ARTHUR COX

Group Briefing
May 2019

GDPR Update for Pension Trustees

TRUSTEE GDPR SHOPPING LIST

By now, one year on from the implementation of GDPR, all Trustees should ideally have the following completed:

1. Data Protection Policy adopted ✓	5. Updated T&Cs with third parties agreed ?
2. Data Breach Procedure adopted ✓	6. Review of scheme forms completed ✓
3. Privacy Notice issued to all members ✓	7. Review of Risk Register completed ✓
4. Employer and Trustee Controller to Controller letter in place ✓	8. Trustee Resolution of Compliance formally adopted ?

PRACTICAL ISSUES ARISING FOR TRUSTEES TO DATE

» Agreeing terms and conditions that are GDPR compliant with third parties has proved difficult, with certain third parties grappling to agree individual terms with a large number of schemes. This often becomes a "battle of the forms".

» Reliance on company policies. The Trustees need their own policies and procedures. It is not sufficient to rely on the sponsoring employer's policies and procedures.

» Data breach procedures have been put to the test as breaches have occurred and have generally required updating in line with lessons learned.

» Losing momentum at the draft stage for policies and procedures without finalising policies or procedures and formally adopting them.

WHAT HAS WORKED SO FAR?

» Most schemes have issued transparency notices to all members.

» Data protection policies, breach procedures and data sharing agreements have been drafted and adopted by most trustees.

NEXT STEPS FOR TRUSTEES FROM LESSONS LEARNED IN YEAR ONE

Test Run of the Trustees Data Breach Procedure/Incident Response Plan

Consider a test run of the Data Breach Procedure to ensure sufficient time is allowed at each stage of the response plan to react before a report has to be sent to the Data Protection Commission. This test run should inform:

- Whether there is a clear system for communicating breaches. Who are the second and third stage contacts in the event of a data breach? Consider setting up a generic email with at least three individuals copied (of whom 1-2 should be trustees).
- Whether a more detailed incident response plan is required. This would set out:
  - agreed communication protocols with relevant parties;
  - how to deal with public relations issues and reputational matters; and
  - the relevant person for dealing with each step.

Resolution of Compliance

Once trustees are satisfied the main GDPR shopping list set out overleaf is substantially complete, a resolution documenting the GDPR compliance steps taken should be passed at the next trustee meeting.

Annual Review

Consider undertaking an annual review of GDPR processes and procedures. This will assist trustees to demonstrate compliance to the Data Protection Commission as well as for the purposes of the IORP II Governance Framework in due course.

OUR TEAM

PHILIP SMITH
PARTNER
+353 1 920 1204
philip.smith@arthurcox.com

SARAH MCCAGUE
OF COUNSEL
+353 1 920 1051
sarah.mccague@arthurcox.com

MICHAEL SHOVLIN
ASSOCIATE
+353 1 920 1046
michael.shovlin@arthurcox.com

DANIEL WATTERS
ASSOCIATE
+353 1 920 1323
daniel.watters@arthurcox.com

GRACE MOORE
ASSOCIATE
+353 1 920 1371
grace.moore@arthurcox.com

AISLING RYAN
ASSOCIATE
+353 1 920 1443
aisling.ryan@arthurcox.com