GDPR & Mailing

Today's to-do list
We are going to look at GDPR. How GDPR affects the way you take and hold data on a website and we are going to take a quick look at privacy policies and then the practical part of your session will be focused on mailing lists and Mailerlite.

Learning objectives:
By the end of this session, you will
Understand what GDPR means for businesses.
Identify how to take and manage viewers' data.
Know what content you should include in a privacy policy.
Be able to connect your site to a mailing programme.

GDPR - **what it means to business.**
Has anyone heard of GDPR? A few years ago, it was all anyone was talking about.

GDPR came in to increase the privacy of people's data. To be honest, it didn't work the way it should have worked. The people that were doing it properly carried on doing it properly and the people that weren't just moved their operations outside the UK where the restrictions didn't apply. People like us spent a week adding disclaimers to hundreds of websites, privacy policies and GDPR compliance notices that no one ever read. The basic premise is that people have the right to control their data. How long it's kept, what it's used for and how it's provided. In the real world, it means that you can only use data for the purpose it's been supplied for.

Under the terms of GDPR, not only will organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners – or face penalties for not doing so. If you are going to be providing social media services to businesses then you need to be aware of the rules, how to use their data, personal information you might hold, usernames, and passwords. If you have access to the back of a clients website or their social media platforms then you need to make sure you are dealing with their private information like orders and messages in the appropriate way.

GDPR checklist – things you should check.
1. **Know your data.**
2. **Identify when you're relying on consent.**
3. **Review your security measures.**
4. **Meet access requests.**
5. **Train your employees.**
6. **Conduct due diligence on your supply chain.**
7. **Regularly review your privacy policies.**
8. **Check if you need to employ a Data Protection Officer.**

There are 7 key principles.

1. Personal data must be processed lawfully, fairly, and in a transparent manner

This is probably the most important requirement. To comply, you must provide people with the name of your business, and details of how their information will be used. You should make it clear that the individual can access and correct the information that you hold about them and how they can go about it.

You must also tell them if the information will be used in any way that's not immediately obvious. If you are going to pass their details on to a credit reference agency as part of the service, couriers for delivery information.

2. Personal data must be processed for specified, explicit, and legitimate purposes

You must be clear about why you are collecting someone's data and how you intend to use it.

You can't use the data collected for any other purpose than the one you are stating and asking permission for. You can't meet someone at a networking event and then add them to a mailing list and if your purpose changes over time and this is not compatible with the original purpose, you will need to get the individual's specific consent for the new purpose. For example, if you are sending a newsletter out about a bookkeeping service that the person has signed up for then you stop that service and start selling beard oil, you will need to ask their permission to mail them about your new product. Just because you have their details, doesn't give you the right to email them about something completely different.

3. Personal data must be adequate, relevant, and not excessive

You should only collect the bare minimum; you can't collect information that isn't immediately relevant to the specified purpose, and you may not collect more information than you need. So, if all you are doing is posting out an order to the customer, all you need is their address and a contact number for the courier. You don't need to know their favourite colour and the name of their first pet.

4. Personal data must be accurate and up to date

Any information you hold must be factually accurate and updated where necessary. Depending on the nature of your business, you may need to develop mechanisms that allow people to update their details quickly. Most web platforms allow people to access their data and edit or delete it where appropriate.

5. Personal data shouldn't be kept any longer than is necessary

This principle states that you shouldn't keep data any longer than you need to. If you collected data for a purpose that's time-limited then you should make sure that the information isn't retained beyond that point. Reducing how long you hold data also helps

you to reduce the risk of storing personal data that's inaccurate or out of date or it getting leaked if your system has a breach.

It's good practice to tell people how long you intend to keep the data and you might find it useful to set retention periods for your data. Again, most web platforms allow you to delete data after a certain fixed length of time.

6. Personal data must be processed securely

You must take adequate steps to maintain the integrity and confidentiality of personal data. Having an information security policy in place can help demonstrate that you're looking after personal data and reducing the risk of it being compromised. That means no sticky notes with customers card numbers on stuck to the wall or desk. You might think that's ridiculous, but I've seen it happen so many times.

7. The controller is responsible for GDPR and must demonstrate compliance

This final principle sets out the law when it comes to accountability. As a data controller, you're responsible for what you do with personal data and must demonstrate how you're looking after people's privacy. If you are the only person in your business, you are automatically the data controller. It's not just a title handed out in a big company. It applies to everyone.

