11 THINGS

TO CONSIDER WHEN GETTING

GDPR READY

digital willow

A WORD FROM US

Hello there,

As you may know, Digital Willow is a growth marketing agency. We help clients generate leads and obtain more customers.

When we first heard of GDPR we looked at the way it would impact us and started the process of getting compliant. During this process we realised just **how in-depth this topic can be and how complicated it is for small to medium-sized businesses.** So much so, that we had to employ the help of a full-time data scientist.
We figured that there must be others just like us, trying to navigate the road to compliance. As such, **we put together this eBook in the hope that some of the lessons we have learned may help your business too.**

This is an eBook to **address the importance of GDPR** and the main points you could be looking at when protecting personal data from your clients.

Note that we do not claim to be giving you the ultimate guide to be fully compliant with GDPR, we do advise your business to reach legal support for that.

We hope you like this content and we wish you the best of luck getting GDPR ready.

Amber Williamson

1. UNDERSTANDING YOUR DATA'S JOURNEY

Compile a report on the information that you hold or collect, how it goes through your systems, and how you share it. Here are some questions you should consider:

Where does the information come from?

- Is it a data capture form on your website?
- Do you use a lead provider?

What information do you collect?

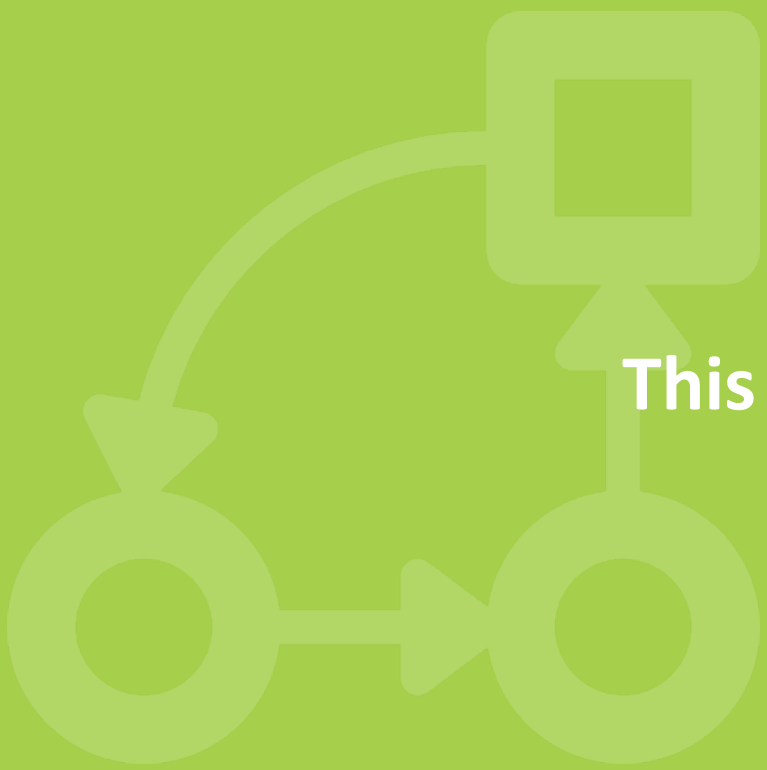
- Personal information such as name, email address, age, gender, income level.

How do you store this information?

- Cloud servers, documents, your personal computer?

Who do you share this information with?

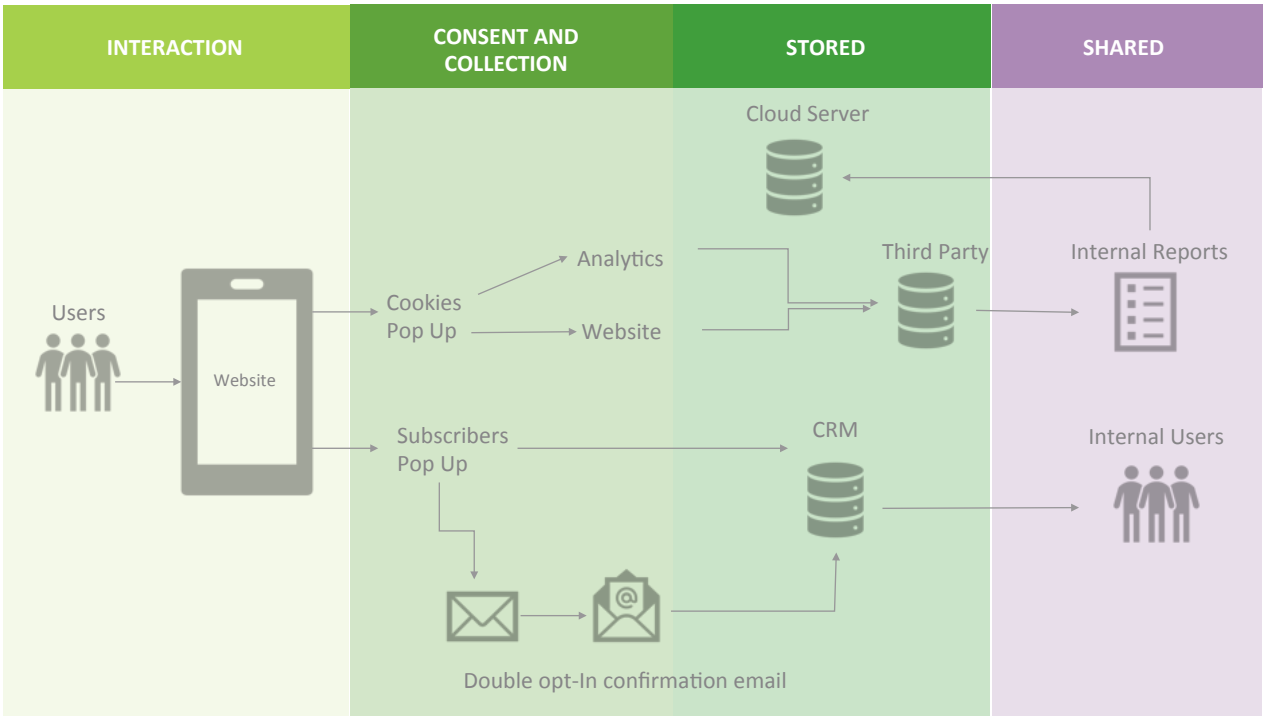
- Other departments, clients, staff, other agencies?



