GDPR Glossary

- **Data Subject** - A data subject is an individual who is the subject of personal data.
- **Personal Data** - The definition of personal data is highly complex and for day to day purposes it is best to assume that all information about a living, identifiable individual is personal data.
- **Data Processing** - Data processing includes reading, amending, storing and deleting data. Data processing is any action taken with personal data including the collection, use, disclosure, destruction and holding of data.
- **Data Controller or Data Processor? -** Control, rather than possession, of personal data is the determining factor here. The data controller is the person (or business) who determines the purposes for which, and the way in which, personal data is processed. By contrast, a data processor is anyone who processes personal data on behalf of the data controller (excluding the data controller's own employees). This could include anything as seemingly trivial as, for example, storage of the data on a third party's servers, or appointing a data analytics provider.
- **Subject Access Request** – Individuals have the right to be told what personal data an organisation is processing about them and, unless an exemption applies, to receive a copy of that information. They do this by making a data subject access request.
- **Data Protection Impact Assessment (DPIA)** - Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. They should be completed for each new project involving personal data an organisation undertakes.
- **Phishing Attack -** Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

Definitions taken from ed.ac.uk, osborneclarke.com, incapsula.com and the ICO.