SQUIRE PATTON BOGGS

General Data Protection Regulation Compliance
Actions for Administering Authorities in the LGPS

Why Is Data Protection So Important?

Pension schemes necessarily hold and process significant amounts of personal data relating to members. As a matter of good governance, it is important that member data is safeguarded. There is already a legal obligation on LGPS fund Administering Authorities to keep member data secure, but new legislation will come into force in May 2018 that will have a significant impact on the obligations of Administering Authorities and the potential financial penalties if they get it wrong.

The GDPR and LGPS Administering Authorities

The General Data Protection Regulation (GDPR) will have direct effect throughout the EU from 25 May 2018. It applies to all EU member states and provides a single EU legal framework for the processing of individuals' data. The maximum potential fine for breaching the GDPR will be €20 million (or 4% of global turnover if higher). The government has confirmed that, despite Brexit, the GDPR will be enforceable in the UK from May next year.

Administering Authorities are responsible for the personal data held by their LGPS funds, meaning the GDPR changes are relevant to them. Every pensions team should be actively planning how to ensure compliance with the GDPR.

Administering Authorities must demonstrate compliance with the GDPR in relation to their LGPS fund. They should be able to show in a meaningful way that both the overall governance structure for data protection compliance and the individual policies and procedures relating to data processing are compliant.

Who Needs to Know?

This document is relevant to anyone working in data protection/compliance or supporting an LGPS fund, and aims to highlight the main steps that Administering Authorities will need to consider in complying with the GDPR in relation to their LGPS funds. Where an authority has already implemented general GDPR compliance processes, or has them in the pipeline, the steps we have set out can be tailored to work in conjunction with or in addition to those processes.

The GDPR – Actions for Administering Authorities

1. Maintain Records of Data Processing

It will become a mandatory requirement for Administering Authorities who employ more than 250 people, or who process sensitive personal data (about members' health or family circumstances), to maintain records of all personal data processing activities. The records may have to be presented to the Information Commissioner's Office (ICO) on demand.

Action for Administering Authorities

- Audit the current position and identify any gaps in compliance.
- Take steps to ensure all personal data processing activities are recorded.

2. Review Data Security Measures and Assess Adequacy

The GDPR retains the current obligation to have appropriate technical and organisational data security measures in place, but also provides that certain specific measures (such as encryption) should be used "where appropriate".

It also requires that processes incorporate "privacy by design and default", i.e. compliance with the GDPR needs to be integrated into all data processing and should be the default setting on all privacy arrangements.

Action for Administering Authorities

- Develop a compliance plan to ensure appropriate technical and organisational data security measures are in place both at the authority and with any third party service provider.
- Review existing applications and processes that involve the use of personal data and ensure they are secure.
- Implement a policy to ensure that data is only stored for the minimum period necessary.
- Consider whether data encryption should be used, especially for sensitive personal data such as health data.
- Default settings (for example, on member portals) must be configured to automatically provide data security.

3. Update Service Provider Contracts

The GDPR requires new content to be inserted into all service and data sharing agreements that govern the use of personal data. It also imposes direct liability on such service providers for data protection compliance.

Action for Administering Authorities

- Work with current service providers and any other third party that receives data from the LGPS fund, e.g. actuaries/auditors, to amend the contractual provisions as necessary to comply with the GDPR.
- Do not agree to any revised contract without first obtaining proper advice that it does not impose additional obligations on the authority/the fund.
- Ensure that the contractual terms applying to all new appointments are compliant with the GDPR.
- Ensure that any third party administrator maintains adequate records.

4. Revise and Update Privacy Notices and Consider Whether Member Consent Is Required

The GDPR requires additional content to be included in all privacy notices regarding how personal data will be used by data controllers. A data controller is any organisation that makes decisions on how personal data is to be processed and for which purposes, so will include the Administering Authorities of an LGPS fund. Data controllers must tell anyone whose personal data they collect what information is held, how it is used, who it may be shared with and what safeguards are in place.

The GDPR also makes it more difficult to obtain valid consent for the use of personal data – consents must be fully informed, specific, unambiguous and freely given by way of a statement or clear affirmative action by the member.

In addition, there is a specific obligation to retain proof of consent.

Action for Administering Authorities

- Review and resend all member privacy notices in order to comply with the GDPR.
- Review consents the authority relies on to justify the processing of personal data.
- Consider new or revised consent to data processing by the fund.
  New joiner information may need to be updated.
- Clear records of all privacy notices and consents must be kept.

