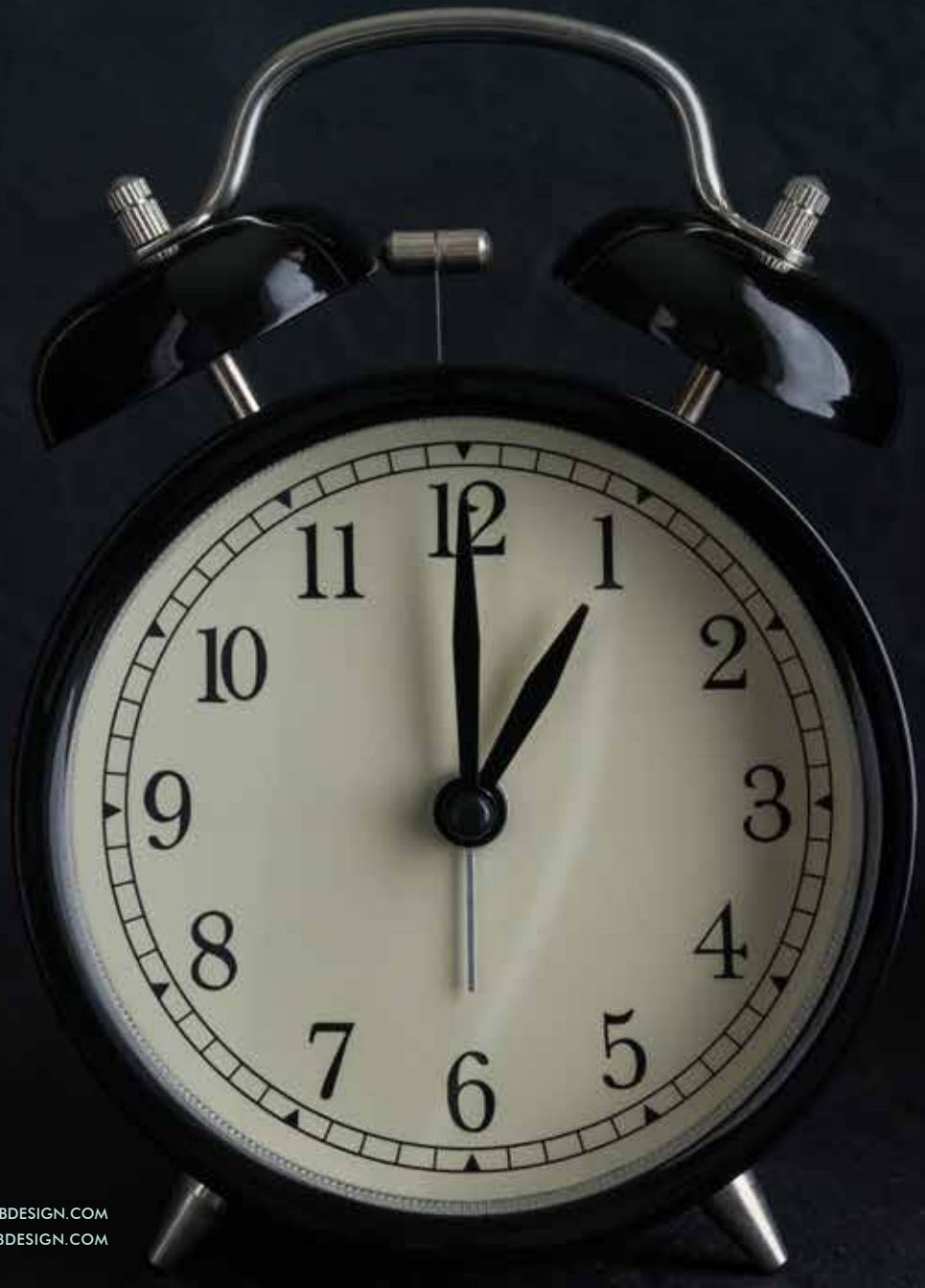
hendersonwebdesign

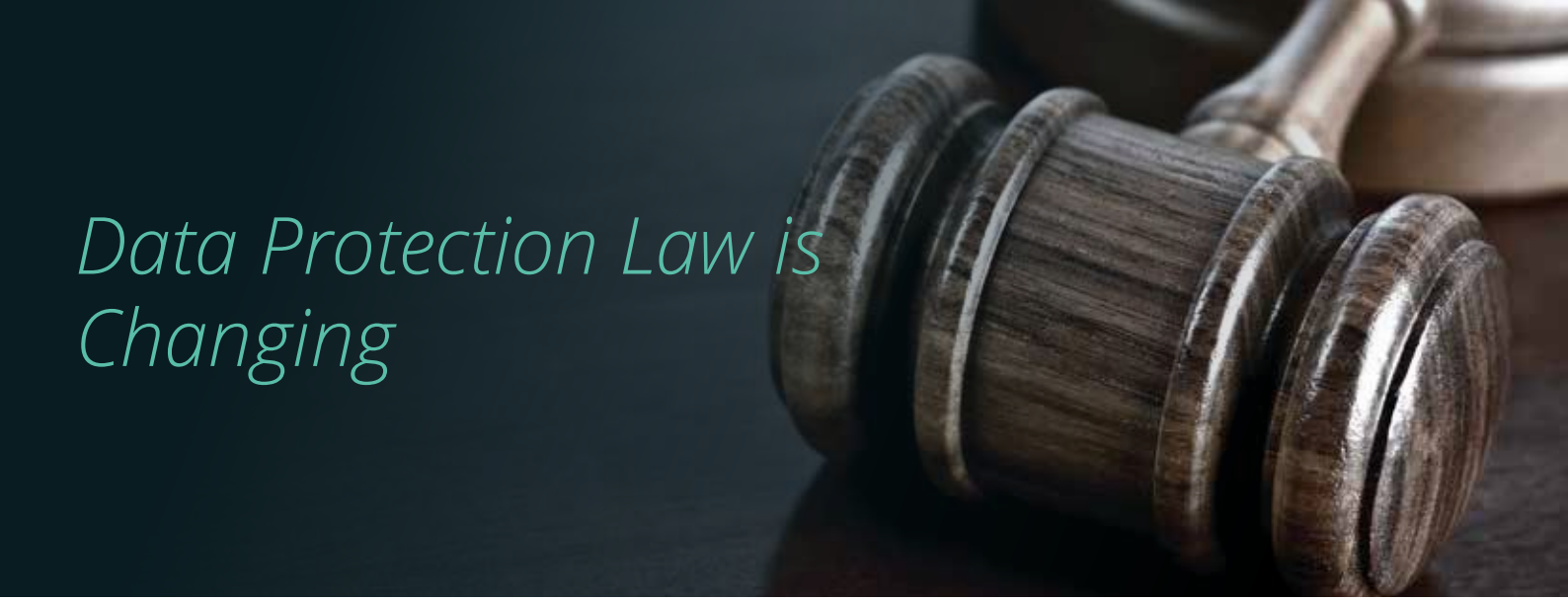
THE CLOCK IS TICKING!
GDPR is coming soon

