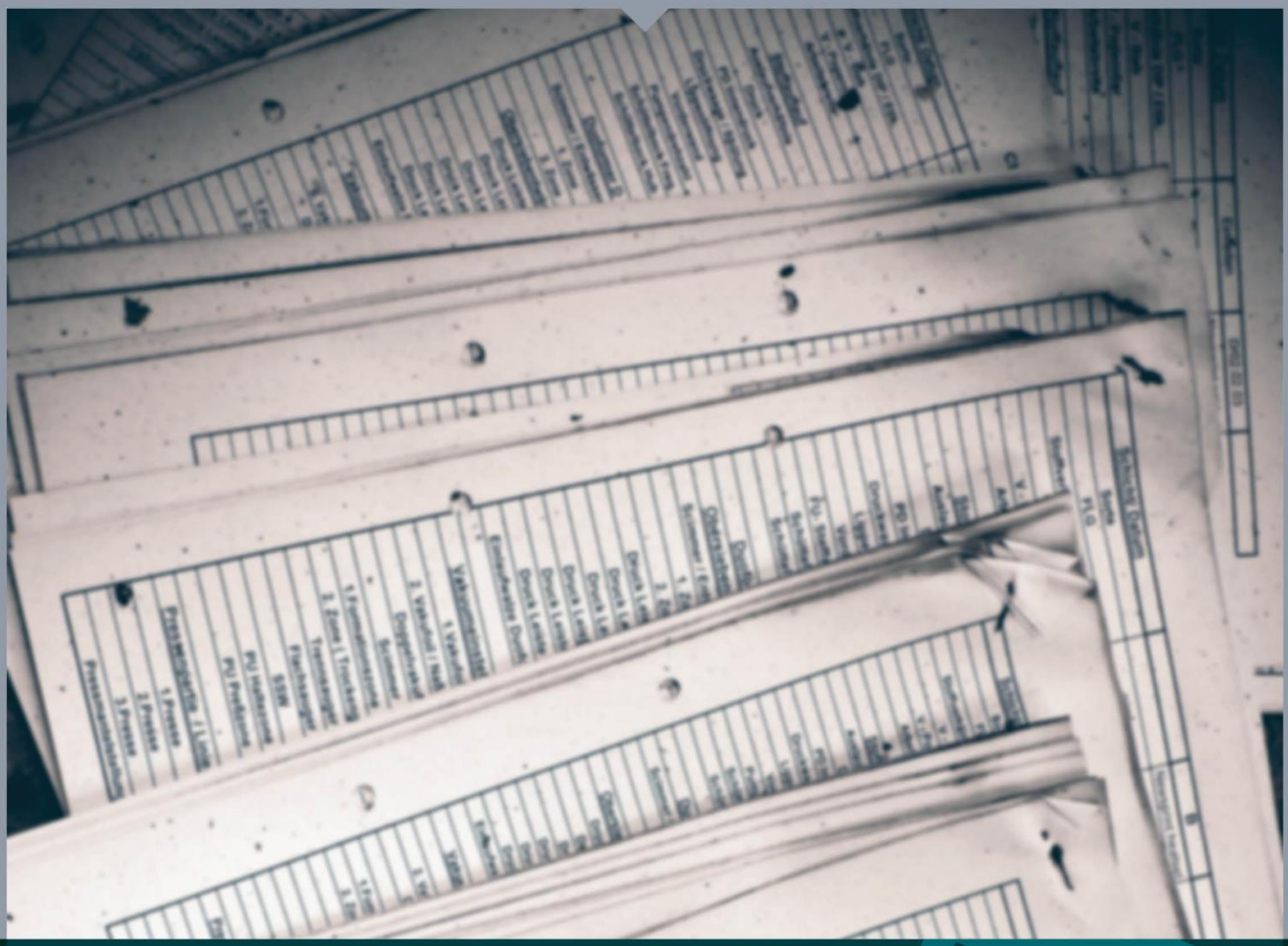
Documents table

Document name	Purpose	Who will prepare?	Relevant reference materials?	Drafting period
The data protection questionnaire	The questionnaire will help trustees to identify the personal data held by the scheme and the processing that applies to it. From this starting point, the trustees will be able to determine the extent to which personal data is currently processed in compliance with the six data protection principles and address any gaps in compliance.	We have prepared a questionnaire template which can be adapted for use by the trustees (see appendix).	n/a	The questionnaire should be completed by trustees, the scheme administrator, legal adviser, scheme actuary, investment consultant and any other relevant scheme adviser/third party as soon as possible. The results should then be analysed by the trustees (with assistance from their legal advisers) for the purposes of identifying any gaps in compliance and preparing an action plan to address those gaps.
Data protection policy	The data protection policy: • documents the steps being	Trustees' legal advisers to prepare or review (as	Current data protection policy (if available), any data protection policy	To commence after the responses to the questionnaire have been

