GDPR for Fire Authorities

Introduction

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018 bringing significant changes to data protection legislation. But what does this mean for Fire Authorities and their pension scheme data?

What is GDPR?

GDPR is the new European Regulation intended to strengthen and unify data protection for all individuals within the EU. The principles under GDPR are broadly similar to those under the current UK Data Protection Act. However there is an increased focus on accountability. Individuals also have some new rights and there is a significant increase in the fines that can be incurred for non-compliance.

GDPR applies to personal data i.e. data relating to an identifiable individual. For pension schemes this will generally include things such as a member's name, address, date of birth, employment details, salaries and pensionable service dates. Some of the personal data held may be classed as sensitive e.g. information on a member's health.

The Government has confirmed that GDPR will continue to apply after the UK leaves the European Union and that GDPR will be enacted in UK legislation via the Data Protection Act 2018.

Surely the administrator will sort out GDPR compliance?

Each Fire Authority is considered to be a Data Controller for pension scheme data and as such determines how, and for what purposes, data is to be processed. Typically administration is carried on each Fire Authority's behalf by an external administrator such as the county council. However the administrator is considered to be a Data Processor and processes the data on the instructions of the Fire Authority. This means that ultimately it is the Fire Authority rather than the administrator that has responsibility for some areas of GDPR compliance.

What are the main changes under GDPR?

Bigger fines

GDPR has raised the profile of data protection by introducing far heavier sanctions for breaches. Fines for major breaches are now capped at 20 million euro (or 4% of worldwide turnover if greater) compared to the current cap of £500,000.

Lawful basis for processing

Under GDPR the data controller is required to have a lawful bases for processing personal data. There are six possible bases under GDPR. The legal basis that is most likely to apply for Fire Authorities is "*processing is necessary for compliance with a legal obligation*". This is because Fire Authorities are required to comply with Firefighters' pension scheme legislation. Each Fire Authority must determine the appropriate lawful basis for processing pension scheme data.

Consent

GDPR tightens the requirements on how individuals should give their consent to data processing. Consent must now be "explicit, informed and unambiguous" with members being able to withdraw consent at any time. Fire Authorities need to be clear when, if at all, they are relying on members' consent to process data. If consent is required, then the way in which consent is obtained should be reviewed to ensure it meets the new conditions imposed by GDPR. For

Firefighters' pension schemes, the most likely scenario in which consent will be required is in the context of processing sensitive medical data e.g. for ill health early retirement applications.

Privacy notices

When you collect data from individuals you need to give them certain information advising them how you process their data. This is typically done via a "privacy notice" (or "fair processing notice"). GDPR significantly expands the information which must be included in the notice which means generally privacy notices will need to be reviewed, updated and reissued to pension scheme members and dependants. As data controller, the Fire Authority has a duty to issue GDPR compliant privacy notices to all pension scheme members prior to 25 May 2018.

Individuals' rights

Under GDPR, individuals will have new rights including the "right to be forgotten". This means if an individual requests that their data be deleted, the data controller will have to delete all personal data held relating to that individual. However this right applies only in specific circumstances such as where the data is no longer necessary for the purposes for which it was originally processed. Fire Authorities will generally have good reason to keep pension scheme data so in general this right is unlikely to apply.

Existing rights will also be strengthened. For example, individuals will continue to have the right to make a subject access request to obtain copies of their personal data. However the data controller is generally no longer able to charge for these (previously a £10 charge was permitted) and must respond within a month (previously 40 days).

Data Protection Officer

Under the GDPR it becomes mandatory for all public authorities to appoint a data protection officer. All Fire Authorities will therefore be required to appoint a data protection officer. The data protection officer is responsible for monitoring GDPR compliance and liaising with the ICO. The data protection officer's role encompasses all personal data held by the Fire Authority and isn't limited to pension scheme data.

Breach notification requirements

Under GDPR there is a legal requirement to notify the ICO of any serious data protection breaches "without undue delay" and in any event within 72 hours. Individuals will also have to be notified if the breach is likely to result in a high risk to their rights and interests. All organisations must be clear how they are going to comply with the new breach notification requirements and have in place a clear plan.

Accountability

It will no longer be sufficient to simply comply with data protection legislation. It will also now be necessary to demonstrate that you are complying. It is more important than ever before to have appropriate policies in place and at to have in mind the concept of privacy by design and default. This means putting into place appropriate security measures at the outset of a project. In certain situations, where there is a "high risk for the rights and freedoms of individuals", a Data Privacy Impact Assessment should be carried out.

Record keeping

Under GDPR data controllers and processors are required to keep detailed records of processing activities. Completion of the record will require a thorough knowledge of the processing being carried out. The records must be shared with the ICO at their request. Refer to the ICO's website for a template record.

What do Fire Authorities need to do?

1. ### Map your data flows and identify the risks

   Identify what data you hold, where it comes from and who you are sharing it with. Do you really need all the data? How long are you keeping it for?
   Document the personal data you hold and keep an up-to-date record of processing activities.

2. Identify your lawful basis for processing data

Identify your legal basis for processing data, determine whether consent is required and communicate to members.

3. Update policies and procedures

Check your (or your administrator's procedures) for responding to subject access requests, requests to be forgotten and other requests from individuals. You need to have standard procedures in place and be able to comply with new requirements on timescales and charges.

4. Issue privacy notices

Review the information that you currently provide. It is likely that you will need to issue new GDPR compliant privacy notices to all pension scheme members prior to 25 May 2018. You may want to combine this with another member communication so plan ahead.

5. Review third party contracts

Update current agreements with any data processors processing data on your behalf (e.g. administrator) to ensure that new mandatory provisions required under GDPR are included. Data processors now have direct liability for breaches so may seek indemnities from controllers where the breach is considered to be caused by the controller.

6. Data Breaches

Ensure you have a breach notification procedure in place. Agree how the administrator and any other parties processing data on the Fire Authorities' behalf will fit into the plan.

How can ITM help?

We can help you prepare for GDPR in a number of ways:

- Mapping data: We can carry out a data mapping exercise, issuing questionnaires to all parties processing data on your behalf and compiling a report setting out the associated risks. Alongside this we can prepare your mandatory record of processing activities
- Provision of training: We provide half-day training sessions on GDPR compliance covering the basics alongside guidance to what you need to do.
- Updating and implement policies and procedures: We have template policies and procedures helping you to put GDPR compliant policies and procedures in place and complying with the requirement for accountability.

Please contact Rebecca Morgan, Technical Consultant at ITM for further help either via email Rebeccamorgan@itmlimited.com or phone 020 7648 9990.

Please note that this note does not constitute legal advice. ITM recommends that you seek legal advice relevant to your own specific situation wherever required