Make sure your website is compliant



T: 01752 263 051
E: INFO@HENDERSONWEBDESIGN.COM
W: WWW.HENDERSONWEBDESIGN.COM

2 OSBORNE PLACE
LOCKYER STREET, THE HOE
PLYMOUTH, DEVON, PL1 2PU



Data Protection Law is Changing

From Fri 25th May 2018 the General Data Protection Regulations (GDPR) will come into force!

It affects all businesses, yours and mine. It's not just for big companies either. Even if you collect the most basic information from your website through a form, conduct any kind of digital marketing, send direct mail or make sales phone calls, you will be affected by this change.

Don't worry though, we are here to help!

We have produced this document to assist you in the easy steps that you can take, right now to ensure you are fully prepared come May 2018.

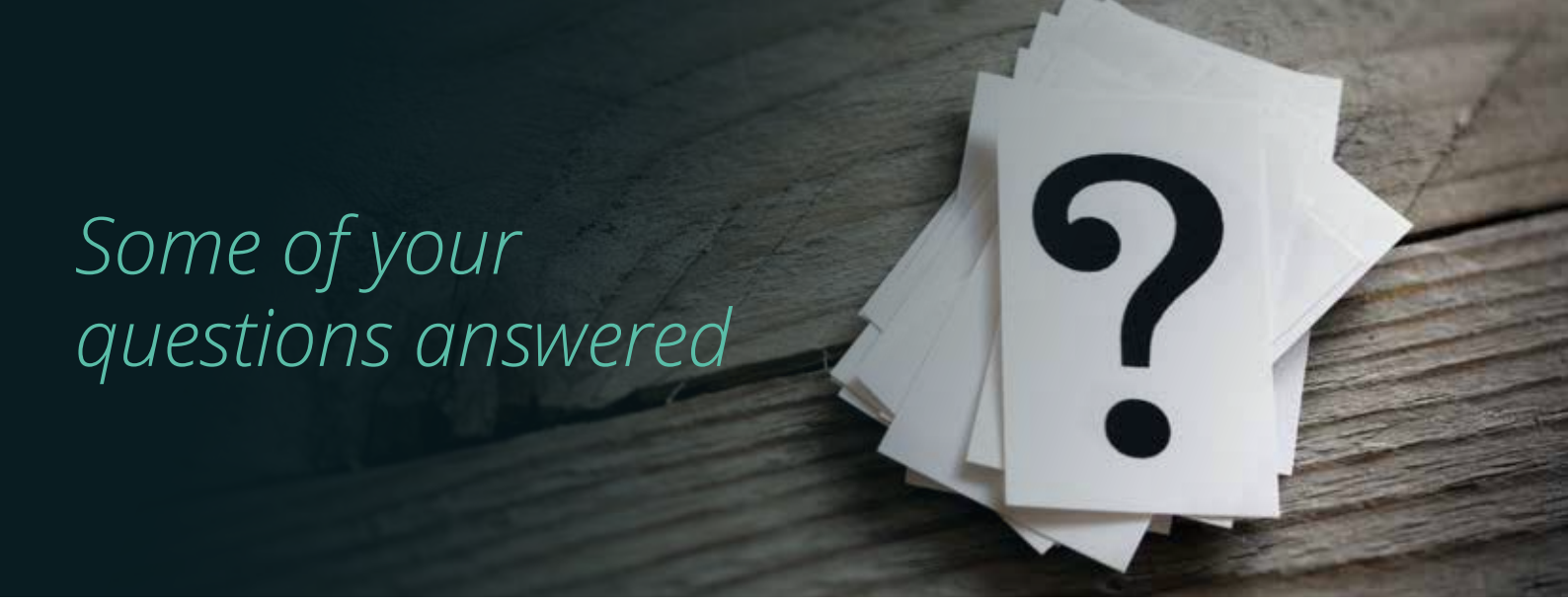
So what are the General Data Protection Regulations?

The General Data Protection Regulation (GDPR) is a new EU regulation aimed at helping to strengthen data protection for EU citizens and residents both within the EU and the wider world. In short, it is saying to businesses and organisations:

"If you want to offer your services or products to customers who are EU citizens or resident, then you need to ensure that you look after their personal data responsibly, or face the penalty!"

It affects any business or organisation that collects data of EU citizens & residents.

The GDPR law applies to data collected about EU citizens and residents from anywhere in the world. As a consequence, a website with any EU visitors or customers must comply with the GDPR, which means that virtually all websites and businesses must comply.



Some of your questions answered

Who does it affect?