Document name	Purpose	Who will prepare?	Relevant reference materials?	Drafting period
	taken by the trustees to comply with the GDPR (in accordance with the new accountability principle), • sets out the technical and organisational measures adopted by the trustees to manage security risks relating to personal data, • sets out the process to apply in certain circumstances, including where there is a personal data breach or where a data subject exercises a right in relation to his or her personal data.	appropriate)	guidance issued by ICO or TPR.	analysed.
Privacy notice	The GDPR requires trustees to provide data subjects with certain prescribed information – the privacy notice serves this purpose. Existing privacy notices are unlikely to meet all of the mandatory requirements of the GDPR, so we expect existing	Trustees' legal advisers to prepare or review (as appropriate)	Current privacy notice, ICO guidance.	Quarter 1 2018.

Document name	Purpose	Who will prepare?	Relevant reference materials?	Drafting period
	notices to be substantially reworked and reissued.			
Written consents	The processing of certain types of personal data can only be done with the consent of the data subject. Consent must be in writing and cannot be inferred / implied. Responses to the data protection questionnaire will help identify the circumstances in which special categories of personal data are collected. Processes should be reviewed / updated to build in a requirement for consent at an appropriate stage (for example, ill health early retirement applications, death benefit cases where details of the spouse are requested).	Trustees' legal advisers to prepare or review (as appropriate)	Existing application forms.	Quarter 1 2018.
Agreements with advisers	GDPR requires controllers to enter into legal binding contracts with their processors to ensure	Contact advisers at early stage to determine whether		From November 2017.

Document name	Purpose	Who will prepare?	Relevant reference materials?	Drafting period
	processing is carried out in compliance with the GDPR. Existing service agreements with advisers (most notably scheme administrators) must be reviewed and amended at an early stage to ensure compliance with the new legal requirements.	they will be providing updated terms to cover GDPR and timescale for doing so.		
Written record of processing activities	It is a requirement of Article 30 of the GDPR that controllers prepare a written record of processing activities where processing is not occasional.	Trustees' legal advisers to prepare or review (as appropriate)	The content of the written record is prescribed by Article 30. Responses to the data protection questionnaire will also help complete the written record.	Quarter 1 2018.

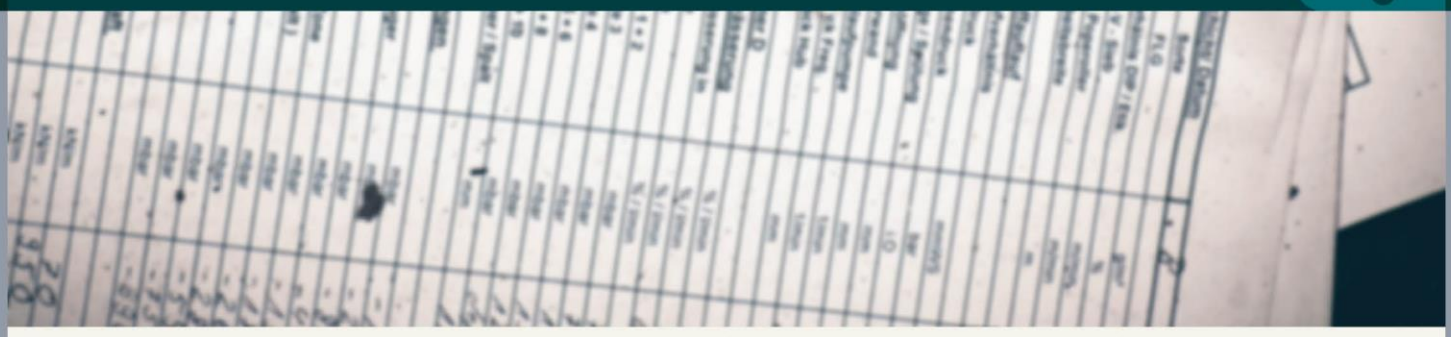


WRIGLEYS
— SOLICITORS —

GDPR
MAY 2018

GDPR Questionnaire

CONFIDENTIAL



HR response from WRIGLEYS

The Legal 500 United Kingdom Top Tier 2016

Top Ranked UK Chambers 2017 Wrigleys Solicitors LLP

Lexcel Practice Management Standard Law Society Accredited

Working to become Dementia Friendly

We are a Living Wage Employer

Questionnaire Introduction

The purpose of this questionnaire is to help the trustees to identify the types of personal data held by the trustees and their advisers and service providers and the processing carried out by and on behalf of the trustees.

