Guide to Understanding

GDPR

GENERAL DATA PROTECTION REGULATION

Contents

Disclaimer:
Important. This document is purely for guidance and does not constitute legal advice or legal analysis. All organisations that process or control data need to be aware that the General Data Protection Regulation will apply directly to them. The responsibility to become familiar with the Regulation and comply with its provisions from 25th May 2018 onwards, therefore, lies with the practice. This guide is intended as a starting point only, and organisations may need to seek independent legal advice when reviewing or developing their own processes and procedures or dealing with specific legal issues or queries.

Section 1 -
LEARNING ABOUT GDPR

1 Introduction to GDPR

GDPR is a new data regulation that came into place on 25th of May 2018 across Europe which aims to unify how consumers' personal data is protected in EU member states. It also aims to create more transparency about how businesses are storing and using people's personal data. This is particularly interesting in the Medical Aesthetics industry, as your practice collects so much personal data from contact details, through to medication records and allergies.

What is GDPR and why will it affect my business?

It replaces the Data Protection Act 1998. In the last 20 years the volume and ease of access to information about us has increased exponentially. This has become an intrusive fact of life. The GDPR is being introduced to give a new protection against the new modalities of identifying facts about individuals. It applies to all human interactions and most importantly it applies to medical practice. This guide contains information meant to help you prepare your practice, and guides you on how to be GDPR compliant for your clients', team's and business's prosperity and success.

Don't worry, we are here to guide you!

GDPR is based on a number of principles.

- There needs to be transparency for data subjects.
- The practice must have a legitimate purpose for processing the data in its possession.
- The data must be limited and relevant to a specific purpose.
- The data collection must be accurate and fit for purpose.
- The data storage must not be replicated.
- The information must be erased when no longer required.
- There must be good governance of the data set.
- It aims to give control to citizens over their personal data.
- It brings a new set of digital rights for those living in the EU.
- It gives a new recognition to the economic value of personal data in the digital age.

Personal data is any information relating to an individual whether it relates to his or her private, professional, or public life. In Ireland the Data Protection Commissioner is responsible for supervising data protection in Ireland.

Don’t worry, It’s not as scary as it sounds!

GDPR is a dense piece of legislation, but there is some good news. Firstly, we are here to help you become GDPR compliant. You are giving your clients peace of mind that their data is safe and not being used for spammy marketing and or being given to other third parties. By being prepared and putting good practices in place you can build credibility and integrity in terms of how you care for your clients, and of course, their personal details.

Does Brexit affect me?

GDPR is EU-wide. The reality is that if the UK leaves the EU, it will effectively have to implement a carbon-copy legislation that will likely be called something else. Why? Simply because GDPR requires you to not just protect the data of clients in your own country, but internationally also e.g. companies that export into other countries. If the UK continues to trade with other EU countries post-Brexit, then they will need to have data-protection to the level of GDPR in order to trade with the other GDPR regulated countries. Prepare yourself for whatever inevitable data policy they implement post-Brexit.

Section 1 -
LEARNING ABOUT GDPR

2 What data in medical aesthetic practices is affected by GDPR?

GDPR affects personal data and special category personal data.

What exactly is personal data?

Personal data can identify a living person and it includes a subject's name, phone number, bank details, and medical history. Any personal information related to a person such as:

- Name
- Date of birth
- PPS number
- Home address
- Phone number.
- Next of kin, their contact details.
- Bank details.
- Photographs that can identify an individual.

What is considered special category personal data?

Special category personal data is about sensitive information. It relates to the patient's physical, mental or sexual health. Other sensitive data include religion, membership of a trade union, or past legal history. The processing of special category data will be prohibited unless the data subject has given his/her explicit consent.

Additional care must be taken when processing the following:

- Health assessment
- Medical details (skin conditions, medication)
- List of medications
- Religion

As you can see, every day you collect clients personal data, which all has to be stored in a specific way to be GDPR compliant.

Section 1 -
LEARNING ABOUT GDPR

3 Who is responsible for what in GDPR?

There are two core parties responsible for data protection with GDPR .

1. **The ‘data controller’**
2. **The ‘data processor’**

In your practice, you are the controller. You collect the data and choose how that data is collected and how to use that data for treatment plans, marketing, retail promotions, etc.

In other words, you are making decisions on how your clients’ personal data should be collected and used.

Phorest Salon Software **IRE: 01 8747800 is a data processor.** It is a tool that can help you process this data. Clinics, salons and medical practices using this software are using it to process and collect the personal data.

Section 2 -
BECOMING GDPR COMPLIANT

4 Becoming GDPR compliant

For GDPR, your practice must prove it has a legal basis for collecting the client's personal information. Meaning you cannot collect personal information without reason or simply say it is for marketing (more on this later in 'Consent').

Also, you must be able to:

- Identify exactly what personal information you are collecting.
- Give a legal reason for taking that information e.g. the reason for asking about allergies could be for performing patch tests.
- Show that all of the processes you have for collecting data are GDPR compliant e.g. if a client makes a complaint to a data protection agency, you need to be able to prove how you collected, stored and used their data in detail.

Section 2 -
BECOMING GDPR COMPLIANT

5 Accountability

GDPR penalties and fines
Go to https://www.itgovernance.co.uk/dpa-and-gdpr-penalties to find out about potential fines the government can impose.

You need a proactive approach to show you are data compliant. This is necessary for any audits or should a client complain.

In order to demonstrate compliance, you need documents such as a **data protection policy and a data-handling procedures manual**. This is required in the event of an audit.

