GDPR for salons

SALON GENIUS
the smart solutions company

GDPR - Salon Guide

Contents

GDPR - Salon Guide

1. INTRODUCTION

The General Data Protection Regulation applies to all businesses and organisation in the EU and will not be affected by the UK leaving the EU. It places additional requirements on business and organisations, and gives consumers improved rights, over and above those required by the Data Protection Act.

It comes in to force on 25th May 2018 and is intended to improve transparency about how businesses and organisations store and use personal data.

IMPORTANT NOTICE
This is intended only as a guide to assist SALONGENIUS customers in preparing for GDPR. For definitive advice and information please refer to the Information Commissioner website
www.ico.org.uk
The General Data Protection Regulation will apply from 25th May 2018 onwards and direct responsibility to understand and comply with its requirements, lies with the salon. Businesses may need to seek independent legal advice when reviewing or developing their own processes and procedures or dealing with specific issues.

a. Already comply with Data Protection?

Although you may already comply with existing Data Protection regulations, GDPR is stricter and more comprehensive than the existing Data Protection regulations; so much so in fact, that:

- certain breaches of GDPR regulation may result in fines of up to 20 million Euros or 4% of annual turnover, whichever is the greater
- EU governments will be recommended to make their citizens more aware of their rights in terms of how businesses and organisations use their personal data, so you can expect to be questioned on how you process personal data
- the Information Commissioner's office is actively increasing its workforce to ensure better policing and enforcement of data processing

However, if you do comply with existing Data Protection regulations, you are already at a better starting point in preparing for GDPR compliance.

As you move towards GDPR compliance you will be able to give your customers confidence in how you control and processing their personal data, and the safety and security of their personal data so giving them confidence in your business.

b. What is personal data?

Basically, any information that relates to an identifiable individual; the Data Subject. The following are examples of types of personal data that chould be critical to your business (but is not a definitive list):

- Name
- Contact Numbers
- Date of Birth
- Medical conditions

c. Who controls the data?

Under GDPR this is the Data Controller. You are the Data Controller.
You decide and are responsible for what personal data, and how that personal data, is collected and how your business uses that data for services, retail, marketing and promotions, etc.

d. What about processing the data?

The processing is done by your SALON**GENIUS** software system; it is the tool you use to collect and process your customers' personal data. SALON**GENIUS** is the Data Processor.

2. COMPLYING WITH GDPR

For GDPR, businesses (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.

The principles of processing personal data are:

e. Processed fairly and lawfully

Your salon must be able to:

- Clearly identify exactly what personal data you are collecting,
- Provide a clear, unambiguous legal reason for collecting and processing that personal data e.g. allergy alert tests could be required to determine if patch tests are require and colour services may be completed,
- Be able to prove how you collect, store and use the personal data you have collected, especially if a client has a complaint.

In addition, to demonstrate compliance, you will need to have:

- a Data Protection privacy policy, and
- a Data-handling Procedures manual. which is required in the event of an audit

f. Consent

If consent is required, your salon must be able to demonstrate that:

- consent was given, without using any preset preferences
- consent may be freely withdrawn as easy as given and at any time,
- consent is not necessary for the performance of a contract

When required by inspection, you must have a record of consent proving the client opted-in to give you the data and the following details must be available:

- Why you hold the personal data?
- How it was obtained?
- For what reason did you obtain it?
- Who has access to it? How is it kept secure?
- How is it stored?
- Is it still needed?
- Has it been passed to/accessed by any third parties?

g. Collected for specific legitimate purposes

Your salon must be able to:

- Provide a clear, unambiguous legal reason for collecting and processing that personal data e.g. allergy alert tests could be required to determine if patch tests are require and colour services may be completed

h. Adequate, relevant and limited

Your salon must only collect and process the personal data that is required.

i. Accurate and up-to-date

Your salon must maintain accurate and up-to-date personal data e.g. technical notes must be completed accurately and timely.

j. Retained only as long as is necessary

Your salon must not keep personal data any longer than is required.

k. Processed with appropriate security

Your salon must be clear on how secure is the personal data you hold and store and who can access it.

