ICAEW
BUSINESS LAW AND IT FACULTY

FAQs

GDPR FOR ACCOUNTANTS: YOUR QUESTIONS ANSWERED

Updated June 2018

Business Law / IT Faculty FAQs are published by ICAEW's Business Law team and the IT Faculty. *GDPR for Accountants: Your Questions Answered* is a series of FAQs designed to provide accountants practical guidance on the implications of the forthcoming changes to data protection legislation arising from the General Data Protection Regulation (GDPR).

This content is not intended to constitute legal advice. Members are advised to seek specific legal advice before taking or refraining from taking any action in relation to the matters outlined.

GDPR AND PENSION FUNDS

INTRODUCTION

This guide outlines the issues the General Data Protection Regulation (GDPR) raises for the trustees of pension funds, including their dealings with administrators and auditors. It is part of a series designed to answer the questions that members have been asking about the GDPR. It should be read in conjunction with the other FAQs in the series *GDPR for Accountants: Your Questions Answered* and the *guidance* issued by the Information Commissioner's Office (ICO).

It is not definitive guidance. The ICO has issued some guidance and will continue to do so after 25 May 2018. Members are advised to check regularly the ICAEW GDPR hub and the ICO webpages for the latest information, links to further information, resources and guidance and to seek legal advice if in doubt.

If you have any concerns or questions about how the GDPR may affect your business or practice that are not addressed here then please get in touch. We will be publishing a summary of the questions asked by members (and the answers) in due course as well as further guidance and webinars. This guide will also be updated as necessary.

Please Note: The GDPR is not a wholesale revision of the current legislation, so if you are compliant with the current Data Protection Act 1998 (DPA 98) you are well on the way to being GDPR compliant. The change in emphasis introduced by the GDPR, however, is significant and the new level of fines and sanctions for getting it wrong are such that no organisation can afford to ignore it. That being said, not everything has to be in place by 25 May 2018 provided you can demonstrate that you have started the process and have a plan to complete it. It is also not a one-off exercise; the accountability principle means that all organisations should be continually reviewing and updating as necessary their data protection policies to confirm that they are still GDPR compliant.

This content is not intended to constitute legal advice. Members are advised to seek specific legal advice before taking or refraining from taking any action in relation to the matters outlined.

BACKGROUND

The GDPR came into force on 25 May 2018 replacing the current legislation, the Data Protection Act 1998 (DPA 98). It will apply to any organisation, whether a data controller or data processor, that processes the personal data of EU subjects, whether or not the organisation itself is based in the EU. The size and type of organisation is irrelevant; this means the GDPR will apply to all pension funds whose beneficiaries are EU data subjects. Once the UK leaves the EU (in 2019) the proposed Data Protection Act (DPA 2018) will cover the same ground as the GDPR so any pension fund that only processes the data of UK citizens post Brexit will still have to update their data processing and protection policies.

A reminder:

1. Processing means:

    - obtaining, recording or holding personal data; or
    - carrying out any operation or set of operations on personal data, including organising, adapting, altering, using, disclosing (by any means) or removing (by any means) from the records (manual and digital).

    Under the GDPR processing covers both automated personal data and manual/paper records if part of a 'relevant filing system'.

2. A Data Controller determines the purposes and means of processing personal data

3. A Data Processor is responsible for processing personal data on behalf of a controller.

The remainder of this guidance considers some aspects of the GDPR that are particularly relevant to or tricky for pension funds. Members are advised to consult the ICAEW GDPR hub or the ICO webpages for more general explanations applicable to all types and sizes of organisation.

TRUSTEES' RESPONSIBILITIES – ANY CHANGES?

The GDPR's greater emphasis on accountability and the increased protection it affords to data subjects means that trustees will have to prove their compliance, although their overall responsibilities will not change.

Under the GDPR (as with the DPA 98) trustees are data controllers and separately liable from the employer for compliance with data protection legislation. The GDPR, however, makes trustees, as the data controller, liable for their own compliance with the GDPR. This means trustees must adhere to the GDPR in their own use of scheme data and must also only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement, though no such schemes are currently available. Furthermore processors must only act on the documented instructions of a controller.