This is the start of your information audit.

2. DOCUMENT THAT DATA

Create a flow chart mapping all of your findings from step 1.



Tip

GDPR's accountability principle requires you to show how you comply – having this map in place will help you achieve this.

3. HAVE A REASON FOR DATA COLLECTION AND PROCESSING

You must have a lawful basis to process data and it **must be clearly stated in your procedures and privacy policies.**

There are 6 lawful bases:

1. Consent: you have been given clear consent

2. Contract: necessary for a contract, or because they have asked you

3.Legal obligation: necessary to comply with the law

4.Vital interests: processing is necessary to protect someone's life

5. Public task: it is necessary to perform a task in the interest of the public

6. Legitimate interests: the processing is necessary for your legitimate interest or the interests of a third party unless there is a good reason to protect the individual's personal data which overrides the legitimate interest

Tip

It is wise to choose early on why you are processing data and not change it later without good reason.

4. OBTAINING CONSENT

The use of subscriptions, emails, and cookies to collect data needs consent from the user. To collect consent you need to have systems in place to gather and record it.

- Keep your consent separate from your T&Cs.
- Avoid making consent a precondition of use.
- Ensure you have an opt-in box that is NOT prefilled. For example, the user has to tick notification requests by themselves. This is the affirmative action needed for consent.
- Be specific on what the user is consenting to.
- Name your business and third party organisations that will rely on this consent. *For instance, when sharing data with another department such as sales or marketing, it is best practice to list these in the consent form.*
- Keep a record of consent; what they consented to, when, and how they were told.
- Ensure individuals know they can withdraw consent at any time.

Tip

Your responsibility does not end once you have the initial consent – you will need to keep it up to date.

Always review consent and policies to ensure your processes, products or services haven't changed; if they do, ensure you get consent again.

5. REGISTERING WITH THE ICO

- In some cases you may need to register with the ICO.
- Data protection officers (DPO) may be required to ensure you are compliant, although you may not need to appoint a DPO if your company has less than 250 employees.

The ICO has a self-assessment tool to determine whether you need to register.

You can find it on the link below:

https://ico.org.uk

6. PRIVACY POLICIES

Things you may want to include in your privacy policy are:

- Your company name.
- Your lawful reason for collecting data and processing it.
- Your business reasons for processing data.
- The ways you collect the data.
- The way you store such data.
- The way you share and disclose data.
- If you anonymise data, disclose this.
- Include the users' right to the following:
  - Right to access
  - Right to erasure
  - Right to rectification
  - Right to restrict processing
  - Right to object
  - Right to data portability
  - Right to automated decision making including profiling

Tip

Make this document jargon free, accessible and understandable for everyone, not just your audience.

7. DEMONSTRATING COMPLIANCE AND ACCOUNTABILITY

A data protection policy outlines key points such **as the changing of passwords, how they will be stored, how you will monitor access and when you plan to review your procedures.**

Within the policy, outline **induction training and regular data protection training** for your teams as well as any impact assessments you plan to do.

Have a data sharing agreement as a standalone document; this will be your guide to a third party processor. It will outline how they are to deal with your data and security and assurances they must have in place. You are liable for your processor's approach to the use of your data.

Complete an information risk assessment

Showing an understanding of risk is important. You need to identify possible areas where information will be at risk and have appropriate actions in place to reduce this risk.

All information you collect from your customers is valuable - do you have a policy about taking information out of the office? There has been many cases of confidential information being left on trains and planes for example, putting companies and people at risk.

8. PROTECTION BY DESIGN

Look at ways you can naturally protect data by designing your processes around minimising exposure, such as limiting staff's access to certain data.

Completing data protection impact assessments will allow you to update your risk assessment, help you fix problems, and help reduce the risk of additional costs and reputation damage.

9. SECURITY AND PROTECTION

Ensuring you have good security for your IT systems is a must; they must be kept up to date, patched and secured whenever you are processing or storing data.

If you store data via the cloud you need to make sure your access points are monitored and remain secure.

10. TRANSFERRING DATA OUTSIDE THE EU

The EU imposes restrictions on the transference of information outside the EU to third countries or international companies.

Personal data may only be transferred outside the EU in compliance with the conditions for transferring data outside the EU.

To find out more please visit the following link:
Chapter V of the GDPR.

11. BREACH NOTIFICATION

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

ico.

You may have to consider notifying the ICO if a breach is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you may have to notify those concerned directly and without undue delay.

In all cases, you must maintain records of personal data breaches, whether they were notifiable to the ICO or not.

To learn more about our GDPR journey, please do get in touch.

Amber Williamson
amberw@digitalwillow.biz