5. Establish a Breach Management Process

The GDPR requires data breaches involving any risk to individuals to be reported to the ICO "without undue delay", and within 72 hours of becoming aware of the breach in any case. The report must contain details of the breach, including the number of individuals affected, the likely consequences and the steps being taken to address/mitigate the breach.

Affected individuals must also be notified directly if the breach is a "high risk" to their rights and freedoms.

Action for Administering Authorities

- Establish an effective data breach response plan that ensures any breach is addressed and assessed for the obligation to notify and that the relevant ICO report and any member notifications can be made in a timely fashion.

6. Appoint a Data Protection Officer (DPO)

As public bodies, Administering Authorities may be required to appoint a DPO. The European data protection authorities recommend that a DPO is appointed even if an organisation is not required to have one under the GDPR. The DPO is expected to be appropriately qualified and should report directly to the senior management at the authority. The DPO will be the contact person in the organisation for questions related to processing of personal data in respect of the LGPS fund, as well as the rest of the Administering Authority's functions.

Action for Administering Authorities

- Appoint a suitably qualified DPO, if your organisation is required to have one. This could be the Authority's appointed general DPO, if there is one, provided that person meets the criteria.
- Where Administering Authorities share pension services, one DPO could be appointed to more than one authority in respect of their LGPS funds.

7. Ensure Processes Are in Place to Cater for the New Individual Rights

The GDPR introduces new rights for individuals, including the right of data portability, the right to restrict processing, the right to object to processing, the right to object to direct marketing and the right to be forgotten – i.e. the right to have one's personal data deleted.

Action for Administering Authorities

- Identify which of the new rights may be exercised by members.
- Establish procedures to ensure that the new rights can be exercised.

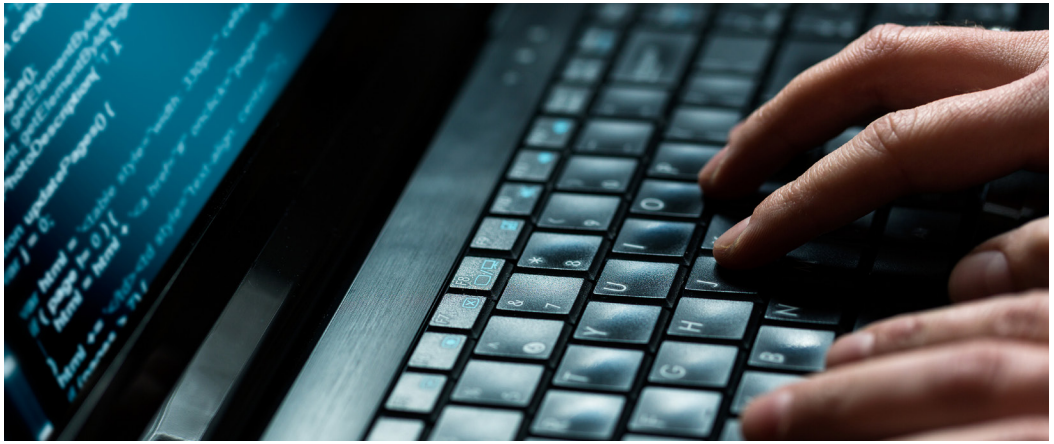
8. Carry Out Data Protection Impact Assessments (DPIA)

DPIAs must be carried out in relation to all "high risk" processing. This is where there is a high risk to rights and freedoms, for example, extensive profiling of individuals using automated processing or large scale processing of sensitive personal data (e.g. medical information). The European data protection authorities recommend to carry out DPIAs as good practice and to demonstrate accountability for processing personal data.

Consultation with the ICO may be required prior to processing in relation to high risk processing in certain circumstances.

Action for Administering Authorities

- Assess whether any use of personal data would be classified as "high risk" under the GDPR and, if so, carry out a DPIA.



Checklist

1. **Create and maintain records of data processing.**
2. **Review data security measures and assess compliance.**
3. **Update service provider contracts.**
4. **Revise and update privacy notices and consider whether member consent is required. If yes, assess whether it meets the GDPR requirements.**
5. **Establish or update a data breach management process.**
6. **Appoint a Data Protection Officer (DPO).**
7. **Ensure processes are in place to cater for the new individual rights.**
8. **Consider if a Data Protection Impact Assessment (DPIA) is required and, if so, carry one out.**

Contacts

Clifford Sims
Partner
T +44 207 655 1193
E clifford.sims@squirepb.com

Kirsty Bartlett
Partner
T +44 207 655 0298
E kirsty.bartlett@squirepb.com

Elizabeth Graham
Partner
T +44 113 284 7494
E elizabeth.graham@squirepb.com