What is the GDPR?

The Principles

The GDPR aims to harmonise regulations across the EU and govern the recent digital wave where individuals share a great deal of personal information online.

At the heart of the regulation lies the human right for privacy, which often overlaps with surveillance by governments striving for public safety, together with corporations striving for profits and consumer satisfaction through accurate profiling of their consumer base.

The regulation empowers data subjects (for clarity – any citizen of any country) residing in the EU to have better control over how their personal data is processed by governments or corporations, and making sure that all actions performed have the citizen's consent.

All government bodies and corporations processing:

- GDPR aims to regulate treatment of data subjects in the EU at the time of processing, regardless of residency status.
- Any company with operations in EU member states must ensure, at minimum, compliance with regulatory requirements.

DPA Versus GDPR

The seven key comparative areas between the Data Protection Directive 1995 and the General Data Protection Regulation 2016.

	Data Protection Directive 1995	General Data Protection Regulation 2016
Sanctions	Maximum penalty of £500,000 in the case of a data subject having suffered harm or financial loss. Local supervisory authorities can also use non-monetary corrective powers.	Two tiers of monetary penalty issued dependant on the type of violation and which articles are in breach, the largest of which is up to €20,000,000 or 4% of global revenue from the previous year in the case of an undertaking. Local supervisory authorities can also use non-monetary corrective powers. In addition, data subjects have the right to seek compensation from local courts, where appropriate.
Consent	A negative opt-in has been relied on by most marketers as a form of consent.	Opt-ins can no longer be negative and non-action is not accepted. Consent is time limited, must be explained in clear language and data subjects must be given options to exercise their rights.

Continued...

...continued

	Data Protection Directive 1995	General Data Protection Regulation 2016
Data Subject Rights	Data subjects have right of access to their data with payment of a nominal fee. Common law right of erasure and rectification.	Greatly expanded. Nominal fees can no longer be applied. In addition to previous rights, data subjects now have the right to portability, objection, notification and restrict processing.
Data Processing	Organisations were required to register with the local supervisory authority to permit the processing of personal data.	Prior registration is no longer required. However all organisations processing personal data are expected to undertake rigorous risk assessments to document and assess whether data processing activities have an undue and negative effect on data subjects.
Personal Data	Personal data is defined as any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.	The scope of personal data has been widened to include online identifiers such as an IP address and has a sub category known as the special categories. The processing of special categories of personal data are forbidden unless specific conditions are met. This category includes religious beliefs, trade union membership, philosophical beliefs, sexual orientation, sexual history, biometric data and health data.
Data Breaches	It is not mandatory to report a breach under the DPD 1995.	It is mandatory to report a breach to the supervisory authority if the rights and freedoms of data subjects are at risk. Data breaches must be reported to the supervisory authority within 72 hours of detection, in the case of a data controller. Initial reporting may be partial if not all the facts have been established.
Data Protection Officer	Some European supervisory authorities made the appointment of a data protection officer mandatory. Notable example being Germany.	The appointment of a data protection officer will be mandatory in all EU/ EEA member states based on three conditions. Data protection officers can be outsourced and be shared amongst joint organisations.

What Data Matters?

Under the terms of the GDPR, any data that identifies a living natural person, so an individual not a business, either directly or indirectly, matters. The definition is divided into Personal Data and Special Category Data, the latter having more controls put around it.

Personal Data

As one would expect, personal data covers any data which will identify an individual. So, a first name and a surname may not constitute personal data as it may not be unique enough to identify a single individual. However, coupled with other data items, there is a narrowing down to an individual. So, a simple test has to be 'can I identify an individual from this data set?' If you can, it is personal data and as far as the regulation is concerned, it matters.

To bring the regulation up to date, a number of elements have been added and are now classed as personal data. Location data, either obtained via device identifiers or an Internet Protocol (IP) address, static or dynamic, is now considered personal data.

Special Category Data

Special Category data may only be processed if there are specific requirements to do so, and the regulation is clear on these conditions. It is also clear what is Special Category data, which is:

- racial or ethnic origin data;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health;
- data concerning a natural person's sex life;
- data concerning a natural person's sexual orientation.

So, in strict terms, this is the data that matters as far as the legal definition is concerned. But what about those edge cases? For example, is a person's work email address personal data? After all, it identifies a natural person. I asked this question of the Information Commissioner some time ago. Their view at that time was that it was not personal data, but it had to be treated with respect and the subject had the right of deletion, etc. Recently a client of mine was told by their legal advisers that in their view, such data was personal and needed to be protected. So, what is the real position? I don't think it is too difficult. When you consider the data you hold, in one way or another it is valuable and therefore important to you. If it isn't, why have it? Why discriminate? Treat it all the same and protect it as you would personal data, then you cannot go far wrong.

So, I suppose I'm saying all data matters. If it isn't important to you, you don't need to hold it. If it is important to you, protect it.