Risk Alert
www.actuaries.org.uk
January 2018

RISK ALERT
General Data Protection Regulation (GDPR)

KEY MESSAGE
GDPR comes into force on 25 May 2018. While many organisations may already be well prepared, it is important that all Members are aware of how the substantial changes and increased obligations under GDPR may impact on their individual role within their workplace.

For those who are not yet sufficiently prepared, there is still time, but it is important that you act now.

Guidance has now been published by the UK relevant supervisory authority, the Information Commissioner's Office (ICO).

The IFoA Guidance for Data Controllers dated 1 August 2014 is superseded by the introduction of GDPR and the new ICO guidance, and will be withdrawn with effect from 25 May 2018.

What are Risk Alerts?
A series of email alerts drawing Members' attention to specific issues where the IFoA asks Members to think carefully about the consequences of actions they are taking or not taking.

The information in the Risk Alert is non mandatory guidance which we publish to protect the public interest.

This Alert is relevant for the following Members
All Members who handle EU residents' personal data. In particular, Members who may be categorised as data controller and/ or data processor[1] should ensure that they are familiar with the changes, the implementation date and any obligations falling on them under GDPR.

Subject matter
GDPR comes into force on 25 May 2018 and applies to all organisations established in the EU or that deal with data belonging to EU residents regardless of where the organisation is based in the world.

Some of the key changes are: -

- New direct regulation of data processors.
- New obligations for data controllers, including a duty to ensure that contracts with processors comply with GDPR.
- More stringent consent requirements in situations where consent is required.
- Some organisations, for the first time, will need to appoint a Data Protection Officer.
- New principle of accountability which places an obligation on businesses to document how they comply not just that they do comply.
- Breaches will have to be notified within 72 hours to the relevant supervisory authority (such as the Information Commissioner's Office (ICO) for the UK).
- Significantly higher penalties for data breaches (maximum fine of €20 million or 4% of annual global turnover, whichever is the greater).

Considerations for actuaries
Many employers of Members who handle EU residents' personal data will already be taking steps to comply with GDPR. Members who are employers may find it helpful to refer to the '12 steps to take now' guide on the ICO website as part of their implementation planning process.

If a Member holds a relevant individual appointment, such as under UK legislation, the Scheme Actuary to a defined benefit pension scheme, he/she may wish to consider taking advice on his/her specific obligations under GDPR if this has not already been done. Such advice should be specific to the role and might include: -

- In my role, do I handle 'personal data' as defined by GDPR?
- Has the lawful basis for processing personal data been established?
- If the lawful basis is the consent of the individual, has consent been given and is it in accordance with the more onerous requirements of GDPR?
- Am I a "data controller", "data processor" or "joint data controller" with a client?
- Do I/we have policies and procedures which clearly set out who is responsible and what the reporting lines are? Are these policies/procedures GDPR compliant?
- Do I/we need to appoint a Data Protection Officer?

The IFoA's website will be updated to provide Members with links to relevant information including the ICO guidance, which is being updated on a regular basis.

The IFoA Guidance for Data Controllers dated 1 August 2014 is superseded by the introduction of GDPR and will be withdrawn on 25 May 2018. The IFoA is not proposing to replace its 2014 guidance in light of detailed information now available on the ICO website

Professional Obligations

When considering their obligations under GDPR, Members should also be aware of the relevance of their obligations under the Actuaries' Code, Actuarial Profession Standards (APSs) and, for actuaries carrying out UK technical actuarial work, the Technical Actuarial Standards (TASs) produced by the Financial Reporting Council.

Further information and support

[1] The terms data controller and data processor are defined in article 4(7) and (8) of GDPR

Actuaries who have specific professional questions or concerns should contact the Professional Support Service.