It is therefore recommended that:

- All trustees are trained on what the GDPR is and what it means for the administration of the pension fund and how they conduct their business in relation to data that passes through their hands. As with staff this training should be updated every two years (see '**Staff Training**' below).
- A trustee protocol for keeping data secure is established and all trustees are made aware of it. It should cover all data held by trustees such as meeting papers, email communication between trustees and the pension fund administrators and/or advisors. This should also cover the return of any data when a trustee ceases to be a trustee.
- Trustees should also be made aware of and follow security measures regarding passwords, physical security of and disposal of data and equipment.

- Trustees who are also pensioners may not have an account on the employer's email system and may use a potentially less secure personal email account to correspond with the employer and other trustees on pension fund issues. If this is the case they should be given practical advice on how to maximise the security of any communications sent by them that covers pension fund business (such as recommended software to install on their personal devices, portals, or vpn access).
- Trustees should be informed of what to do in case of a breach, suspected or actual.
- Trustees will need to decide (and document) which lawful basis they will rely on when the pension scheme is processing personal data (see Appendix 1 for more detail on what can constitute a lawful basis for processing personal data).
- Contracts with service providers need to be reviewed to check if they adhere to the GDPR requirements (see below).

COMMUNICATION WITH MEMBERS – DO WE NEED TO ISSUE A PRIVACY NOTICE?

A Privacy Notice is a document explaining to data subjects (ie, pension scheme members) their rights and how their personal data will be used. They are not new but the GDPR is more prescriptive as to what they should include and how they should be prepared. In particular they must be easy to understand and not excessively long.

For pension funds this means:

- All new members must be issued with a privacy notice at the time of joining the scheme.
- Privacy notices for existing members should be (re)drafted to cover the requirements of the GDPR.
- It is recommended that newsletters to members or benefit statements should be amended to include ongoing reminders of members' rights under the GDPR.
- People included in 'expression of wishes' or death benefit forms may not need to receive a privacy notice given the confidentiality and impermanence of such nominations (but note that the ICO has been requested by the pensions industry to provide guidance on the treatment of personal data in relation to such third party beneficiaries). The Trustees should, however, ensure that the scheme only holds the minimum data necessary for it to be able to contact the beneficiaries on the death of the scheme member.
- If a fund is unable to trace a member, then provided the fund has recorded what action has been taken to try to find the member (and this is deemed reasonable), this will suffice. The GDPR in this instance will give leeway because of the disproportionate effort involved to continue to trace members and issue them with a privacy notice.

SENSITIVE INFORMATION (SPECIAL CATEGORIES OF DATA) – IS THIS RELEVANT TO PENSION FUNDS?

The GDPR like the DPA 98 contains additional provisions relating to personal data of a more sensitive nature than, say, name and address and affords it more protection. It is defined in Article 9 as 'special categories of personal data' and now includes genetic data and biometric data if processed to uniquely identify an individual (in addition to health, sexual orientation, racial or ethnic origin, political opinions, and trade union membership). Pension schemes are likely to hold special category data relating both to members and may also hold special category data in respect of third party beneficiaries nominated by members' death benefit nomination forms.

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. There are ten conditions for processing special category data in the GDPR itself, but the UK's proposed new DPA 18 is expected to introduce additional conditions and safeguards. See Appendix 4 for more detail on the conditions that must be satisfied in order to process special category (or sensitive) data. Given the limited nature of the

other conditions, if a pension scheme needs to process special categories of data, it is likely that consent would be required consent (but, under the GDPR this must be explicitly given and can be withdrawn at any time). Therefore, you will need to assess whether you still need to hold any such sensitive information (eg details such as health conditions, sexual orientation or union membership) and, if such information is still needed (for instance in relation to ill health early retirement) medical information can be held with explicit consent on the basis that, if consent is withdrawn, the early retirement is also withdrawn.

As with all personal data, you must determine (and document) your condition for processing special category data before you begin any processing.

If you have relied on consent for historically obtained special categories of personal data you will need to reassess whether this is still appropriate. As mentioned above, implied consent is no longer a legitimate basis for processing personal data; consent under the GDPR must be explicitly provided (and can be withdrawn at any time).