Anyone who collects and processes personal data (as defined by the GDPR as a Data Controller) will be required to comply with the new regulations to a certain degree. As well as organisations who run websites or apps, this also includes any organisations who use internal databases, CRM systems or even simple email.

When does all this happen?

The GDPR comes into effect on the 25th May 2018 - so you have nearly 6 months to ensure your business or organisation is compliant and up to speed.

But we are leaving the EU aren't we?

The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Why now, what is the point?

The aim of the GDPR is to give citizens of the EU control over their personal data and change the approach of every organisation towards data privacy.

What are the penalties for non-compliance?

The penalties for non-compliance can be severe. "Under GDPR, organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements".

The GDPR provides much stronger rules than the existing Data Protection Act laws and significantly strengthens the requirement to gain consent for any form of Digital Marketing.

As a website owner what are my responsibilities?

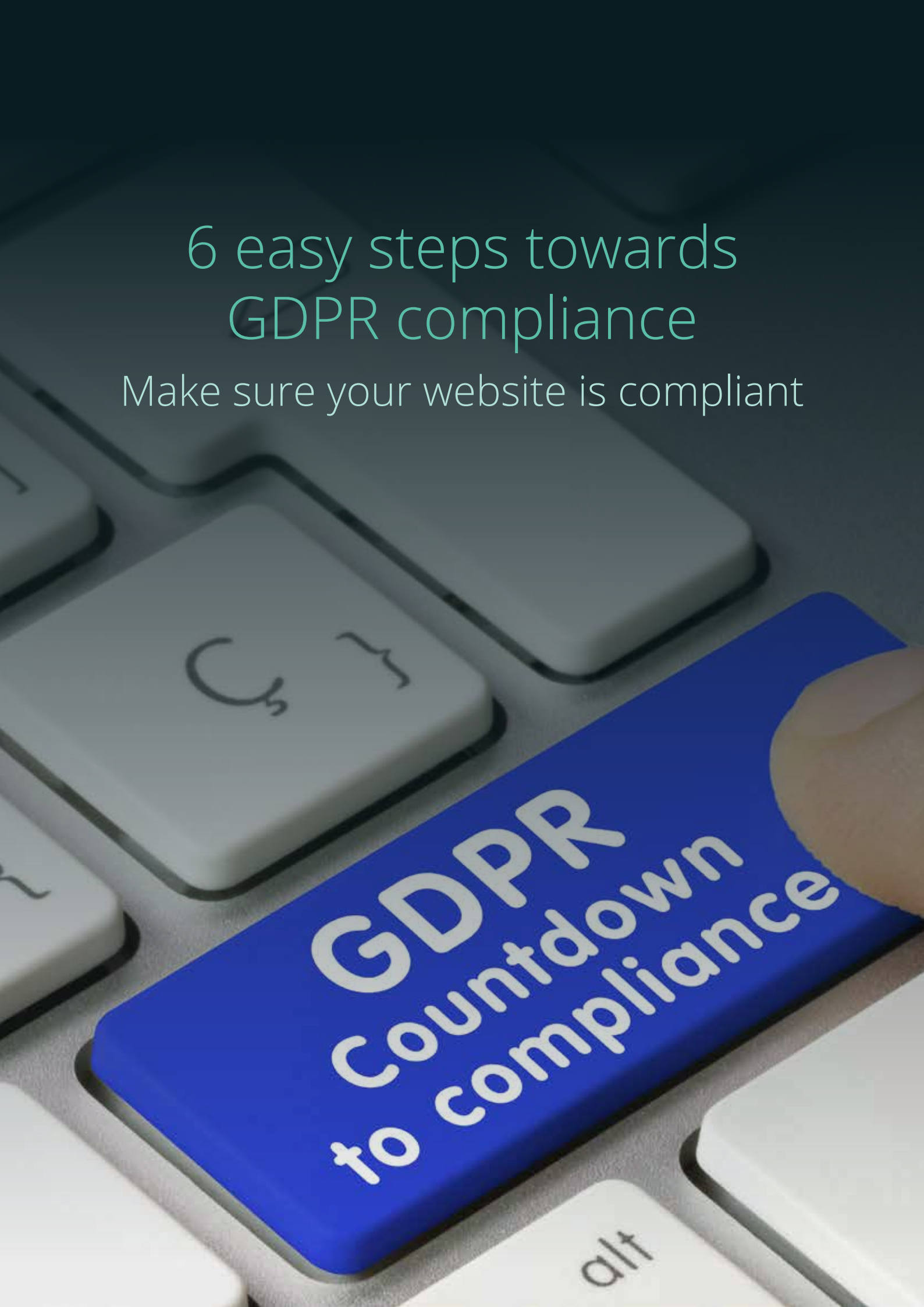
There are several. But don't worry, they are easy to implement if you plan ahead and act now.

