GDPR – Getting Data Protection Ready

General Questions

On 25 May 2018 the General Data Protection Regulation (GDPR) replaced the Data Protection Act (DPA). The aim of GDPR is to give individuals more control over how their personal data is used and for businesses to be more transparent in how that data is processed. These FAQs were produced by Ian Grey of Wadiff Consulting.

Does Brexit mean we don't have to do anything?
The UK Government has confirmed that Brexit has no impact. As part of the work on Brexit, there will be a new Data Protection Bill which will comply with the GDPR requirements so what you've done up to now is not wasted effort.

Is this a new set of rules?
It is an evolution in data protection requirements, not a revolution. It demands more accountability for the use of personal data and enhances existing rights of individuals. If you are already fully complying with the DPA, and have an effective data governance programme in place, you are already well on the way to being ready for the GDPR.

If the GDPR is not followed, the Information Commissioner's Office (ICO) can take action. This includes fines of up to €20m or 4% of global turnover, whichever is the greater. The ICO said it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm". They have "a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. While these will not hit organisations in the pocket – their reputations will suffer a significant blow."

What is the scope of the GDPR?
Although it is mainly about the personal data of people in the EU, the scope is wider. It is covered in Article 3 of the GDPR. It applies if a company:

- is established in the EU
- is based outside the EU and offers goods or services to people in the EU or monitors the behaviour of people in the EU

For a company established in the EU, the GDPR needs to be followed for the personal data used in all the events it runs, including those outside of the EU. The GDPR says protection of personal data is a 'fundamental right' so the same rules should apply for all the personal data being processed. 'Processing' covers the collection, storage, updating and use of personal data. The full definition is in Article 4 of the GDPR.

The GDPR would ***not*** apply to a company established outside the EU, running events outside the EU and holding no personal data of anyone in the EU. However, if an individual in the EU signs up to their marketing email, the GDPR does apply to the personal data for that individual.

What is meant by Personal Data?
Personal data is any information that can directly or indirectly identify an individual. This includes name, email address, identification number, location data, IP address and physical data. There are "special categories" of data which require extra levels of consent and security. This is data about race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, genetic data, biometric data, health data and data concerning a person's sex life or sexual orientation.

For a company (data controller), it will include details of your staff (full time, part time and contractors), customers, clients, partners and suppliers. The data could be on paper, held electronically (files, emails, SMS etc.), as voice mail, images on CCTV etc.

Email addresses such as ***info@companya.co.uk*** or ***sales@companya.co.uk*** are not personal data as you cannot identify an individual. ***firstname.lastname@companya.co.uk*** definitely is personal data. Addresses such as ***firstname@companya.co.uk*** or ***firstname@gmail.com*** should be considered as personal data as they could be indirectly linked to a person if combined with other data.

Isn't this an issue for IT?
The GDPR is mainly about processes and procedures across an organisation. It mentions "...appropriate technical and organisational measures" ten times. IT plays a big part by providing secure systems, ways to protect data while it is being transferred (this includes encryption of mobile devices) and tools to locate, report on and delete personal data, but treating it as an IT issue isn't the right approach.

How do we delete personal data we can no longer use?
Paper records in an office or held in offsite storage need to be shredded or securely disposed of using a third party that deals with confidential waste. Electronic records need to be deleted. This includes any copies of the data made by downloading it from a CRM system or database to spreadsheets or another format.

How do we deal with a subject access request?
The ICO has a code of practice for subject access requests. Although it was produced for the DPA, the approach is still valid https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf. As personal data is being transferred it should be done securely, e.g. in password protected files.

What should we be doing?
1. Use the ICO website to find out about the GDPR Principles and the increased rights of individuals
2. Do a 'data mapping' exercise to identify the personal data you hold, where it came from, who it is shared with, the legal basis for holding it, how it can be used to support the rights of individuals and how it is protected
3. Work out where changes are required to the processes, procedures and systems that are currently used to manage personal data
4. Create a plan to make changes; prioritise changes that present the highest risks and remember that the GDPR mandates organisations to put into place comprehensive but ***proportionate*** governance measures
5. Implement the changes