More information on the GDPR principles can be found on the ICO website. You can also survey to see just what you need to do to comply.

Here are some key things to think about when it comes to collecting individual data:

- Check your consent practices and existing records – and refresh them where necessary.
- Offer people genuine choice and control.
- Where using an opt-in, don't rely on pre-ticked boxes or default options.
- Explicit consent means a very clear, specific statement of consent.
- Keep your consent requests separate from other terms and conditions be specific, granular, clear, and concise.
- Name any third parties who will rely on the consent.
- Make it easy for people to withdraw consent (and tell them how).
- Keep evidence of the consent (who, when, how, and what you have told people).
- Avoid making consent a precondition of your business services.

So, in basic terms you can't:
Add people to a mailing list without consent.
Sell or provide their data to anyone else.
Harvest contacts for mailers.
Pre-populate consent. For example, for the 'would you like to be added to our mailer' yes or no, you can't tick yes as default and then tell them to untick the box. It's all about choice.

If you are going to send out newsletters or mailers then make sure you use something like MailChimp or Mailerlite that includes all the appropriate consent sections and unsubscribes. Believe it or not, some people make a living from trawling websites and tripping businesses up on GDPR rules and claiming compensation.

Privacy Policies

GDPR means we all need to now include a Privacy Policy on our website somewhere. Most of the platforms include some form of generic privacy policy although these don't always meet the UK GDPR requirements. In essence, a Privacy Policy should outline what you collect, how it is stored, how it is used and how it is maintained. Although you can combine them, it is usually better to have a separate Cookie and Privacy Policy and we will look at cookies in more detail later in the course.

Depending on what you are doing/selling/servicing you will need to make sure that the information in your Privacy Policy accurately details how any data is held. For example, if the site is for a life coach or mentor then you will need to identify how the client's private details and session information will be held. A Privacy Policy should be about the business as a whole, it's not just how the data is dealt with on the website but the business in its entirety.

There are some links and examples in today's useful links download, make sure you take a look as it will form part of tomorrows coursework.

Practical - Mailerlite

For the rest of the session we are going to look at mailing lists and how to collect data properly and how to embed these features into our sites. There are several different platforms available to you for collecting data and creating mailing lists. Two of the biggest Mailchimp and Mailerlite also offer you a powerful set of tools to build landing pages, create pop up sign ups and automate mailings to customers to encourage repeat purchases and upsells.

We are going to explore Mailerlite, the tools it contains and we are going to add some functionality to our sites with newsletter signups.

Todays Task

Create a MailerLite Account
Create a subscribe form
Embed the form on your website using the HTML block editor

MailerLite

If you don't already have one, lets go to https://mailerlite.com/signup and create a new account. You can use your google or Microsoft account or an email address and password. There is a limit to the type of email accounts you can use. You can't use outlook.com or Hotmail.com, but you can use a gmail account. There are issues with that though, and you are restricted on what you can do. For today that doesn't really matter.

Account Settings

Domain Verification & Authentication
Familiarise yourself with the settings. Not all will be available to you at this point.

Create a Form
The slides show the following actions:
Create a form
Create a Group
Card Type
Form Design
Content
Signup
Privacy Policy
Confirmation Checkbox
Marketing Permissions
reCAPTCHA
Interest Groups
Custom Success Page
Success Message or Redirect
Signup Form Created

I like to have a short discussion about 'Best Practice' vs 'User Experience' when looking at all the options. I will usually just use one message and reCAPTCHA.

Form Overview
Double opt-in is another 'Best Practice' option. Even though you have asked them to confirm and tick a box on sign up, this option will then send them an email asking if they are really sure they want the emails. The problem is in real life a lot of subscribers don't reply to the message. We once had 20 signups and only 2 replied to the opt-in email! Below that button is a 'Share URL' button. This will share the form in a page on its own. It can be really useful to share on socials.

Copy the Code
On the bottom half of the page is the 'Embed form into your website' box. We will want to **COPY** the **HTML Code**

Embed on Website
In our block editor we want to add this to our footer.
NOTE: It's the HTML code not the 'Share URL' code

Final words
Quick whiz around the room, any comments on today, what do you feel you have learnt?

Extra help
If you need any help with anything from today's session, feel free to message me in the WhatsApp group. If you have any other issues or problems related to the course or the tools speak to Andrew and Irfana, they are here to help you.

Up next
See you next week when we start on Elementor. Don't forget your coursework assignment tomorrow and carry on with your project as much as you can!