GDPR
COMPLIANCE IN 10 EASY STEPS

ADVENTURE

ARE YOU UNSURE HOW TO SHOW THAT YOU HAVE TAKEN GDPR SERIOUSLY AND TAKEN STEPS AND ACTIONS TO MAKE YOUR BUSINESS GDPR COMPLIANT?

The good news is it's very straightforward and easy to do.

The simple, easy trick that can save you time (and headaches) is to set up a GDPR folder for your own business.

We've mentioned this in lots of our blogs, but here we are going to tell you section by section how to create a GDPR folder that will help you comply with GDPR and give you a focus and format to manage your data in the future.

We think we have explained it as simply as possible but if you need any assistance or have any queries, please drop us a line here hello@adventuregraphics.co.uk, and we will be happy to help in any way we can. So grab a folder and set of 10 dividers and here we go!

TIP! Remember that every business is different, and you will know your company the best so you may want to adapt and change the headers but it will give you a starting point.

SECTION 1

PREPARATION FOR COMPLIANCE

- This is where you store the information you have found and the steps you have taken. These can be handwritten notes or printed information. It's anything you have considered, looked at, anything that could be useful to your business later on.

SECTION 2

DATA AND RISK AUDITS

- This is where you store the data and risk audits you have conducted.
  For a refresher, you can look at my blog
  https://adventuregraphics.co.uk/2018/03/16/gdpr-managing-your-data/.
  You can use the sections and turn them into a table to make it easier to complete.

- Not sure where to start with the audits? We can help you. Just get in touch now
  hello@adventuregraphics.co.uk

SECTION 3

LEGITIMATE INTEREST BALANCE TEST

- Legitimate interest assessments need to be completed if you contact people/businesses that you do not have a contractual or consensual basis to do so.

- It doesn't mean that you can't contact them, but you do have to have shown that you have applied a balance test to make sure it is appropriate, and in both your interests (not just yours), to do so.

SECTION 4

PRIVACY POLICY

- Here you can store your privacy policy for your records.
  Not got one yet? Here's what you need to include
  https://adventuregraphics.co.uk/2018/04/20/what-do-you-need-in-your-privacy-policy/

Finding this confusing? It is. Give us a call on 0121 354 1010, so we can have a chat and help you see the wood for the trees.

SECTION 5

DATA REQUESTS

- You now have 30 days to respond to a data request. Have you thought about the process you will follow or how you will verify their identity? A short process or document here will make it easier should you receive any such requests so, you have already given the process some thought. It also shows how seriously you are taking GDPR.

SECTION 6

DATA BREACH PROCESS

- IIf you have a data breach do you know what to do? You only have 72 hours to report the violation if you decide it is severe enough to let the ICO know. Even if you do not report it, you need to show you have investigated it, evaluated the impact of the risk and take actions to prevent the same breach occurring.

  Take a look at the reporting guidance from the ICO and make notes that would be relevant to your own business (the ICO reporting telephone line is also useful for you to store in this section. You can also download the reporting form, so you have it for your records.

  Visit https://ico.org.uk/for-organisations/report-a-breach/ for more information.
  If you would like us to set up a data request and breach process let us know.

SECTION 7

SUPPORTING PRIVACY POLICIES

- We all use software to help us process our data. Our email system, our accounts system, our automated emailers, google analytics. All businesses will use at least one package, which is fine. What is important however is that you have taken steps to ensure that these support packages are themselves GDPR compliant. The simplest way to do this is to either ask for confirmation from them directly or look at their privacy policy.

- In this section, you compile the replies to your emails or copies of their privacy policies for your evidence and GDPR compliance. A little tip here may be to file the name of the software and the link to their privacy to show that you have indeed investigated their GDPR commitment. We started printing off all of ours, and they are very long so to save the planet we stopped and made a note of the links and filed those in this section instead!

SECTION 8

INSURANCE AND ICO REGISTRATION

- Here is where you can store your insurance records and your ICO registration if you need to register. To find out if you are required to register take the ICO's little quiz **https://ico.org.uk/for…/data-protection-fee/self-assessment/**

SECTION 9

DATA AMENDMENTS AND DO NOT CONTACT LIST

Arguably the most important part of your folder and your GDPR compliance. This is where you will show you are taking GDPR seriously and thoroughly respecting the personal data you hold.

- This may be where you make a note that you improved your software security protection by signing up to a maintenance contract with a local IT company (you can also file a copy of the invoice/agreement here). Or it may be where you make a note that you deleted 18 cold leads as you feel they would no longer expect you to be in contact with them (maybe they were clients from quite a while ago, but you haven't worked together since). Or if you manually added someone to your newsletter subscription because they asked you. Or if you amended your privacy policy because you added some tracking software to your website.

- This does not need to be complicated. A simple table with date, action and reason would be sufficient. You need to have somewhere to record the what you do concerning the personal data you collect, store and use.

- The Do Not Contact list is self-explanatory. The problem with being asked not to contact them is that if you delete entirely, you may unintentionally re-contact them, especially if they fit your usual prospective customer avatar. Our solution is to make a note of the company name only on this list as we B2B. However, if you are B2C, this may be more complicated.

- It is only personal identifiable data that is covered by GDPR, therefore, your 'Do Not Contact' list will need to ensure that the information is as vague as possible to ensure that you do not contact them again.

- If you think a manual "Do Not Contact' list would be useful for your business you need to think of the least obtrusive and risky way of doing so.

SECTION 10

ANNUAL GDPR DATA REVIEWS

- The thing about GDPR is that it is not a 'one hit' wonder. You can't follow a checklist and then be compliant forever. It is an ongoing commitment that will change, adapt and evolve. So how as companies do we ensure that we consistently meeting GDPR and that what we were doing a year ago is still appropriate and lawful?

- We recommend that every 12 months you conduct a GDPR data review and record in this section when the review took place and the changes/ amendments that occurred as a result of the review. (If you handle significant amounts of data or your data is high risk you may want to start with six monthly reviews. This will depend on your type of business.)

- This would also be particularly useful to ensure that you are meeting the data retention guidelines you detailed in your privacy policy. For example that we store personal data of those who enquire for three years. An annual review would help you keep on top of this while you are perfecting the systems to achieve this.

- You could set up an annual review form that you follow, or if you are a very small business, a simple table format might be easier.

What we have to remember is that GDPR is very new and what we are doing now to become compliant may not be quite right in the long term, however, if you set yourself up a comprehensive GDPR folder based on the above the Information Commissioners Office (ICO) cannot fail to be impressed. If you need to make changes to your practices and policies in the future, there will be no doubt of your good and thorough intentions, at the beginning, and your approach to personal data.

Please note: we are not lawyers or GDPR experts, and we provide advice to the best of our knowledge based on the current information available and without prejudice. GDPR remains the ultimate responsibility of the business owner, and we encourage you to always do your research.

WISHING YOU GDPR SUCCESS!

NOW YOU HAVE THE INSIDE KNOWLEDGE.

If you would welcome some advice and guidance on your journey why not get in touch?

ADVENTURE

Give us a tinkle
0121 354 1010

Drop us an email
hello@adventuregraphics.co.uk

Take a look
www.adventuregraphics.co.uk

Come and meet us
Station House
Midland Drive
Sutton Coldfield
B72 1TU