Most importantly, you must have a record of consent proving the client opted-in to give you the data and the following details must be available regarding data on inspection:

- ❏ Why do you hold it?
- ❏ How did you obtain it?
- ❏ For what reason did you obtain it?
- ❏ Is the data secure?
- ❏ Who has access to it?
- ❏ Where do you store it?
- ❏ Do you still need it?
- ❏ How long will you hold it for?
- ❏ Do other third parties have access to it?

The maximum fine under the GDPR is up to 4% of annual global turnover or €20 million – whichever is greater – for organisations that infringe its requirements.

However, not all GDPR infringements lead to fines.
How are GDPR fines applied?

When deciding whether to impose a fine and to what level, supervisory authorities must consider a range of factors:

1. The nature, severity and duration of the GDPR infringement.
2. Whether the infringement was caused intentionally or by negligence.
3. Any action taken by the organisation to mitigate the damage suffered by individuals.
4. Technical and organisational measures that have been implemented by the organisation.
5. Any previous infringements by the organisation.
6. The degree of cooperation with the regulator to remedy the infringement.
7. The types of personal data involved.
8. How the regulator found out about the infringement, and the extent of any notification by the controller or processor.
9. Adherence to approved codes of conduct or certification schemes.

Section 2 -
BECOMING GDPR COMPLIANT

6 Consent

Previously, as the company collecting the data, it was ok to have a check-box at the bottom on your website or consultation forms saying 'I want to receive marketing, offers and other updates from your salon'. This is not sufficient anymore.

You may even have seen some examples that were pre checked i.e. you had to untick them to opt-out. With GDPR, this all has to change.

- ❏ You are required on forms to clearly outline all processing of the collected data i.e. what exactly will the data be used for.
- ❏ This must be stated in your terms and conditions and readily accessible.
- ❏ One checkbox for all data collection is not acceptable.
- ❏ **You cannot pre-check boxes and ask clients to opt-out.**
- ❏ **They have to opt-in.**
- ❏ Clients must have the ability to request that ALL of their information is deleted.
- ❏ You must have an audit trail of how the information was collected and that the client explicit opted-in.

Section 2 -
BECOMING GDPR COMPLIANT

7 Greater Rights of the Individual Under GDPR

The principle behind data protection is that personal data always belongs to the data subject no matter who it is shared with.

Clients of your practice will have ALL of the following rights under GDPR legislation and you must uphold them by being GDPR compliant:

A. The right to be informed. Clients must be informed before personal data is gathered. It must be **opt-in** and the reasons for gathering personal data must be provided.

B. The right of access. Clients have the right to request access to their personal data and for information on how their information is used after it has been gathered.

C. The right to rectification. Clients can have their personal data corrected if it's incomplete, incorrect or out of date.

D. The right to be forgotten. If clients are no longer customers or withdraw their consent to use their personal data, they retain the right to have their personal data deleted.

E. The right to data portability. Clients have the right to request that you transfer their personal data to another business in a commonly used and readable format.

F. The right to object to processing and direct marketing. Clients can request their personal data is not used for processing. Their personal data can remain in place but not used.

G. The right to be notified. Clients have the right to be informed of a breach of their data within 72 hours of its discovery.

Section 2 -
BECOMING GDPR COMPLIANT

8 GDPR Training & Development

While this guide gives you a basic overview of GDPR, you really need to have an in-depth understanding of the legislation and it is advised that you explore GDPR training for your team by a certified expert.

The legislation needs to be taken into consideration when making business decisions for your practice for the future. Becoming GDPR compliant is an ongoing process.

If you bring the team on training, it is recommended that you appoint a ‘GDPR Guide” for the business. This is a person on the team that owns GDPR compliance and educates, helps and works with others on the team to understand and work within the guidelines. Human error is the cause of the majority of data breaches.

Examples of data breach include:

- ➢ Mishandling paper files containing customer data
- ➢ Loss or theft of hard copy notes, USB drives, computers or mobile devices
- ➢ Sending an email to the wrong person.
- ➢ A bulk email using 'to' or 'cc', but where 'bcc' (blind carbon-copy) should have been used.
- ➢ a disgruntled employee copying a list of contacts for their personal use
- ➢ a break-in at the office where personnel files are kept in unlocked storage

Section 2 - BECOMING GDPR COMPLIANT

9 Children in Your Salon

Children are considered vulnerable individuals and are afforded specific protection under GDPR. If a child is under 16 years of age, you must obtain consent from the child's parent or legal guardian to collect and process their data.

A. Consent of the child and a parent or guardian must be obtained before collecting any personal data from children.

B. As health data is considered sensitive personal data and is subject to additional restrictions, you could avoid offering services to a minor that would require them to collect health information.

C. Practices who do offer these services to minors should seek additional, professional guidance on the matter.

D. It is good practice to design forms specifically for bookings taken from minors to ensure you implement additional safeguards.

Section 2 - BECOMING GDPR COMPLIANT

10 Clients Requesting a Copy of Their Data Under GDPR Legislation

A 'SAR' is a 'Subject Access Request'

Your clients can request a SAR under GDPR.
A 'SAR' is a 'Subject Access Request', meaning you have to produce ALL information you hold on the client to that person free of charge within 30 days.

Items covered in this would have to include (but not limited to):

1. All medical, contact etc. data you hold on the client
2. Why you hold that information
3. All activity and processing you are using it for
4. People you have sent or shared the data with (if consent was provided)
5. How you collected the data
6. Copy of the consent provided from that client
7. How long you have held it for, and how long you intend to hold it in the future if the client has requested the 'Right to be forgotten'.