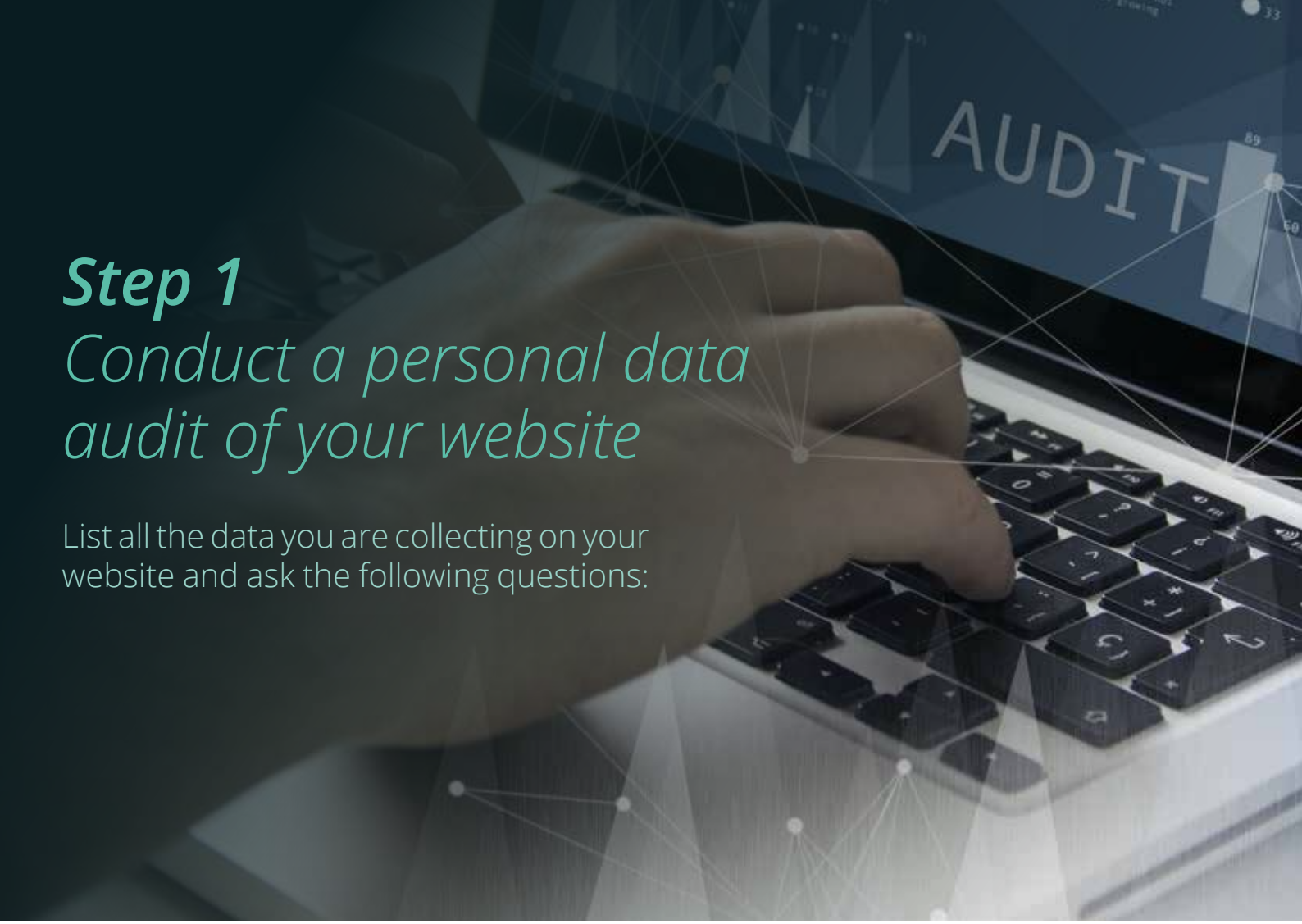
Over the next few pages we have provided you with a guide to your responsibilities, what you need to do, and when.

And we are here to help you!

6 easy steps towards GDPR compliance

Make sure your website is compliant





Step 1
Conduct a personal data audit of your website

List all the data you are collecting on your website and ask the following questions:

What data do I collect?

This can be personal data you collect and store through your own website or personal data collected by a 3rd party processor. For example:

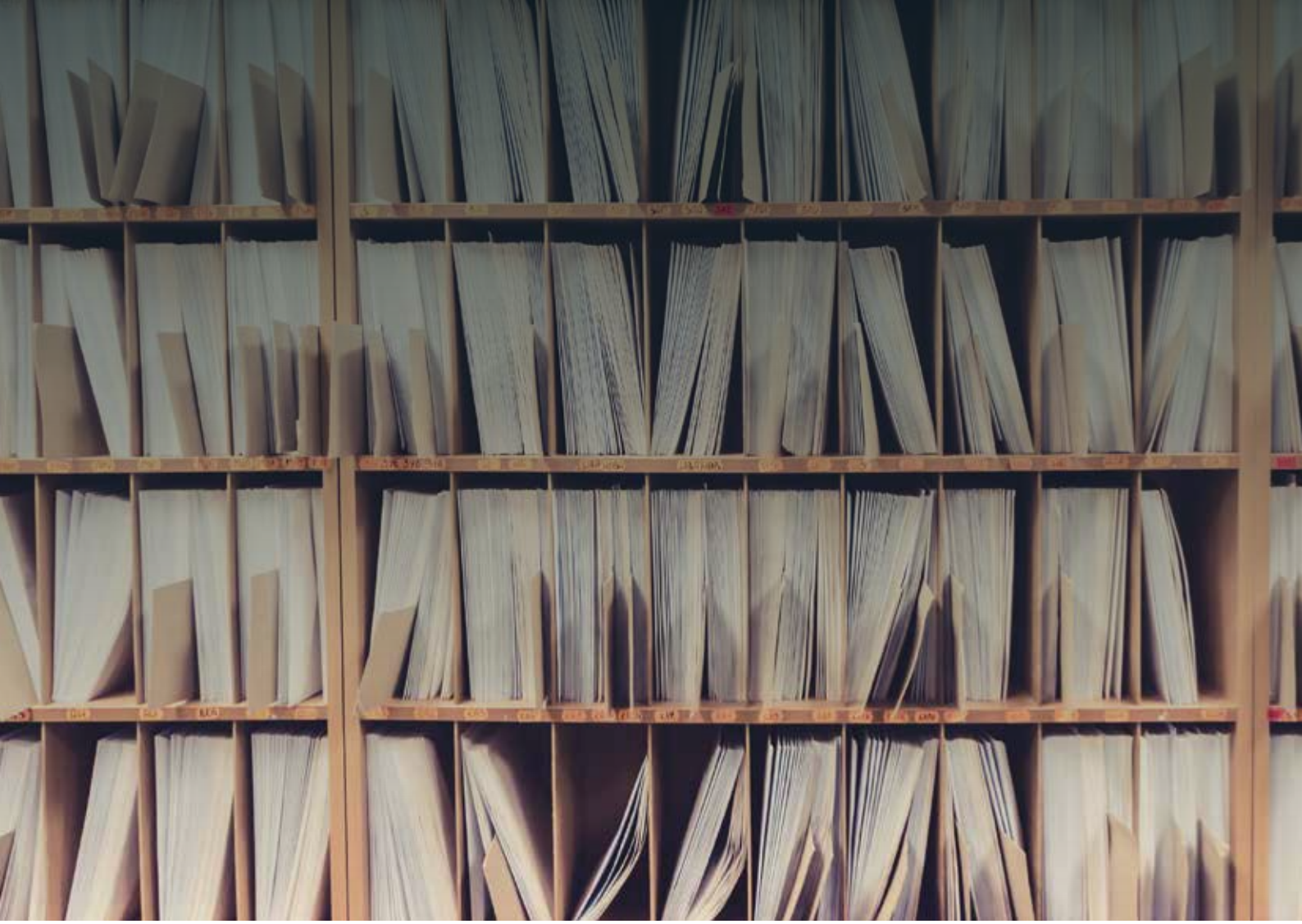
- Do you have a contact form collecting things like name, email address, telephone number, etc ?
- Do you collect personal details on a third party email marketing service like MailChimp ?
- Do you operate an online store and collect customer data for processing their orders ?
- Does your website hold any personal data of any kind?