Please note: The proposed new DPA 18 (but not the GDPR) includes specific provision for occupational pension schemes permitting the processing of special category data under Article 9(2) (g) if the processing meets all of the following:

- It is necessary for the purposes of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme.
- It is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme.
- It is not carried out for the purposes of measures or decisions with respect to the data subject.
- It can reasonably be carried out without the consent of the data subject (that is, the controller cannot reasonably be expected to obtain the consent of the data subject and is not aware of the data subject withholding consent).[1]

This provision is similar to an existing provision on the processing of sensitive personal data under the DPA 98 (*paragraph 5 of Schedule 1 to the Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417)*).

CONSENT – WHEN IS IT NEEDED AND HOW IS IT OBTAINED?

One of the six possible lawful bases for processing personal data is 'consent of the data subject'. The GDPR standards for 'consent' are much higher than under the DPA 98 as the GDPR strengthens the rules regarding when 'consent' can be deemed to have been given by a data subject. Under the GDPR 'consent' must be freely given, explicit, affirmative, finite and documented. All data subjects must be informed that their consent can be withdrawn at any time and withdrawing consent must be as easy as giving consent. This means 'consent' can no longer be assumed or used as a 'default' lawful basis.

Pension funds are no different to any other organisation in this respect except that 'consent' under the GDPR is now less likely to be an appropriate lawful basis for the processing of personal data by a pension fund (although it may be needed in relation to 'special category data' – see above). This is because the nature of the relationship between the employer and the employee is not conducive to consent being freely given and moreover i) any such consent could be withdrawn at any time and ii) the introduction of auto-enrolment into workplace pensions means that employees cannot be required to do anything prior to becoming members of schemes.

People included in 'expression of wishes' forms do not need to give their consent to their personal data being held by the pension fund (as this is covered by the 'legitimate interests' lawful basis), and are unlikely to require a privacy notice although the scheme member will (see above). The Trustees should,

[1] (*Clause 9(3) and paragraph 21, Part 2 of Schedule 1 to the Data Protection Bill.*)

however, ensure that the scheme only holds the minimum data necessary to be able to contact the beneficiaries on the death of the scheme member.

Please note: The ICO has now published an updated version of their guidance on consent and more guidance on legitimate interests.

DOCUMENT RETENTION – HOW LONG IS NECESSARY?

The GDPR like the DPA 98 specifies that personal data should only be held for the purpose for which it was originally collected and only for 'as long as necessary'. Unfortunately the GDPR does not define 'as long as necessary'.

Pension funds, even though they typically need to hold personal data for far longer than many other organisations, will still need to consider just how long is necessary and draft a policy to explain their reasoning. Furthermore, the fund will need to ensure that they only retain the data they need to administer the fund, for example, to calculate fund values, amounts to pay out, when and to whom etc. Different data can be retained for different periods but again the pension fund will need to draft a policy explaining why it is necessary to hold each category of data, for the period specified.

It is unlikely that you will need to keep all member information – 'just in case' is not a justification for retaining data - and different types of information can be retained for different periods and in different ways. For example:

- Actuarial data can be anonymised.
- 'core membership data' can be held for many years, for example covering active, deferred and retirement phases and potentially continuing in relation to surviving spouses/dependants' pensions, but data derived or extracted from this for a specific purpose can be held for a much shorter period and so deleted when it is no longer required.
- historic scheme valuation data may not be needed once subsequent valuations have been carried out

With regard to members who have transferred out you may need to keep some of the data for a period but it should not be retained indefinitely and, in any event, only keep the data you need. To ensure compliance with the GDPR we recommend that you write a policy on how long you will retain it and why you need to retain it. Keep to the policy and review it periodically to ensure it is still appropriate.

DATA SUBJECTS' RIGHTS - HOW WILL THE NEW RIGHTS AFFECT PENSION FUNDS?

In the same way as they do for any other organisation. It is worth remembering that not all rights are absolute and not all rights may be applicable to any one pension fund. See Appendix 2 for a list of the rights. See also our FAQS - *What is the GDPR?* and *What does the GDPR mean for Accountants?*.

DO TRUSTEES NEED TO APPOINT A DATA PROTECTION OFFICER (DPO)?

