The EU’s General Data Protection Regulation (GDPR) comes into force on 25th May 2018, enforcing a strict set of new rules concerning privacy and data security and imposing strict penalties on violators.

Many of the GDPR’s main concepts and principles are much the same as those in the current Data Protection Act (DPA).

However, there are new elements and significant enhancements.

GDPR will see individuals have more control over their own personal data. This means that when handling an individual’s personal data, we will have a responsibility, as a business, to meet their rights.

From a small business view point GDPR relates mainly to Personally Identifiable Information (PII) and includes any data that is held about someone and which could be used to identify them.

This covers not just someone’s name, address and phone number but also any of their genetic, health, cultural, economic and social details (which other than perhaps on job application forms we don’t ask for such personal details).

So, what does GDPR mean in practice?

Individuals will have eight rights. These are:

* The right to be informed how you use their personal data
* The right to access their personal data
* The right to be forgotten and have their data deleted in specific circumstances
* The right to data portability to transfer their data to another service provider
* The right to have information corrected if it’s out of date, incomplete or incorrect
* The right to object to, or stop, their data being processed on certain grounds
* The right to restrict processing, meaning they can request that their data is only kept on file and not used for processing
* Rights in relation to automated decision making and profiling, meaning that in some cases individuals have the right not to be subject to a decision that is based on an automated process.

Whilst as a business and our central customer database allows us to quickly identify our customers and the information we hold on them, there will be still be a few changes required over the coming months. One of the advantages of being a franchisee and using our niceneasy CRM system and in particular the quoting system is that you would be informing your potential clients that you are GDPR compliant.

However, as an individual business (be it Limited, Sole Trader or Partnership) we all hold information on our clients, staff and probably suppliers which are outside of the CRM.

Whilst thankfully there are a number of concessions to small businesses we all have to comply with a number of the key acts and I would urge you to be prepared for this in particular any “Subject Access Requests” (SAR’s) – a request under the DPA used by individuals who want to see a copy of the information that you hold about them – and the ’right to be forgotten’, which may require you to identify and erase all of an individual’s data.

You should therefore start to consider what data / information you hold, where it is stored and why. This could be customers data such as bank details, old spreadsheets for scheduling, pictures etc. and even information on current and ex staff members.

If you are using a third-party Accountancy System, it would also be prudent to ask them if they are GDPR compliant.

GDPR shouldn’t have a major impact on each of our individual businesses but please be aware of the new rules as I am sure that we all have at least one customer or potential client who may challenge or ask you regarding this. Rest assured that nicenstripy Gardencare Limited is GDPR compliant where applicable but as individual businesses you do have a duty of care and responsibility.