If the answer is yes to any of the above. Where is the data being stored ?

For Example:

- Does your contact form store personal details on your website's database ?
- If your website has an e-commerce facility, personal customer information, details and orders are likely being stored in your website's database.

The data in the database itself is likely stored unencrypted so if the database was breached then the personal data could be exposed.



Do I really need all this data ?

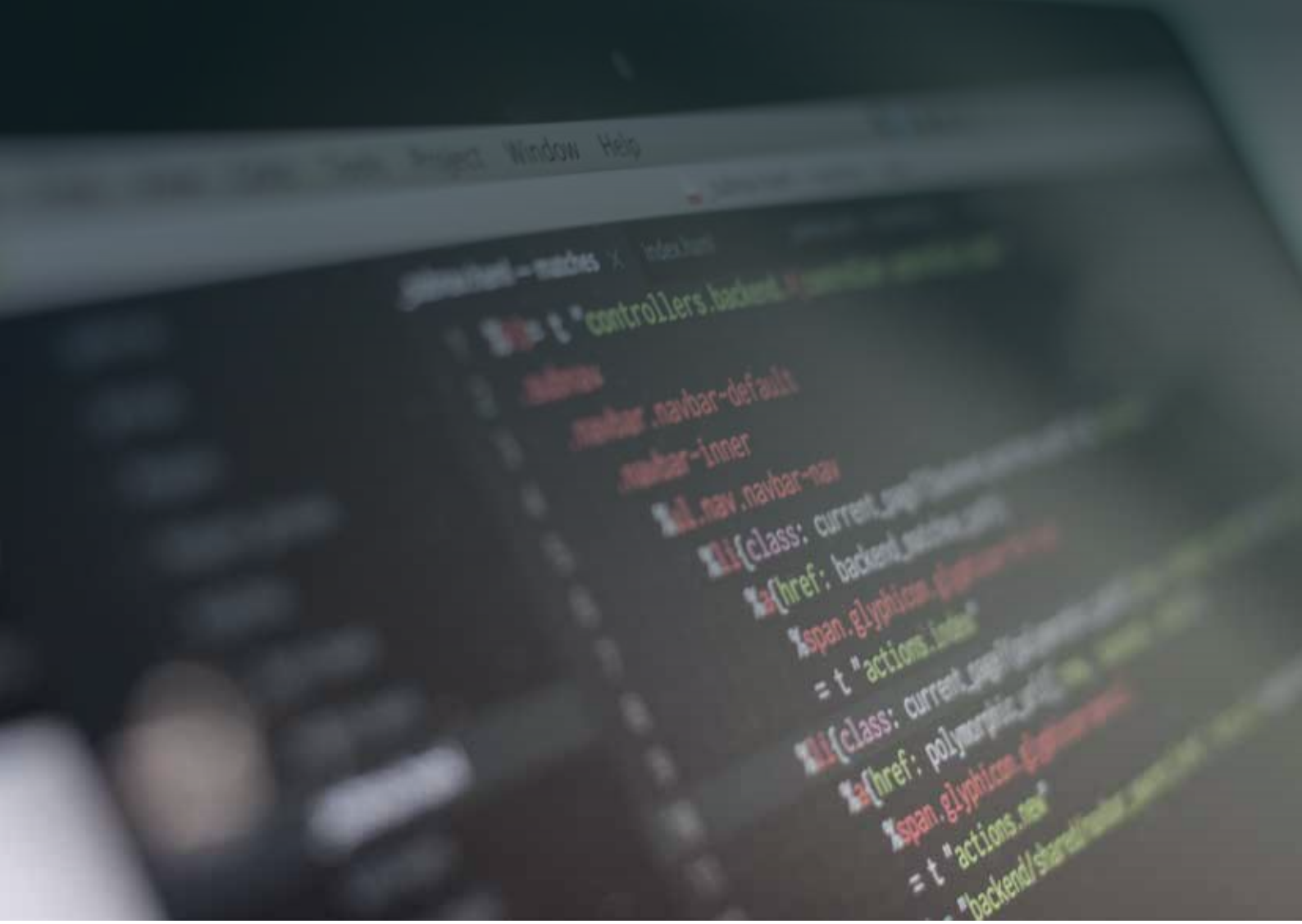
Limiting the personal information you collect and store also limits your potential for breach and non-compliance with GDPR. If you don't absolutely need to collect some of the personal information you currently collect and/or store on your website, you can either stop collecting it or stop storing it!