This is a new post under the GDPR. A DPO must be appointed by any organisation classified as a 'public authority' and /or processes large amounts of data. The GDPR does not define either a public authority or large-scale processing but the UK's proposed new DPA 2018 (which is currently going through Parliament) has specified that a 'public authority' will be as defined in line with definitions included in the Freedom of Information Act (FOI), subject to the following qualification: a public authority will only be treated as a public authority for the purposes of the GDPR when it is carrying out a task in the public interest or in the exercise of official authority vested in it.

A DPO is the person within an organisation who:

- advises the organisation on its data protection obligations;
- monitors the organisation's compliance with the GDPR; and
- is the first point of contact with the ICO and data subjects.

The Pensions Research Advisory Group (PRAG) is currently advising that it is unlikely that a pension fund will need to appoint a DPO but it can be done on a voluntary basis[2]. Either way it is recommended that all pension funds appoint someone senior to oversee GDPR compliance and whose role may include the responsibilities of a DPO as outlined above.

For further details on the role and responsibilities of a DPO please see the ICAEW guide *So Who wants to be a DPO?*

CONTRACTS – WILL ALL HAVE TO BE REWRITTEN?

The GDPR stipulates that data processors and data controllers must have in place a written contract. Furthermore it sets out in detail what should be included in contracts between data controllers and data processors. These include the subject matter of the processing, its duration, and purpose, type of personal data and categories of data subjects. Contracts will have to be rewritten if they do not adhere to the GDPR requirements but not if they are already GDPR compliant.

As Data Controllers, trustees are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – no such schemes are currently available.

The GDPR allows standard contractual clauses from the EU Commission or a Supervisory Authority (such as the ICO) to be used in contracts between controllers and processors. However, no standard clauses are currently available. We understand that, standard contract clauses may be provided in future by the European Commission or the ICO.

Please note: the ICO is still finalising its guidance on this area. In the meantime it has produced a useful checklist of what to include in contracts. As this is a complex area we are currently advising members to seek legal advice if in doubt.

CONTRACTUAL RESTRICTIONS – POSSIBLE?

It is possible to impose contractual restrictions on access to data but care should be taken in the following situations:

- Only possible to restrict the information provided to advisors if to do so has no bearing on the outcome of the query from the advisor.
- Service Providers – should only provide them with the data necessary for them to fulfil their service obligation so again can be restricted but not if it prevents them from fulfilling their obligations to you or others (eg, a legal or statutory obligation).
- With regard to auditors – anonymised member data is unlikely to be sufficient to enable an auditor to carry out their audit, although in some situations it may be sufficient. You may request that all data retained by an auditor is anonymised subsequent to the audit (principle of data minimisation) but auditors will need to retain some data to meet their own statutory obligations.

TRANSFERS OUTSIDE THE EU INCLUDING TO/BETWEEN GROUP FUNDS – ALLOWED?

The GDPR will not change the rules on transfers outside the EU. As under the DPA 98, the GDPR imposes an 'equivalence' test to determine whether the personal data of EU data subjects can be transferred outside the EU. This will apply to intra-group transfers at it does now.

[2] PRAG – GDPR Working Party

TRANSFERS TO THIRD PARTIES INCLUDING CLOUD STORAGE PROVIDERS

Trustees should ensure that anyone who processes data on their behalf, including cloud storage providers, is fully compliant with the GDPR.

STAFF TRAINING – WHO, WHEN AND WHAT?

All staff will require training so they are aware that the GDPR is the new legislation but this can be tailored to their needs and level of responsibility. For many staff a refresher course on information and cyber security and what to do in case of a suspected or actual breach will suffice. For others, more detailed training will be required on, for example, document retention. In both cases the ICO has indicated that all staff training should be repeated (and the content updated) every two years to ensure that staff are fully aware of their data protection responsibilities. Remember the aim of the GDPR is to make sure that all those who process personal data do so securely and as appropriate: ensuring that staff are trained is one way to prove this.

ARE FINES THE ONLY SANCTIONS?

The new much greater level of fines have grabbed all the headlines but potentially more worrying for trustees is the fact that the ICO has the power to stop them from further processing.

INFORMATION AND CYBER SECURITY – HOW CAN WE ENHANCE THIS?

The best way to avoid fines and sanctions is to have robust information and cyber security. It is recommended that trustees, as part of their GDPR compliance, review existing security measures and update as necessary. As mentioned above staff and trustee training is an essential part of this.

