Appendix A – GDPR and Data Protection Comparison Overview

Themes	DPA	GDPR
Rights of Data Subjects	• Access to personal data • Prevent processing likely to cause damage or distress • Prevent processing for direct marketing • Object to automated decision making • Have inaccurate personal data removed • Claim compensation for damages caused by a DPA breach	• Data portability • Right to be forgotten • Object to processing • Right to request opt out after permission given • Must be notified of automated decision making and have the right to request "human decision making" • Continues not to apply to deceased persons
Subject Access Requests	• Where an individual requests access to their own information • Required ID and a written request • 40 day deadline to respond • £10 fee required	• Deadline to respond 1 month • No fee required • Reasonable steps to verify identity
Data Breaches	• Report to Senior Responsible Information Officer (SIRO) • No obligation to automatically report to the Information Commissioner's Office (ICO) • Maximum fine £500,000	• Must be reported to ICO within 72 hours • Fines up to 2% of turnover or €10m for poor record keeping, contracting etc • Fines of up to 4% of turnover or €20m for breaches of rights or principles • New definition 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed

Privacy Notices and Consent	• A privacy notice should contain: the identity of the data controller; the purpose for which you intend to process the information; any extra information you need to give individuals the context to enable you to process the information fairly • Soft opt in to data protection and use of information for specified reasons is permitted (e.g. tick this box if you don't want us to use your information)	• Show the legal basis for processing information • Data must be trackable • No more 'soft opt ins' • Controller must prove consent
Privacy Impact Assessments	• Not Mandatory • Recommended when processing large amounts of data	• Mandatory for all business cases • Privacy by design
Other Considerations		• DP Officer's mandatory role in an organisation processing data • Consent for use of Children's Data • Child likely to be defined as anyone under 13 years