You may not process any data yourself, but you may keep personal data in 3rd Party programs like Payment Handlers, MailChimp or other online CRM systems.

The GDPR would call these systems third party data processors. They are processing the data controller's (that's you!) data on their behalf. Most (but certainly not all) of these systems are run by US-based companies who should be working towards GDPR compliance, if they have not already done so. US companies should also be Privacy Shield compliant. The US Privacy Shield framework has been co-developed by the US Department of Commerce and the European Commission to provide mechanisms to protect the flow of personal data between the EU and the US.

"Data processor" definition *"Data processor" in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. So, for example, an email marketing service such as MailChimp would be a 3rd party data processor as it holds and processes personal data on your behalf for the purpose of sending out communication emails.*

For each 3rd party data processor you should check their respective privacy policy and make sure they are GDPR compliant.



Step 2
Modify your website

If you have a Web Form of any size, that you collect individuals data and you intend to use this for future marketing, you must:

- Explicitly ask permission to send someone email marketing. This can be achieved by having a 'Check Box' with a statement asking permission to use the individual's details for marketing purposes. They must opt in. It's not OK to assume you have permission. It's not OK to hide it in your privacy policy. And it's not OK to pre-tick a box which people have to untick.

- If you store personal data in a database within your website, you must ensure its security.

We can make your web forms compliant from **£75 each**

Step 3
Write a Privacy Policy

Ensure your website features a privacy policy page, informing users how the data you collect will be stored and used, how they can request access to their data and how they can request to withdraw consent for their data to be stored and used. You can look at our privacy policy on our website (we can provide a template to assist you in drafting your own Privacy Policy).

If you are unsure about what your privacy policy should say, we have examples but....we are not Solicitors....so please seek legal advice.

We can add a Privacy Policy Page from **£75**

Step 4
Implement an SSL Certificate

Websites that use HTTPS send data over an encrypted connection so if your website has an SSL certificate it is a useful step towards GDPR compliance. Without HTTPS, any data, for example from a contact form, is sent "in clear" and could therefore be read if intercepted. If you would like more information about SSL certificates and HTTPS please give us a call.

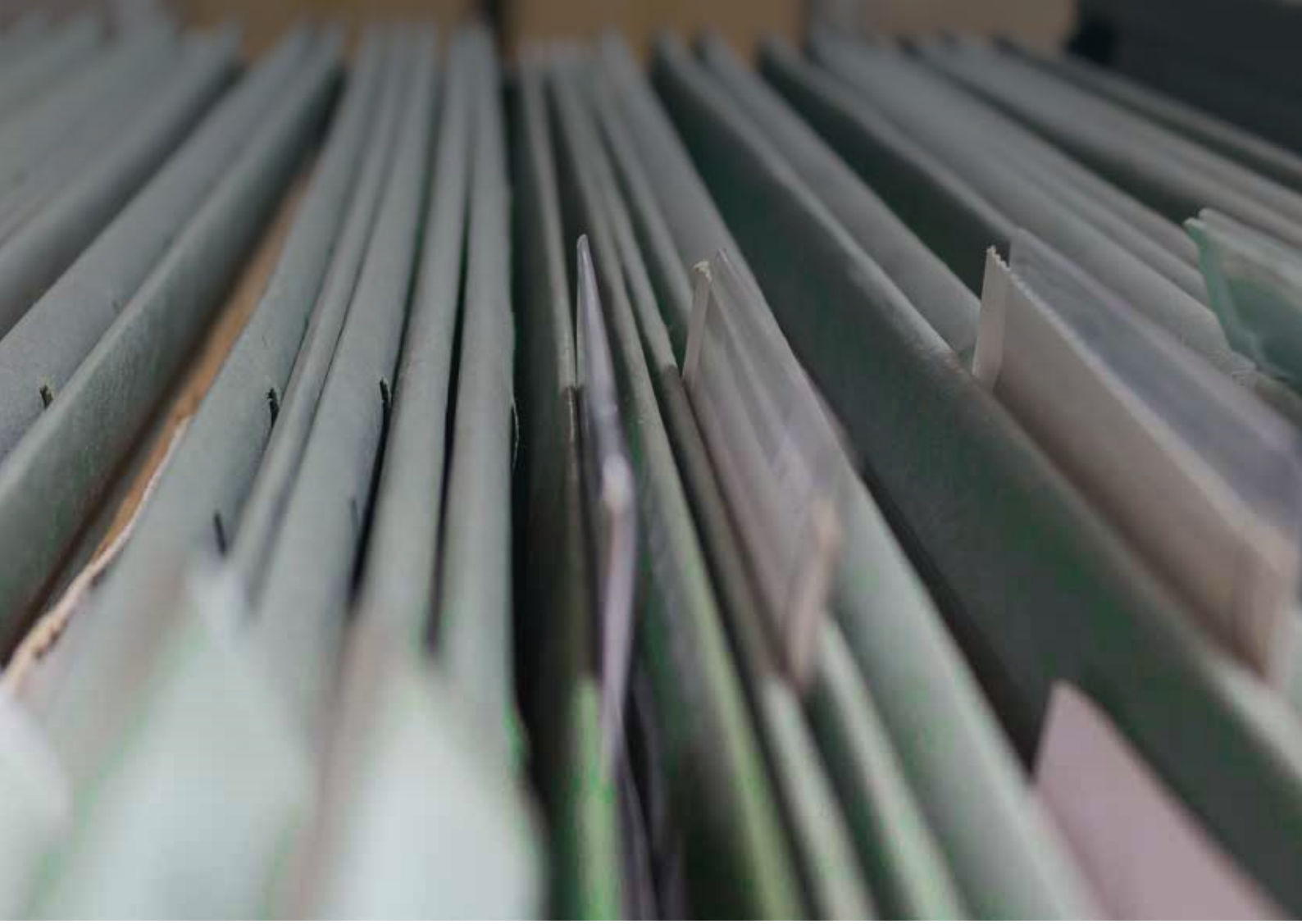
We can purchase, install and manage your SSL for as little as **£75 per year**

Step 5

Understand data breach reporting requirements

The GDPR requires the data controller (that's you!) to have suitable processes defined and in place in case of a data breach. Depending on the severity of the breach, the data controller has a legal obligation to report a data breach within 72 hours.