Your responses will help the trustees:

- to draft a comprehensive data protection policy and privacy notices,
- to identify where individual consent may be required to process personal data,
- to provide you with better instructions regarding the processing of personal data relating to the scheme, and
- to put in place appropriate contractual provisions with you which regulate, amongst other things, the transfer, processing, retention and security of personal data relating to the scheme.

These questions are addressed to advisers; however, the trustees should also complete the questionnaire to identify, amongst other things, any personal data in their physical possession. The last five questions are addressed specifically to trustees.

Questionnaire completed by : (***insert your name***)	
Questionnaire completed on behalf of: (***insert name of firm where applicable***)	
Date:	

NB - Where you are completing the questionnaire on behalf of a firm or other organisation, references to 'You' should be read as a reference to the firm or organisation.

Questionnaire

1.	**What personal data do you hold relating to the scheme?** Where possible, please identify "types" of personal data held in relation to the scheme and by reference to the different "categories" of data subjects.

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.*

Generic data held in relation to all categories of member:	
Additional data held in relation to the following categories of member:	
• **Active members:**	
• **Deferred members:**	
• **Pensioner members:**	
• **Transferred out members:**	
• **Dependants in receipt of pension:**	
• **Ex spouse participants:**	
• **Other:**	

2.	What sensitive data do you process relating to the scheme?

Sensitive data covers *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.

For pension scheme purposes we expect sensitive data to be processed in connection with death benefits (where identity of spouse / civil partner reveals sexual orientation) and ill health early retirement applications.

3.	Please list the sources of scheme personal data. How was/is personal data collected? For example, a transfer of data from a previous administrator, a membership application form.

4.	**In relation to each item of data identified under 1 and 2 above, please indicate:** • **how long you intend to hold the data and** • **why (i.e. what criteria do you use to determine the relevant period)?** **Alternatively please provide a copy of your data retention policy.**

5.	**In relation to each item of data identified under 1 and 2 above, do you hold any data which is not necessary for the day to day administration of the scheme?** If yes, please provide details.

6.	In relation to each item of data identified under 1 and 2, what steps do you take to ensure the data is accurate and up to date?

7.	What categories of processing do you carry out on the trustees' behalf?

"Processing" *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

8.	**To the best of your knowledge what consents (if any) have members given to the processing of personal data? Is the obtaining of member consent built into any scheme processes (membership application forms, ill health early retirement application forms)? Please provide copies of any consent forms currently in use.**

9.	**Do you share personal data or sensitive data with third parties?** If yes, please provide details.

10.	**Do you send personal data or sensitive data in an encrypted format:** **a. Within your firm / organisation?** **b. Outside your firm/ organisation?**

11.	**Has any personal data relating to the scheme been transferred overseas or do you intend to transfer personal data overseas in the future?** If yes, please provide details.

12.	**What processes are in place to detect and report personal data breaches and cyber crime? Please provide copies of any breach reporting / cyber crime policies.**

13.	**What steps are you taking to ensure that you comply with the GDPR? In particular, what measures are you taking to comply with Article 32?**

Article 32 provides*, inter alia, that the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:*

(a) *the pseudonymisation and encryption of personal data;*

(b) *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

(c) *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

(d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*

14.	**Do you carry out any automated decision making or profiling in relation to the personal data? Please describe any circumstances where this might occur in the future.** For example, as part of a FRO / enhanced CETV / PIE exercise or a buy-in project?

15.	**How many subject access requests have been received in relation to the scheme? Do any processes or policies apply to the handling of a subject access request?** If yes, please describe the process or provide a copy of the policy.

16.	**If you intend to seek the trustees' agreement to new data protection provisions, please indicate your timescales for providing a copy of the draft provisions**

Trustees Only (to be answered individually and/or discussed at trustee meeting):

17.	**Who holds and / or processes personal data relating to the scheme other than the scheme administrator?** Consider: • the scheme actuary • legal adviser • internet service provider • annuity provider • IFAs • investment consultant

18.	**Please provide copies of the following documents:** a. **any privacy notices that have been issued to members** b. **any data protection and / or cyber security policies that apply to the scheme**

19.	**What personal data relating to the scheme is currently in your possession (whether in hard copy or stored on a computer/phone including email)? Where did the personal data come from?** For example, trustee meeting papers? emails from advisers or other trustees? In each case, was it necessary for the personal data to be disclosed or could it have been anonymised / redacted?

20.	**How secure is personal data held by the trustees?** Consider how personal data is shared. If personal data is shared by email, is the data routinely encrypted / password protected? Does the trustee have a company email address or a personal email address? Who has access to the email / computer other than the trustee?

21.	a. **What steps are the company taking in relation to GDPR?** b. **Are there any areas where the company and the trustees can work together? (For example, agreeing a cyber security policy? A disaster recovery policy? The aim here would be to make use of any company expertise in these areas)**

THE END
THANK YOU FOR COMPLETING THE QUESTIONNAIRE