BRIEFCASE

Data Protection (GDPR)

What is GDPR?

The General Data Protection Regulation is a new EU law that replaces the UK's Data Protection Act 1998 (DPA); its implementation is not affected by Brexit. GDPR sets out how organisations need to handle personal data from 25th May 2018.

What does GDPR mean for risk management?

GDPR should only mean a need to 'develop' your current risk management practices around data protection, presuming your organisation is fully compliant with the DPA.

However, many organisations are taking this opportunity to fully assess their data protection and information security arrangements, even if they are compliant with the DPA.

How should you prepare for GDPR?

The Information Commissioner's Office (ICO) has released a Guide to GDPR, GDPR FAQs for charities and 12 steps to prepare for GDPR. The steps that charities, social enterprises, voluntary and community groups and faith-based organisations should consider in preparation for GDPR include:

- Awareness
  Ensure decision makers, such as directors, trustees, managers and department heads are aware of GDPR and appreciate the impact it will have.
- Data Mapping / Data or Information Audit
  Document what personal data you hold, where it came from, who you share it with, what you do with it and under which legal justification.
- Communication
  GDPR requires more stringent and clear communication with data subjects. Review privacy notices and plan necessary changes in time for 25th May.
- Individuals' Rights
  GDPR provides data subjects with more rights. Review these and ensure you understand them; put in place processes for allowing subjects to exercise these rights.
- Consent
  GDPR requires more stringent recording of consent. Where you process data with consent as the legal justification, review your process for recording it.
- Children
  GDPR requires more stringent systems to be in place regarding data belonging to children. Review if you need to verify subjects' ages or gain parental consent.
- Data Breaches
  GDPR requires more of organisations if data breaches occur. Make sure you have processes in place to manage detection, reporting and investigation of breaches.
- New Processes
  Familiarise yourself with the ICO's code of practice on Privacy Impact Assessments and any other new 'data protection by design' processes.
- Data Protection Officers
  Someone in your organisation should be responsible for data protection and GDPR. You may need to formally designate a Data Protection Officer (DPO).

What does GDPR mean for your insurance?

The cover your organisation has in place for claims surrounding data protection (such as for data breaches) is dependent on your insurance policy. You may find that you have some cover under Public Liability and/or Professional Indemnity but you should consider specialist cyber and data protection insurance.

The implementation of GDPR should not change any cover you previously had that related to DPA, but this depends on your policy wording.

Summary

All not-for-profit organisations need to have a comprehensive awareness of data protection legislation and its impact. You should consider what preparations and protections are necessary.

Further information

GDPR: Guide for Charities – Charity Finance Group

Guide to GDPR - ICO

GDPR: Charity FAQs - ICO