GDPR in a nutshell for Owners of Small Businesses

1 What is GDPR?

GDPR is the new Data Protection and Privacy law which comes into effect at midnight 25th May, 2018.

It stands for the '**G**eneral **D**ata **P**rotection **R**egulation' and it is designed to protect the individual rights of all European citizens, wherever they or their information is around the world. Enforced by a set of high-impact legal and financial penalties capable of getting the largest organisations to pay attention, GDPR provides a set of tools by which individuals can gain some control over their online identities.

In the UK, where data protection is enforced by the Information Commissioners Office (ICO) through the Data Protection Act, this will be replaced by a new Data Protection Bill which enforces GDPR and which will remain on the statute books once the UK leaves the EU in 2019.

2 What does it mean for us as individuals?

We now have rights which are legally enforceable by an authority with legal and financial clout. This gives us as individuals a degree of influence we have not previously benefited from.

We can now:

- find out what data an organisation holds on us, and know exactly what they are using it for;
- ensure that we have to give our consent to any changes of use of our data before the event;
- request our data is corrected if we believe it is inaccurate
- remove our consent for its use especially for direct mailing or personal profiling;
- get copies of our information to take elsewhere;
- request an organisation removes our data and forgets us (subject to contractual requirements);
- force organisations to stop using our data while it is inaccurate or we dispute its usage;
- ask for human intervention when the computers make decisions we disagree with;

Organisations must provide a named individual as the main data protection contact and they only have 1 month to respond without being allowed to charge for their time!

3 What does it mean for you as a business owner?

As a business owner, you have to fulfil the individual's rights above and your business needs to adhere to a set of overarching principles about how it acquires, manages and uses personal information:

- You must be open, lawful and fair about what information you have, why and how you use it;
- The data you collect, store and process must be for specific purposes which you inform the individual about at the time of collection and they have explicitly consented to;
- You can only collect the minimum amount of information you need to fulfil your requirements;
- The data you process must be accurate with the onus being on you to verify this and provide simple ways for the individual to correct it;
- You can only hold information for a limited time and no longer than contractually necessary;
- You must store and process information in a secure manner;
- You must have a named individual that people can contact to exercise their rights. They will be accountable for information security in your business!
- Being given someone's business card at an event is not explicit consent for you to contact them

You must respond to individual's Subject Access Requests within 1 month and you can't charge.

And you must be able to prove your compliance with GDPR through documented processes and measures, though how far you need to go depends on the size of your business and its resources.

4 What do you need to do?

- Find your data –know what you have and where it is. Categorise it. Decide who should access it. Create a simple spreadsheet to catalogue data so you know where to look.
- Clean it – do you need it? If not, be brave and get rid of it. But this conflicts with HMRC requirements – so for now go with HMRC until they publish clarification.
- Do you have any sensitive data? Do you really need it? If you do, encrypt it now! If not, delete it!
- Periodically clear out data you don't need. Keep on top of your information!
- Have you got consent from all your customer database? If you have the details, send a letter to get consent so you have things in writing. If you only have email then send link to webpage asking for explicit consent but be warned that doing this has already caused problems for some businesses!
- Add explicit consent option to sign-up pages – remove all prefilled boxes. Make sure you are explicit about what you need, why and how you will use it and give them the option to consent to this. Implicit consent is illegal and subject to the largest penalties!
- Be careful about Google activity tracking – you must tell people if you use it. Also check if your business website is using logging as this is classed as PII and needs to be protected separately.
- Add a Privacy statement page to your website with a link to it near to every sign-up option!
- Make sure you publish the name of the person responsible for Data Protection in your business (the "Data Protection Officer"). As the owner of a small business, this will be you!
- If you don't have a legal purpose or explicit consent to use the data you can't. Get rid of it!
- Personal data cannot be sent to any nation outside the EU or so called second countries (where there are comparable data protection/data privacy rules such as the UK, Argentina, New Zealand)
- Make sure you know where your data really is. Ensure all cloud providers adhere to GDPR or Privacy Shield if they are American. They will have a privacy or data processing statement explaining this. If they don't and something goes wrong, you are liable. Google, DropBox, Microsoft, Amazon all use EU data centres. Apple will do before GDPR becomes law
- Get your cyber security in order- Cyber Essentials would be good and is becoming de-facto requirement for minimum security standards
- Document everything (even if you only get screenshots). You must be able to prove you have taken reasonable measures.
- If someone gives you a business card, get them to initial and date it so you can contact them!
- If in doubt, seek advice!

Helpful Definitions

- Personally Identifiable Information (PII)– anything which on its own, or when combined with other information can identify a living person. i.e. Name, address, phone numbers, email addresses, NI numbers, NHS numbers, IP addresses
- Sensitive Personal Information – anything which can prejudice a person such as religious beliefs, union membership, sexual preferences, political affiliation, criminal record etc.

Compliance will take time and effort, but it will cost much less than being caught not bothering!

So, if I can help your business with any data protection or compliance issues,
please call me on **0121 405 8369**,
email me at **scott@ebitconsultancy.co.uk**
or visit my website at **https://ebitconsultancy.co.uk**.
I look forward to helping you soon,

Scott