10 steps to becoming GDPR compliant*

*Please note that this is not legal advice

After more than three years of discussion the EU General Data Protection Regulation (GDPR) framework has been finally agreed on, which will replace the current 1998 Data Protection Act and will be effective from 25th May 2018.

The main intent of GDPR is to give individuals more control over their personal data and electronic privacy, impose stricter rules to companies handling it and make sure companies embrace new technology to process the influx of data produced.

We know that GDPR can seem frightening and confusing, so we've created 10 steps to becoming GDPR compliant.

1 

Ensure the whole team is aware of GDPR and assign a trained GDPR officer within your company. Your assigned officer should be the main point of contact for anything GDPR related – it is their role to ensure the following steps are put in place and inform each team of any updates.

2 

Make a list of all the systems you use that hold personal data and define exactly how you are using it. For example, the data you have may be customer orders or you may use the list for marketing purposes. If so, determine which method you are using to contact each list; whether it's email, post or telephone.

3 

Document the data collected in each system i.e. what type of data you are collecting. This might be a person's name, address, email, telephone – even nationality is classed as personal data. Also ensure that if a person's data is duplicated across several lists, you're aware of this.

4 

Decide whether you are a controller, processor or even both.

Controller – "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". So if you're making the decisions on collecting personal data, who to collect data about, the purpose for collecting the data and whether to disclose the data, you are a controller.

Processor – "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". So for example if you are a marketing company and your client gives you data to upload to Mailchimp, you're processing the data on behalf of another company but do not make decisions as to how it is used, you are a data processor.

5 

Understand how you're transferring data. Do you have a marketing company outside of the EU? Or perhaps you use Mailchimp for your email marketing? Ensure these companies are all GDPR compliant, and that this is stated in your terms and conditions so the person is aware of where their data will be processed.

6 

All customers have a 'right to be forgotten'. Determine whether your data can be deleted. A person will be able to request their data to be deleted for no legitimate reason; if a person requests this you must remove them from all systems, unless the information is needed for tax purposes.

7 

Data portability allows individuals to obtain and reuse their personal data for their own purposes across different services, this information should be given free of charge. You must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

8 

You must document every sign up you receive and be able to prove that a person has opted-in to receive communication from you, this information must be given freely by the person so for example you cannot use pre-ticked boxes. If you do not have proof of this, each person should be contacted so proof is obtained. You should also document the path, so if a person signs up, unsubscribes and then signs up again this must be documented.

9 

Determine security controls. How is your data protected? Could a better process be put in place? And who has access to the data?

10 

Review the data breach plan. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

Do you need support with your email marketing and getting GDPR ready?
Get in touch with the PRG team today!