



The Salon Owner's
Guide to
Understanding &
Preparing for

GDPR

www.salonGDPR.com

Contents

SECTION 1: Learning About GDPR

- 1 Introduction to GDPR
- 2 What data in salons is affected by GDPR?
- 3 Who is responsible for what?

SECTION 2: Becoming GDPR Compliant

- 4 Becoming GDPR compliant
- 5 Accountability
- 6 Consent
- 7 Greater rights of the individual under GDPR
- 8 Getting GDPR training
- 9 Children in the salon
- 10 Clients requesting a copy of their data under GDPR legislation

Back Cover: Learning About GDPR

- 11 How Phorest can help you become more GDPR compliant

.....

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 Salon. 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

If your salon is in Europe, you probably have been hearing the letters GDPR at events, online and all over the media. We are hoping to help you navigate this new data legislation, the 'General Data Protection Regulation', in a way that is easy to understand. This guide contains information meant to help you prepare your salon for the inevitable launch of it in May 2018, and guides you on how to be 'on top of it' for your clients', team's and business's prosperity and success.

What is GDPR and why will it affect my business?

GDPR is a new data regulation coming into place in 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 hair and beauty industry, as your salon collects so much personal data from contact details, through to medication records and allergies.

That is why, together, we need to get prepared and get it right from the get-go. Worry not, we are here to guide you!



But my salon is in Britain, and Brexit is likely to go ahead so... does it apply to 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.

In other words, prepare now for GDPR if you are in Britain, and you are preparing yourself for whatever inevitable data policy they implement post-Brexit.

There are already lots of data-protection laws, why worry about this one?

GDPR is more comprehensive than any other data-protection law. There are a few reasons you need to really pay extra attention to it:

- > You can be fined up to 4% of revenue capped at 20 million euro e.g. if your salon's turnover is €385,000 you could pay a fine of over €15,000.
- > Closer to the time, each country will be pushed by the EU to advertise in mainstream media, making people aware of their rights in terms of how businesses like your salon use their personal data. This will heighten consumer-awareness, and you need to protect your business by being able to answer clients' questions and prove you are handling their data in a secure and GDPR compliant way.

This sounds like a lot of work, and kind of scary...

GDPR is a DENSE piece of legislation, but there is some good news. Firstly, we are here to help you become GDPR compliant (see back cover).

Plus, salons that are GDPR compliant by May have the advantage of giving their clients peace of mind that their data is safe and not being used for spammy marketing and/or by other third parties.

Those who are prepared, can turn this into an advantage by further building credibility and integrity in terms of how you care for your clients, and of course, their personal details.



Section 1 - LEARNING ABOUT GDPR

2 | What data in salons is affected by GDPR?

GDPR predominantly affects 'personal data'. So, in a salon, what exactly is personal data?

- > Any information related to a person, for example name, date of birth, PPS number, address and medical details
- > A phone number or photograph that can identify an individual is also considered personal data
- > Medical details (skin conditions, medication) constitutes sensitive personal data and additional care must be taken when processing it. It is vital for staff to understand the financial and reputational consequences that may occur as a result of its mishandling

So, as you can see, you are currently collecting a lot of data that GDPR applies to!

Section 1 - LEARNING ABOUT GDPR

3 | Who is responsible for what in GDPR?

There are two core parties responsible for data protection with GDPR - the 'data controller' and then the 'data processor'.

As a salon, **you are the controller**. You collect the data and choose how that data is collected and how to use that data for styles, colours, treatments, 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 is a processor, as it is a tool that can help you do this. Salons using our software are using it to process and collect the personal data.

THIS IS WHY IT IS CRITICALLY IMPORTANT TO USE A FULLY GDPR-COMPLIANT SALON SOFTWARE.



Reach out to Phorest Salon Software's grow team today and

Learn How We Can Help You Become GDPR Compliant

UK: 0207 100 9290 / IRE: 01 8747800

www.phorest.com



Let's Grow!

Section 2 - BECOMING GDPR COMPLIANT

4 | Becoming GDPR compliant

For GDPR, your salon must prove it has a legal basis for collecting the client's personal information i.e. 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 in your country, you need to be able to prove how you collected, stored and used their data in detail

Section 2 - BECOMING GDPR COMPLIANT

5 | Accountability

In addition to the above, you need a proactive approach to show you are data compliant, not just the ability to cover your tracks in case of a client's complaint or audit.

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?

Section 2 - BECOMING GDPR COMPLIANT

6 | Consent

You have probably entered your data into an online form to receive a newsletter, or a demo of a product... maybe even Phorest Salon Software!

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'. 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. One big vague statement with a checkbox 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.



Let's Grow!

Phorest Salon Software can help you capture, store and show consent with our fully GDPR compliant consultation forms

UK: 0207 100 9290 / IRE: 01 8747800

www.phorest.com



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 salon 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 'Ignorance is not a defense' policy definitely applies to GDPR.

The legislation needs to be taken into consideration when making business decisions for your salon for the future. It is not a once-off exercise to become GDPR compliant, but an ongoing process.

If you bring the team on training, it is recommended that you appoint a 'GDPR Champion' for your salon. 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. Also, it is a great chance for a promotion, particularly if you have a dedicated receptionist.

Human error is the cause of the majority of data breaches. Examples of this include mishandling paper files containing customer data, losing a laptop with unencrypted personal data, or sending an email to the wrong person.

Section 2 - BECOMING GDPR COMPLIANT

9 | Children in Your Salon

Children are considered vulnerable individuals and are afforded specific protection under GDPR. Under GDPR, children are considered as anyone under the age of 16, but this may be reduced to anyone under the age of 13 under certain countries' laws e.g. Ireland.

Consent of the child and a parent or guardian must be obtained before collecting any personal data from children. As health data is considered sensitive personal data and is subject to additional restrictions, salons should avoid offering services to a minor that would require them to collect health information.

Salons who do offer these services to minors should seek additional, professional guidance on the matter. It is good practice to design forms specifically for bookings taken from minors to ensure you implement additional safeguards.

Included in the system, Phorest Salon Software provides these child-focused, GDPR-compliant forms as well.

Section 2 - BECOMING GDPR COMPLIANT

10 | Clients Requesting a Copy of Their Data Under GDPR Legislation

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):

- > All medical, contact etc. data you hold on the client
- > Why you hold that information
- > All activity and processing you are using it for
- > People you have sent or shared the data with (if consent was provided)
- > How you collected the data
- > Copy of the consent provided from that client
- > 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'.

This is the perfect example of why you need a GDPR-compliant salon software.

If you are using pen and paper and maybe an online email tool for example, it will be virtually impossible to provide all of the data above. Also, how do you delete a client's details from pen and paper if you have multiple entries in different diaries?





Phorest Salon Software Can Help You Become GDPR Compliant

Phorest Salon Software can help you with GDPR by:

- > **CONSENT:** Providing you with the industry's first fully digital compliant consultation forms meaning you opt-in all clients in a traceable way as per GDPR legislation.
- > **MARKETING:** Giving you filters and tools to create marketing campaigns using email, social media and SMS that are opted-in and won't get you in trouble when clients request a copy of their consent!
- > All data stored on Phorest Salon Software is fully encrypted meaning you and the team are protecting your clients' data from leaking!

Contact the Phorest Salon Software's 'Grow Team' today
and learn how we can help you become GDPR compliant



Let's Grow!

UK: 0207 100 9290 / IRE: 01 8747800

www.phorest.com