WHAT DOES THE GDPR MEAN FOR PENSIONS?

BRODIES LLP

The General Data Protection Regualtion

How will the pensions industry be affected?

The pensions industry processes huge amounts of personal data - member's names, addresses, dates of birth, salary details, other financial information as well as sensitive data concerning physical and mental health.

The GDPR makes important changes to data protection law and raises the bar quite substantially in terms of obligations on those who handle personal data. Coupled with a much tougher enforcement regime and increased penalties for non-compliance, trustees and administrators should be getting to grips with their responsibilities under the GDPR now.

> We always get **excellent service** from them. **They always understand what we're looking for**, they communicate in plain English, stick to timelines and **always deliver**.
>
> Data Protection & Information Law, Chambers & Partners 2016

Changes include:

Consent

There is a new requirement for 'clear affirmative action' and an end to pre-ticked boxes and bundled consents.

Transparency

Much more information must be given to individuals at the point of collection.

Lawful Processing

There are stricter rules on processing data for new purposes.

Access rights

Greater rights are given to individuals, including rights of erasure, protection against profiling and a right of data portability.

Privacy by design and default

Existing good practice recommendations must be hard-wired into day to day operations.

Breach notifications

There are express statutory obligations to notify privacy regulators and affected individuals in the event of a data privacy breach where there is risk of harm to individuals.

Accountability

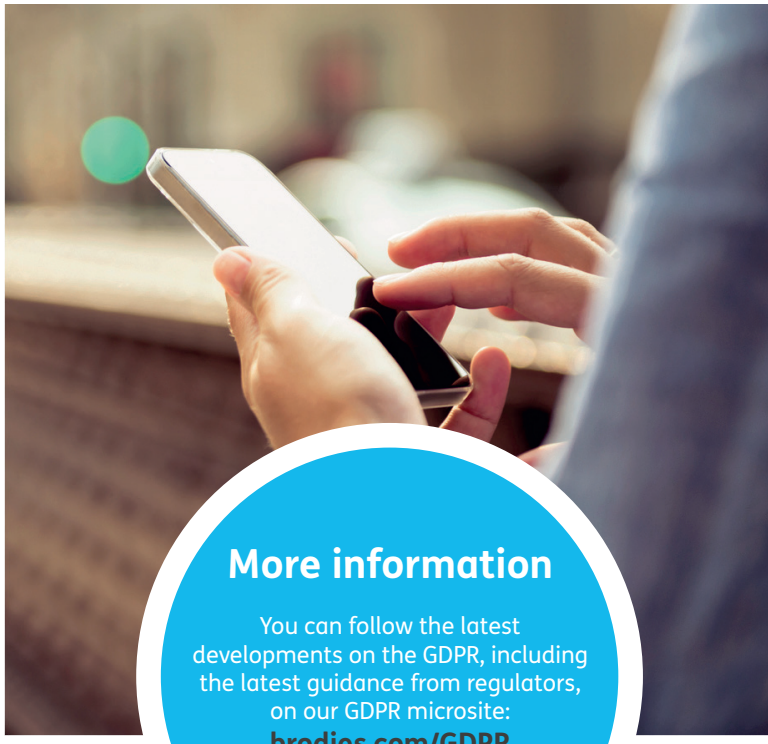
There is an ongoing requirement to demonstrate compliance to regulators on an ongoing basis and maintain records.

Sanctions

The maximum fines that can be imposed for serious contraventions are the greater of €20m or 4% of total worldwide turnover but lesser contraventions also carry hefty fines.

One stop shop

There will be a simplified regulatory oversight for organisations that operate in multiple countries in the EU.



More information

You can follow the latest developments on the GDPR, including the latest guidance from regulators, on our GDPR microsite:
brodies.com/GDPR
or our blog:
techblog.brodies.com

Specific issues:

Privacy notices

Trustees will need to refresh the privacy/fair processing notices used with members.

Consent

Where personal data is processed on the basis of consent, the basis upon which consent has been given will need reviewed. Where the consent does not meet GDPR standards, can it be refreshed or is there some other basis for processing?

Contracts

Contracts under which personal data is processed by data processors will need to be reviewed to make sure they contain the mandatory provisions required by GDPR and are updated generally. This will affect current and new contracts and is likely to impact administration services and other relevant agreements.

Individual rights

Pension schemes need to be prepared to handle the new and enhanced rights given by the GDPR to individual members in respect of their data.

Records

Trustees and those who process personal data on their behalf, such as scheme administrators, must keep appropriate records and keep them available for inspection by the Information Commissioner's Office on request.

Security and breach notification

Data security is an increasing issue. Procedures for handling data may need to be tightened and measures taken against new risks such as cyber attacks. With new requirements for mandatory breach notification, pension schemes need to make sure that they are on top of data security, monitoring and reporting requirements.

What do I need to be doing?

- identify your team and plan your strategy for compliance;
- create an information asset register – what personal information and where, why, how and with whom do you process it;
- review the legal basis for your data processing activities;
- review your data collection forms and privacy notices to ensure they meet the new requirements;
- identify your status under the GDPR;
- review your processes and systems for dealing with data subjects rights, as well as responses to FOI requests;
- implement data governance policies and measures and training to ensure your organisation operates in accordance with the requirements of the GDPR;
- review your supply chain arrangements with data processors; and
- ensure that new technology and systems are GDPR ready.

Key contacts

To discuss how the GDPR will impact on your organisation, or how Brodies can assist you with your preparations, please get in touch with a member of Brodies' information law or pension teams.

Grant Campbell
PARTNER
+44 (0)131 656 0115
grant.campbell@brodies.com

Juliet Bayne
PARTNER
+44 (0)131 656 0049
juliet.bayne@brodies.com

More information

You can follow the latest developments on the GDPR, including the latest guidance from regulators, on our GDPR microsite: **brodies.com/GDPR** or our blog: **techblog.brodies.com**

BRODIES LLP

brodies.com