Whilst we can't help you with this bit, further information on the reporting of a data breach can be found on the Information Commissioner's Office website. **www.ico.org.uk**



Step 6
Keep consistent and detailed records

All data controllers must keep detailed records of:

- All individuals who have given explicit permission for their details to be used for marketing purposes.
- All individuals who have opted out.

This should include details of what the user explicitly consented to, and what the method was used to provide consent (e.g. web form checkbox).

Summary of your responsibilities

In short, you need to:

1. Ensure you have an up to date Privacy Policy.
2. Ensure your website has an SSL Certificate to encrypt any data that your website transmits.
3. Ensure any web form has an opt-in checkbox for marketing and make sure that you keep detailed records of the those who have opted in, what they have opted in for and those who have not.
4. Provide users with a method to withdraw consent and purge personal data collected on them. This is called “Right to Be Forgotten”.
5. Have a means or process for users to request access and view the data you have collected on them.

Do you have a website?

NO → *NO! Maybe you should, give us a call we can help with that one. 01752 263051*

YES

Does your website have an SSL Certificate?

NO → *Visitors will be told that your website is insecure! Plus, you need to be GDPR Compliant.*

YES

Does your website have a form which collects personal information of any kind?

NO → *You may not now, but you might in the future. Why not build an email list ?*
We can help. 01752 263051

YES

Do you have a Privacy Policy in place?

NO → *You definitely need one! Whether you collect data on your website or not.*

YES

Do you ask users to opt-in to digital marketing?

NO → *You need to, GDPR states you must have explicit opt-in permission?*

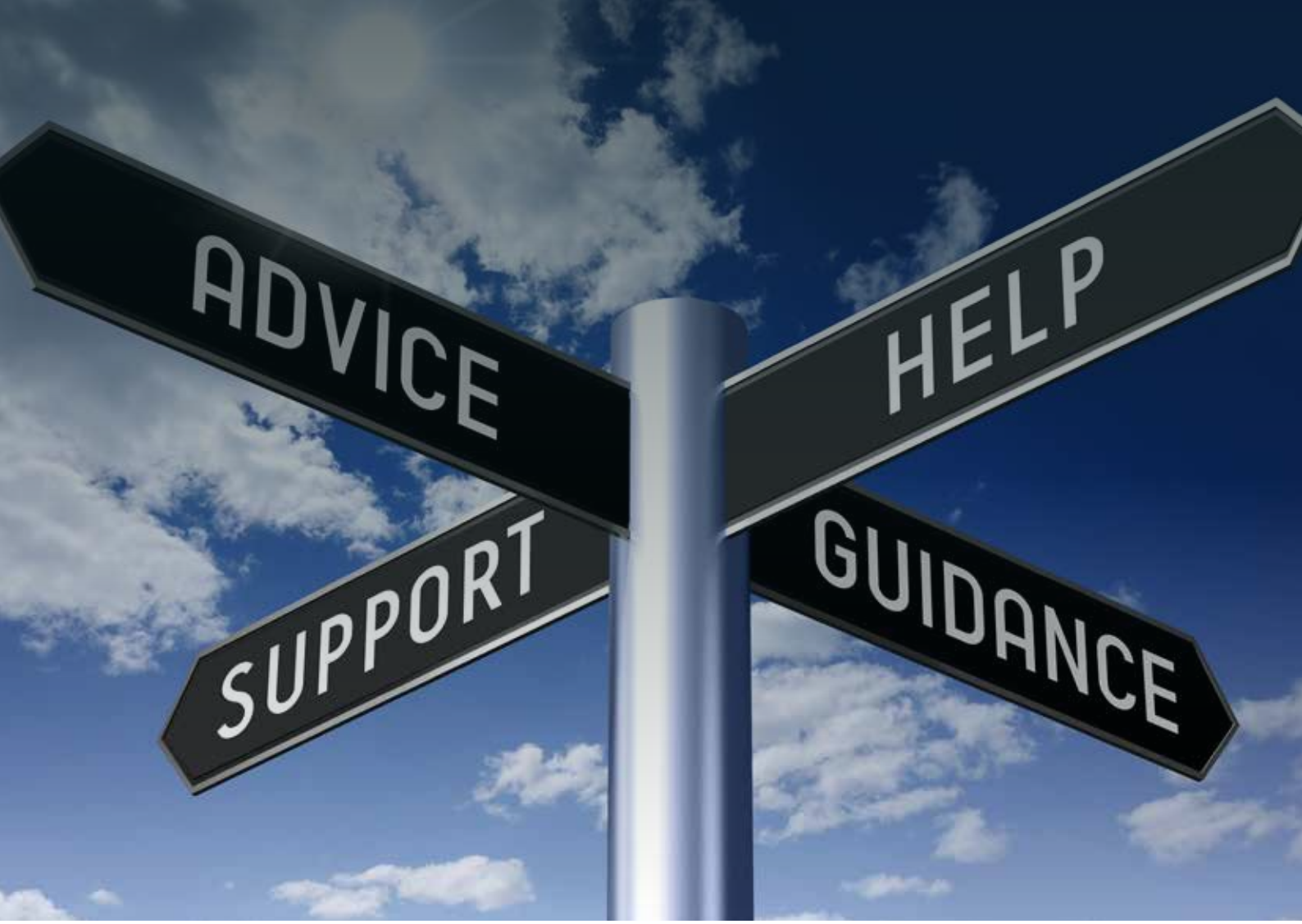
YES

Do you make it easy for users to opt-out or to obtain the data you hold on them when requested?

