GDPR & Policies

Today's to-do list
We are going to start today with your mini-session on GDPR. We are going to look at 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.

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

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.

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 isn't 'compatible 'with the original purpose, you'll need to get the individual's specific consent for the new purpose.

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

You should only collect the bare minimum; you may not collect information that isn't immediately relevant to the specified purpose, and you may not collect more information than you need.

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.

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've 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. So, 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 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.

Practical Brief

You have completed all your sessions and practice builds now so we want you to decide on which platform you want to use to develop your portfolio website for your Skills Bootcamp Project. We want you to make a start and put together your portfolio site based on the site plan you created in your first week. Start adding your work from your previous sessions and linking to the test sites you have built with descriptions of what you did and why. This site should showcase your work and skills during the sessions.

What we want to see:

- Pick at least 2 communication methods to include
- Consider GDPR and Privacy Policies and how data is going to be collected
- The key site elements, strong navigation, home page and portfolio and blog elements that you will add to over the next few weeks.

You can use any of the platforms that you choose, it is totally up to you which one you want to build your site in. Email us screenshots or links to the relevant pages to dms4alltrainers@gmail.com

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.