**Top Tips on GDPR!**

GDPR came in to effect on 25th May and there is a lot of scaremongering being driven largely by consultants wanting to make lots of money! This is not only our view but the view of the CEO of the ICO: “some of the fear is rooted in scaremongering because of misconceptions or in a bid to sell ‘off the shelf’ GDPR solutions.”

Our Managing Director Jayne Bratton has been very vocal about her frustrations on the scaremongering and therefore ran 3 courses at a ridiculously low price to help the owners of SMALL businesses to understand what they need to do and bust some myths!

Based on our understanding of how GDPR applies to small businesses, here are some of the key messages we feel you might want to be aware of:

* **GDPR** is **The Data Protection Act of 1998** with a few bells and whistles. Much of what has been highlighted in the media as actions that must be taken by businesses has been in existence since 1998
* **Privacy notice:** you do need a statement about how your company uses data. Here is to the GDPR advice on this <https://ico.org.uk/global/privacy-notice/> and here is a link to our own statement as an example: <http://thebrattongroup.co.uk/wp-content/uploads/2018/05/Data-Protection-and-Privacy-Statement-21-5-2018.pdf>
* **What is ‘Personal information’?** This means any detail about a living individual that can be used on its own, or with other data, to identify them. e.g. name, identification number, location data or online identifier
* **What is the ‘ICO’?** The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. ICO stands for Information Commissioner’s Office
* Most businesses need to **register with the ICO.** Here is a link to see if you need to register: <https://ico.org.uk/for-organisations/register/self-assessment/> For small businesses this costs £35 per annum
* GDPR:
* **will still apply** when we leave the EU
* applies to both **paper and online** data filing systems
* There are now **data controllers** and **data processors** in GDPR.
* Controllers are the people who decide what the data is used for and how it is used
* Processors act on the controller’s behalf.
* **Training your team:** you must train your team in GDPR and the processes within your company
* **People have the right to:**
* request a copy of all the personal information you have about them. You must provide this within 30 days and you cannot charge for this.
* insist you to remove all the data you have about them.

To review these rights see this link: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights>

* **Data cleanse:** take time to look through the data you have and if you no longer use or need it then you should remove it. For example, we are removing any person’s information that we have held on our systems for years if we don’t know where we got it from or who they are as we can’t explain how we obtained it.
* **How long should I keep the data?** Our summary of this is as follows: can you stand up in court and justify why you have kept the data for this long? Your reasons for doing so might be in case of a tax inspection, for example, in order to adhere to legal obligations. Most people are keeping their key data for at least 7 years – though I do stress that if someone asks to have their data erased then you DO NOT have to delete anything you need for legal or adherence purposes!
* There are many **different legal reasons for holding and processing personal information** including:
* Consent (this is the one where everyone was sending out emails in the weeks leading up to 25th May)
* Contractual: to deliver an agreed piece of work
* Legitimate Interest: when you use people’s data in ways they would reasonably expect, and which have a minimal impact on privacy
* Processing laws: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>
* **Contractors and suppliers:** you must have in place a written agreement explaining how each party will process the data, who controls it and how the data will be used
* **Special category data:**
* The requirement is to identify a specific condition for processing this type of data e.g.: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation
* In most circumstances, you can only process this information with the person’s explicit consent. Although there are 10 conditions this is by far the most common
* **Data breaches:** technically you do not have to report all data breaches; it depends on the impact on the people whose data you hold. However, as this has still not been clearly defined by the ICO we recommend you always call the ICO for advice and guidance
* **Data Protection Impact Assessments**: contrary to some scaremongering out there you do not need to have a Data Protection Impact Assessment of all the ways you process and hold data. However, they are mandatory in certain circumstances where data processing is likely to result in high risk to individuals, for example, where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals, where there is processing on a large scale of the special categories of data.
* **Top 4 things we think you should focus on to start with:**
1. Register with the ICO
2. Create a Privacy Statement and/or review any you currently have
3. Know your responsibilities for GDPR
4. Write your internal procedures for GDPR

**For more information:**

We always advise referring to the ICO as they are the ones who can best advise you. They have a dedicated advice line which offers help to small organisations preparing for the new data protection law, including the General Data Protection Regulation. Their phone service is aimed at people running small businesses or charities. To access the new service dial the ICO helpline on 0303 123 1113 and select option 4 to be diverted to staff who can offer support.

A link to a fairly new summary for micro business owners and sole traders: <https://ico.org.uk/media/for-organisations/documents/2258293/eight-practical-steps-for-micro-business-owners.pdf>

Link to a summary for larger businesses: <https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf>

*Please note: this is a summary of our understanding of the key points in the legislation based on what we have read on the ICO website and training we have received. The information in this article must be read with the knowledge that we are not lawyers and therefore we do not accept liability for any actions you do or do not take as a result of what we have shared in this article, presentations or talks we have given. We recommend you refer back to the ICO itself for the most accurate guidance.*