ICAEW's Cyber Resource Security Centre and the government's National Cyber Security Centre's *Ten Steps to Cyber Security* have lots of practical advice. Trustees may also wish to consider certification schemes such as the National Cyber Security Centre's Cyber Essentials and Cyber Essentials Plus or IASME and ISO 27001.

FURTHER INFORMATION

- ICO's Guide to the General Data Protection Regulation webpage for a continually updated guide to the GDPR
- The EU's Article 29 Working Party news page for updates on their latest guidance
- ICAEW's GDPR hub
- ICAEW's FAQS 'GDPR for Accountants: Your Questions Answered'
    - *What is the GDPR?*
    - *GDPR – What does it mean for Accountants?*
    - *A GDPR Checklist*
    - *GDPR: Members' Questions Answered*
    - *GDPR Members' Questions Answered: Consent and Marketing*
    - *Engagement Letters and Privacy Notices*
- ICAEW Webinars – see Events webpage for details

APPENDIX 1: LAWFUL BASIS FOR PROCESSING

As under the DPA 98, the GDPR stipulates that before you can process data you must establish that you have a lawful basis for doing so. The GDPR, however, states that you must identify upfront the lawful basis, document the reasoning and inform the data subject of it.

Under the GDPR (Article 6) the lawful bases for processing are:

- consent of the data subject;
- performance of a contract with the data subject or to take steps to enter into a contract with a data subject e.g. personal data relevant to the provision of a specific service;
- compliance with a legal obligation, e.g. data required to fulfil a statutory requirement such as maintaining books of records, statutory audits, submitting tax returns or satisfying AML regulations;
- protection of the vital interests of a data subject or another person, e.g. medical data where the health of a data subject is at risk;
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller e.g. Public Authority duties; and
- legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. Eg, marketing of services to existing clients where the balance of rights favours the business over the data subject (the client) would not constitute a legitimate interest.

Before you can process data you must satisfy (and document how you satisfy) all the principles (see Appendix 3 for more detail on the Data Protection principles) and at least one processing condition.

For more details see the ICO guidance on *Lawful Basis* for processing.

APPENDIX 2: RIGHTS OF INDIVIDUALS

The GDPR has enhanced the rights of individuals (data subjects) and so all organisations need to be aware of these and set up policies and procedures to deal with them. The rights are now:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restrict processing
- Right to data portability
- Right to object
- Rights re: automated decision making and profiling

Please Note: Not all rights apply in all circumstances. For further details see the ICO's guidance.

APPENDIX 3: DATA PROTECTION PRINCIPLES

As with the DPA 98, the GDPR (Article 5) stipulates that the processing of personal data must be in accordance with the data protection principles. These have not changed, although the principle of 'accountability' has been added.

The principles are that personal data shall be processed in a way that is:

- fair, lawful and transparent;
- only 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 up to date;
- 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.

Furthermore Article 5(2) requires that controllers should be responsible for and be able to demonstrate compliance with the other principles outlined above. This is the 'accountability' principle and means that internal mechanisms and control systems are put in place to ensure compliance with the GDPR and that there is (documentary) evidence to prove this. This evidence may need to be produced to external stakeholders, including supervisory authorities (such as the ICO in the UK)

APPENDIX 4: SPECIAL CATEGORIES OF DATA (SENSITIVE DATA)

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

There are ten conditions for processing special category data in the GDPR itself (see below), but the DPA 18 will introduce additional conditions and safeguards.

You must determine your condition for processing special category data before you begin this processing under the GDPR, and you should document it. The conditions are listed in Article 9(2) of the GDPR:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; 4.5.2016 L 119/38 Official Journal of the European Union EN
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the

right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

For further details see the ICO guidance on special category data.

There are over 1.7m chartered accountants around the world – talented, ethical and committed professionals who use their expertise to ensure we have a successful and sustainable future.

Over 149,000 of these are ICAEW Chartered Accountants. We train, develop and support each one of them so that they have the knowledge and values to help build local and global economies that are sustainable, accountable and fair.

We've been at the heart of the accountancy profession since we were founded in 1880 to ensure trust in business. We share our knowledge and insight with governments, regulators and business leaders worldwide as we believe accountancy is a force for positive economic change across the world.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

T +44 (0)20 7920 8100
E itfac@icaew.com