NO → *You need to!*
This should be explained in your Privacy Policy.
If you send out marketing emails you must have an unsubscribe/opt-out process.

YES

WOW...that's great!
You have everything covered.



Don't worry, we can help

Conduct a full website Audit on your behalf	£50 per website
Create a Privacy Policy Page on your website *(We can help with the text too)*	from £75 per page
Adjust any existing forms on your website with the relevant check box.	from £75 per site*

Options for your SSL Certificate

SSL Certificate Standard - Single Domain	£75 (including install)
SSL Certificate - Multiple Domains (up to 5)	£150 + £25 per site on set up
SSL Certificate - Multiple Domains (up to 10)	£200 + £25 per site on set up
SSL Certificate - Wildcard (unlimited sub-domains)	£240

Note: *All SSL Certificates are invoiced on an annual basis and are subject to VAT*
** Depends upon the number of forms your website has and whether they are linked to your T & C's.*

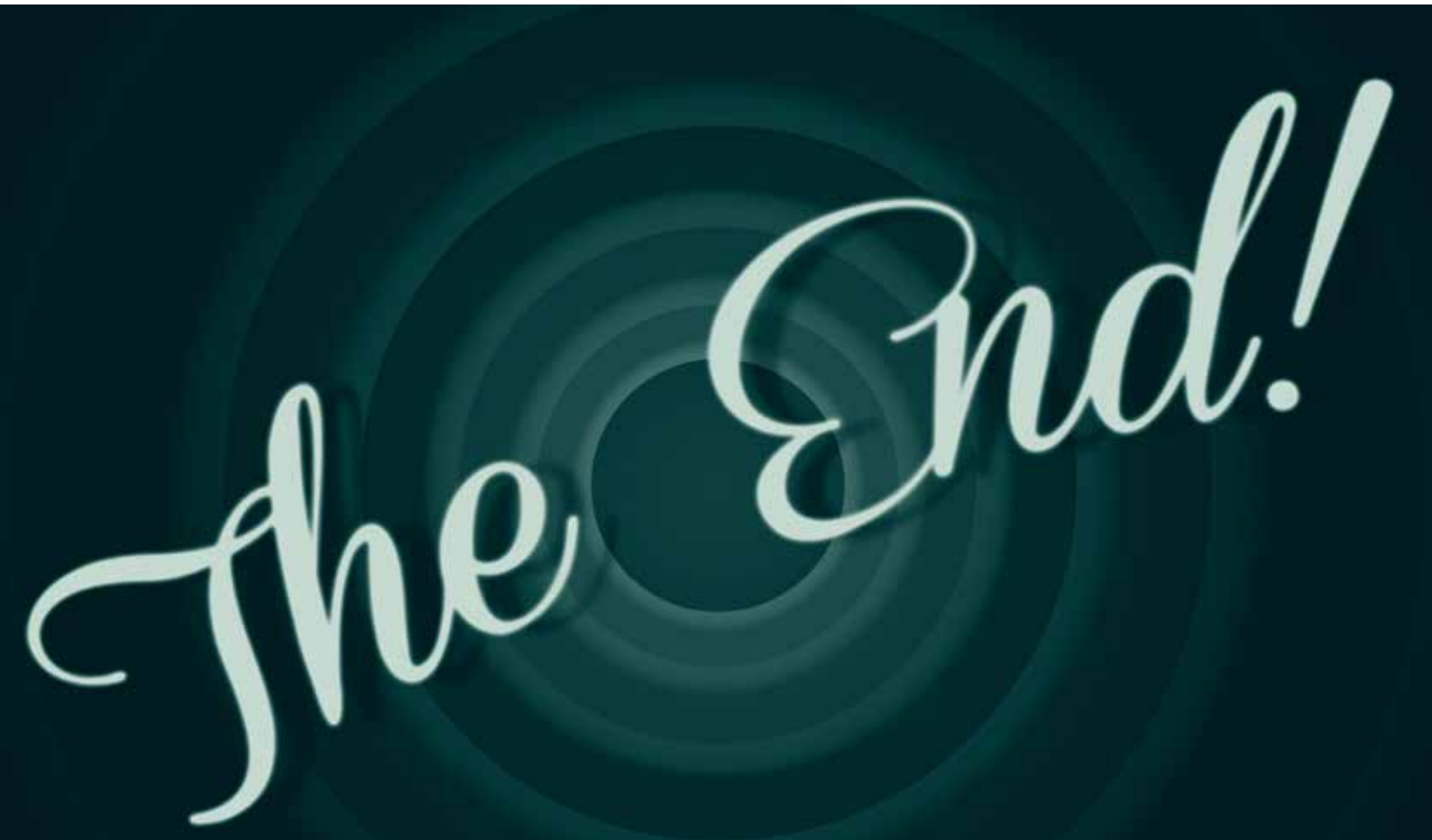
And Finally.....

There is a lot to take in...we are here to help...if in doubt call us on **01752 263051** and we will assist where we can. In the meantime here are some useful resources for you:

Information Commissioner's Office: **www.ico.org.uk**
This is the organisation who are responsible for the enforcement of these regulations, upholding the law and issuing fines.

They are taking this very seriously....so are we....and so should you.

*Call us now on **01752 263051** and lets talk about how we can assist you meet your obligations now! Don't wait until May 2018!*



T: 01752 263 051
E: INFO@HENDERSONWEBDESIGN.COM
W: WWW.HENDERSONWEBDESIGN.COM

hendersonwebdesign

2 OSBORNE PLACE
LOCKYER STREET, THE HOE
PLYMOUTH, DEVON, PL1 2PU

Registered No: 4794550 Registered in England and Wales VAT Number: 865 0800 26