Need help understanding GDPR? **Email marketing@goodwille.com**

Good to know.

The General Data Protection Regulation (GDPR)

From 25th May 2018, a new data protection regime will apply in the UK – the General Data Protection Regulation ("GDPR"). The GDPR brings with it increased obligations for businesses and will have a major impact on the way in which businesses manage personal data. Its aim is to ensure greater accountability and transparency when it comes to personal data. Personal data means any information relating to a living person who can be identified, directly or indirectly, using that data.

What do you need to do?

Now is the time to put in place the correct policies, practises and procedures to ensure ongoing compliance, transparency and accountability by 25th May 2018. You should consider:

- A full audit of current practises and policies to identify gaps in compliance with current data protection legislation and how to amend these to ensure compliance with the GDPR;
- Reviewing terms & conditions and privacy policies with clients/customers;
- Checking contracts with suppliers and sub-contractors;
- Reviewing/implementing training for staff.

Remember that any investigation into your business' practises will mean unwanted attention, damage to your reputation and potential loss of business. Besides - historic, obsolete and uncategorised data is expensive to store and of little relevance to your business going forward.

What is changing?

Consent

The definition of consent is changing under the GDPR. Consent to collect and process personal data will now have to be "freely given, informed and unambiguous".

- Express, active opt-in will be needed.
- Silence and/or pre-ticked boxes are not acceptable.
- Existing consents may need to be refreshed.
- Additional consent is required for direct marketing purposes.

Accountability and Governance

The need to register with the Information Commissioner's Office (ICO) will no longer apply under GDPR, but you will have to demonstrate compliance with legislation through accountability and governance. This means having the appropriate written policies and procedures in place.

Data Processors

There are lots of new obligations and responsibilities for data processors, and if you process data on behalf of another business, or use data processors, you need to be aware of these new obligations and update your contracts with those processors to reflect the changes.

Breach reporting

Under the GDPR, it will become mandatory for all data processors to notify the ICO and data subjects of certain breaches within 72 hours of a breach.

Individual Rights

The GDPR increases emphasis on the rights of individuals; for example, the right to be forgotten, and the right to restrict how data is used. You and your staff need to understand what these rights are and what they mean in practise.

Data Protection Officer ("DPO")

It will be mandatory to appoint a DPO in certain circumstances, such as where a business has over 250 employees, or if it is a public authority.

The maximum fine will be €20 million (or 4% of worldwide annual turnover, whichever is higher). This is a significant increase from the current maximum penalty in the UK of £500,000!