3. INDIVIDUALS RIGHTS

GDPR has the principle that personal data always belongs to the Data Subject. Your clients have the following rights under GDPR regulations and your salon is required to comply with them.

l. Right to be Informed

Clients should be clearly and transparently informed before collecting personal data, what will be collected and why and be given the opportunity to opt-in.

m. Right of Access

Clients may request access to their personal data, how their personal data was gathered and how it is processed. This is known as a Subject Access Request (SAR). This means your salon has to:

- Produce all information your hold on that client within 30 days
- You are NOT allowed to charge a fee for providing this information
- You should explain why you hold the personal data
- How that data was collected, including consent
- What processing is done on that personal data
- Identify who it has been shared with
- How long you have held it and how long it will be held

n. Right to Rectification and Erasure

Clients have the right to have their personal data corrected, or completed, if missing, incorrect or out-of-date.

They also have the right to have their personal data deleted if they are no longer customers of your salon or have withdrawn consent. This is the 'right to be forgotten'.

o. Right to Data Portability

Clients have the right to request that you provide their personal data for transfer to another business in a commonly-used and readable format, including human readable.

p. Right to object to Processing

Clients have the right to request that their personal data is not used for processing. Your salon may store the data but it must not be used e.g. direct marketing.

q. Right to be Notified

In the event of a breach of the personal data your salon holds and processes, the client has a right to be informed of the breach of their data within 72 hours.

4. SENSITIVE DATA

The processing of sensitive personal data e.g. Health data, requires **EXPLICIT** consent from the client.

Your salon must also have a clear lawful and legitimate reason for collecting and processing these types of data.

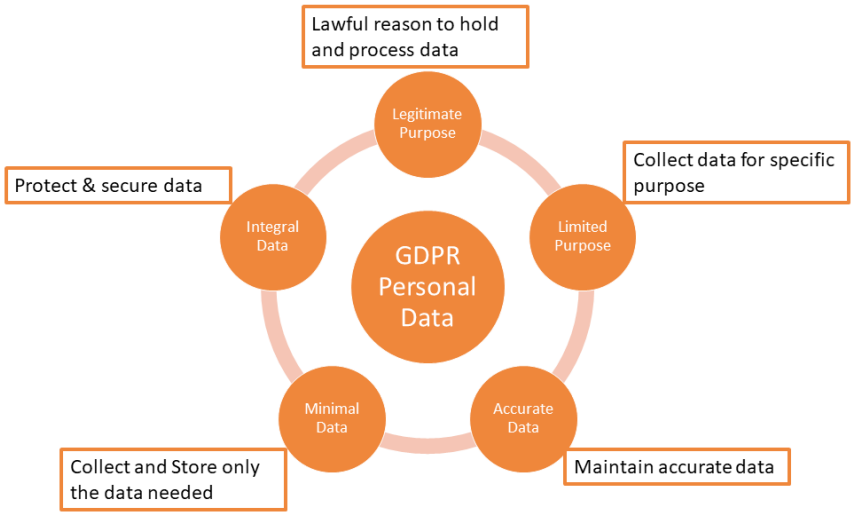
Under GDPR, Children are considered vulnerable and are afforded specific protection.
Generally, children are considered as anyone under the age of 16, but this may be reduced to anyone under the age of 13 under certain countries' laws.

Specific 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 ay wish avoid offering services to children that would require them to collect health information.

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

While this guide gives a basic overview of GDPR, SALON**GENIUS** advise that you explore GDPR training for your salon by a certified trainer. GDPR is here to stay and not a visit once exercise. If you invest in educating your team on GDPR compliance you will future-proof your business regarding Data Security and your clients will keep coming back.



Copyright © 2018
Mascolo Support Systems Ltd.
All Rights Reserved.

SALON**GENIUS**® is a Registered Trademark of Mascolo Support Systems Ltd.

All other Trademarks used in this document are recognised and acknowledged as the property of their respective owners.

This document, including preceding and subsequent versions of it, remains the property under Copyright of Mascolo Support Systems Ltd.

No unauthorised copying, transmission or storage, using any form of data storage and retrieval system, will be permitted without the prior written permission of Mascolo Support Systems Ltd.

Revision Date: 12 April 2018 10:03 AM

ico. Information Commissioner's Office

GDPR General Data Protection Regulation