GDPR: General Data Protection Regulation

General Data Protection Regulation

The General Data Protection Regulation (GDPR) legislation will apply to all the personal data you have on record as a business. The new legislation takes effect from the 25th May 2018. This legislation is replacing the Data Protection Act (DPA) of 1998.

GDPR will affect all UK businesses that process or store personal data, and your beauty business will be one of these, so you will have to comply with the GDPR.

This course will guide you through the stages of ensuring you comply with the GDPR.

Introduction

This course is split into 12 steps which have then been divided into 4 modules. The 12 steps this course will guide you through are the Information Commissioner's Office (ICO) recommended steps that all businesses should take to ensure that they are GDPR compliant.

We have divided this course into 4 modules as a way to ensure that the course is presented in manageable chunks. After each module you will be examined on what you have learnt. You also have the option of downloading a checklist as part of this course, the checklist can be used to demonstrate that your business has taken all of the necessary steps towards becoming GDPR compliant. Other course downloads are also available to help you.

What is GDPR?

The General Data Protection Regulation (GDPR) legislation will apply to all the personal data you have on record as a business. The new legislation takes effect from the 25th May 2018. This legislation is replacing the Data Protection Act (DPA) of 1998.

These regulations are designed to safeguard personal data, such as the information kept on client record cards. This balances the needs of businesses to collect and use this information against the right of the individuals' privacy.

The new legislation gives more rights and control to individuals, meaning that businesses will have to be prepared to fulfil more varied requests from individuals with regards to their data within tighter time frames than previously.

What is the ICO?

ICO stands for Information Commissioner's Office. The ICO is an independent authority in the UK that reports directly to parliament and is sponsored by the government but is not directly a part of it. It upholds information rights, helping to protect data privacy for individuals and to promote transparency and openness on the part of the organizations that collect and process personal information.

What are the 12 steps?

What are the 12 steps according to the ICO?

1. Awareness - Ensuring the right people know about the changes that will be happening.
2. Information you hold - Understanding what information you hold and what you do with it.
3. Communicating privacy information - Reviewing your privacy notices.
4. Individual's rights - Understanding the rights people now have and ensuring you can comply with these rights.
5. Subject access requests - Making sure that you can respond to requests relating to personal data within the new timescales.
6. Lawful basis for processing personal data - You'll need to identify your lawful reason for processing data.
7. Consent - Review the way you ask for, record and manage consent to make sure you are GDPR compliant.
8. Children - Verifying individual's ages and understanding when you'll need parents' or guardian's consent to process data.
9. Data breaches - Knowing who to report a data breach to and in what time frame.
10. Data Protection by Design and Data Protection Impact Assessments - Considering data protection from the beginning of any new IT project.
11. Data Protection Officers - Do you need to appoint one?
12. International - For businesses based in more than one country.

Why should I comply?

Heavy fines could apply if you fail to comply with the new regulations by the 25th May 2018. Depending on the severity of the violation, you can be fined:

Up to 20,000,000 euros or 4% of your annual global turnover - whichever is greater

Moreover, knowing that you will correctly manage their data will give your clients the confidence to disclose their personal information to you.

<u>Step 1: Awareness</u>

You will need to ensure that everyone working in your business is aware of the basics of data protection policy, the changes that are happening to this policy when the GDPR takes effect and how this affects the data they handle within their role.

Business owners and managers will need to understand the impact the GDPR will have on the business.

Your business should have an appropriate data protection policy. The way in which you handle data and your security controls should be reviewed regularly. Your business' compliance with the GDPR should also be reviewed regularly.

Step 2: Information Auditing

What is an information audit?

An information audit is a process in which you, as an organization, ask yourselves a series of questions about how and why you store and process personal data and what the data in question is. You'll need to document your responses to these types of questions.

Why do I have to do an information audit?

You don't have to, but it would be a very good idea and is strongly recommended. It will help you to understand what your current processes are and why they are as they are. The main purpose of asking yourself these questions is to uncover anything you might be doing which will become unlawful when the GDPR comes into effect so that you can change these processes to GDPR compliant ones.

Step 2: Information Auditing

What kind of questions should I ask myself about my business?

What data does our company hold?

Where is this data stored? Is this place secure?

Why are we storing this data and what are we using it for? Are all of our uses legitimate and necessary?

Who has access to our data? Is it completely necessary for everyone who has access to have access?

How long do we retain data for? How long do we need to retain it for?

What is our lawful basis for processing data? (see part 6)

Step 3: Privacy Notices

At present, when collecting a client's personal data you have to give them certain information, including your identity and how you will use their information. Normally, a privacy notice is provided which explains this.

Under the GDPR it will be necessary for you to make some changes to your privacy notices as there will be additional information you need to give your clients in order to comply with the new legislation.

Step 3: Privacy Notices

Your privacy notices should already state:

Who you are

What you will do with the client's information

Who their information will be shared with

You will need to add the following things to your privacy notices in clear, concise and easy to understand language.

What your lawful basis for processing data is

How long you will retain the client's data for

That your client can complain to the ICO if they believe you are not handling their data correctly

You can find an example GDPR compliant privacy notice in the course downloads.

You can find an example GDPR compliant privacy notice in the course downloads.