KEY DIFFERENCES BETWEEN THE DATA PROTECTION ACT AND GDPR

From ***General Data Protection Regulation: A guide for charities,*** 49pp, free download from Charity Finance Group via *http://www.cfg.org.uk/resources/Publications/cfg-publications.aspx#GDPRguide* (or go to www.cfg.org.uk and click on Resources near the top of the page, then Publications). **Highly recommended.**

Circulated as an attachment to Sandy Adirondack's legal update on GDPR for voluntary organisations, 13/2/18. Contact legalupdate@sandy-a.co.uk to receive email updates on voluntary sector law and governance.

Here are some key differences:

DATA PROTECTION ACT	GDPR
EU member states created their law around data protection	A unified approach across all member states – the UK will continue to be part of the GDPR even after departing the EU.
Covers Personal Data and Sensitive Personal Data	Covers Personal Data and Special categories of Personal Data – now includes biometric and genetic data and online identifiers.
Data Protection Officer is not required in an organisation	Data Protection Officer is required for Public Authorities (e.g. local councils, regional government) and organisations where core activities consist of processing, on a large scale, special categories of personal data OR the processing activities require regular systematic monitoring of data subjects on a large scale (e.g. hospitals).
Consent – must have been freely given, be specific and informed	As before, but also consent must be clear, recorded, and be able to be withdrawn. Data Controllers must be able to demonstrate that consent has been given if consent is used as the basis for processing.
No legal obligation for data controllers to report breaches of security	Data breaches must be reported to supervisory authority (ICO in the UK) within 72 hours and in some cases to the data subjects as well.
Data Protection Impact Assessments are good practice for projects involving personal data	Data Protection Impact Assessments are now mandatory for projects/processing likely to result in a high risk to rights and freedoms of natural persons
Subject Access Requests – data to be provided to subject within 40 days and a fee of £10 could be charged	Subject Access Requests – data to be provided within one month and no fee chargeable. However, a 'reasonable fee' can be charged if the request is manifestly unfounded, excessive, or repetitive. A reasonable fee can also be charged to comply with requests for further copies of the same information. This does not mean that an organisation can charge for all subsequent access requests. Any reasonable fee must be based on the administrative cost of providing information.
Maximum penalty is £500,000	Maximum penalty could be up to €20 million or up to 4% of global turnover.
Accountability – limited and Data Processors have very little unless tied down in contract with a Data Controller	Data Controllers must be able to demonstrate that they comply with GDPR and there are requirements on Data Processors.