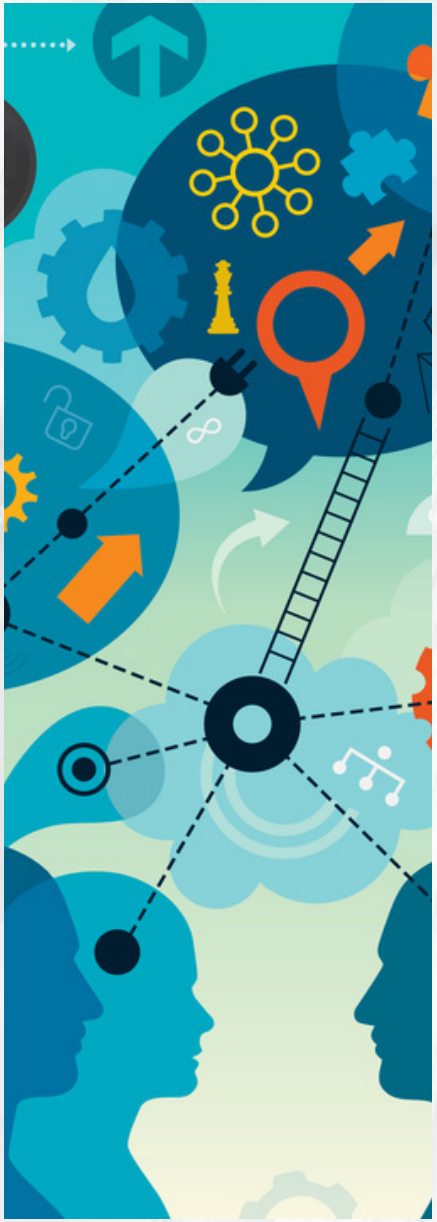
SQUIRE PATTON BOGGS

PENSIONS LIFE HACKS

May 2024



Pensions Life Hack by Philip Sutton

Data Protection Impact Assessments (DPIA) – When Are They Needed?

What Is a DPIA?

A DPIA is a process designed to describe a processing activity, assess its necessity and proportionality and help manage any resulting risks to the rights and freedoms of data subjects. In other words, a DPIA is a way for data controllers, such as pension trustees, to build and demonstrate compliance with data protection requirements.

What Is the Issue?

Under UK GDPR, trustees, as data controllers, are required to undertake a DPIA where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. The Information Commissioner's Office (ICO) has published guidance making it clear that this catches a wide variety of processing activities, including the processing of special category data to determine access to a benefit (such as processing health data when considering eligibility for ill health early retirement pensions). In other guidance, the ICO also states that it is "good practice" to carry out a DPIA for "any other major project which requires the processing of personal data". Under UK GDPR, noncompliance with the DPIA requirements can lead to the imposition of fines by the ICO.

Lessons Learned

Recent high profile cybersecurity breaches in the pensions sector have highlighted the need for trustees to keep their house in order when it comes to data protection. The widespread rollout of artificial intelligence (AI) warrants consideration under a DPIA in line with ICO guidance on the topic. We also anticipate that the ICO would expect a DPIA to be carried out on a change in administrator, or where the transfer of personal data in connection with a de-risking activity (such as a buy-in) could give rise to a "high risk" from the members' perspective. Note also that The Pensions Regulator has stated, in its initial guidance on pensions dashboards, that it may be necessary for trustees to prepare a DPIA in respect of processing activities associated with pensions dashboards. As with other data protection documents, a DPIA is not a "once and done" document. It can be updated as projects and technology evolve.

Top Tips

1. Trustees may wish to check if their service providers, particularly administrators, are planning to deploy AI to support their services (or have already done so) and undertake a DPIA accordingly.
2. Build a DPIA into project plans when switching administrator.
3. Consider if a DPIA is required when transacting a buy-in.
4. Do not forget that new data flows and data processors should be captured in other data protection documents too, notably the trustees' data map and privacy notice.
5. Use a DPIA to assess measures taken to safeguard health data collected when processing ill-health early retirement applications.

63405/05/24