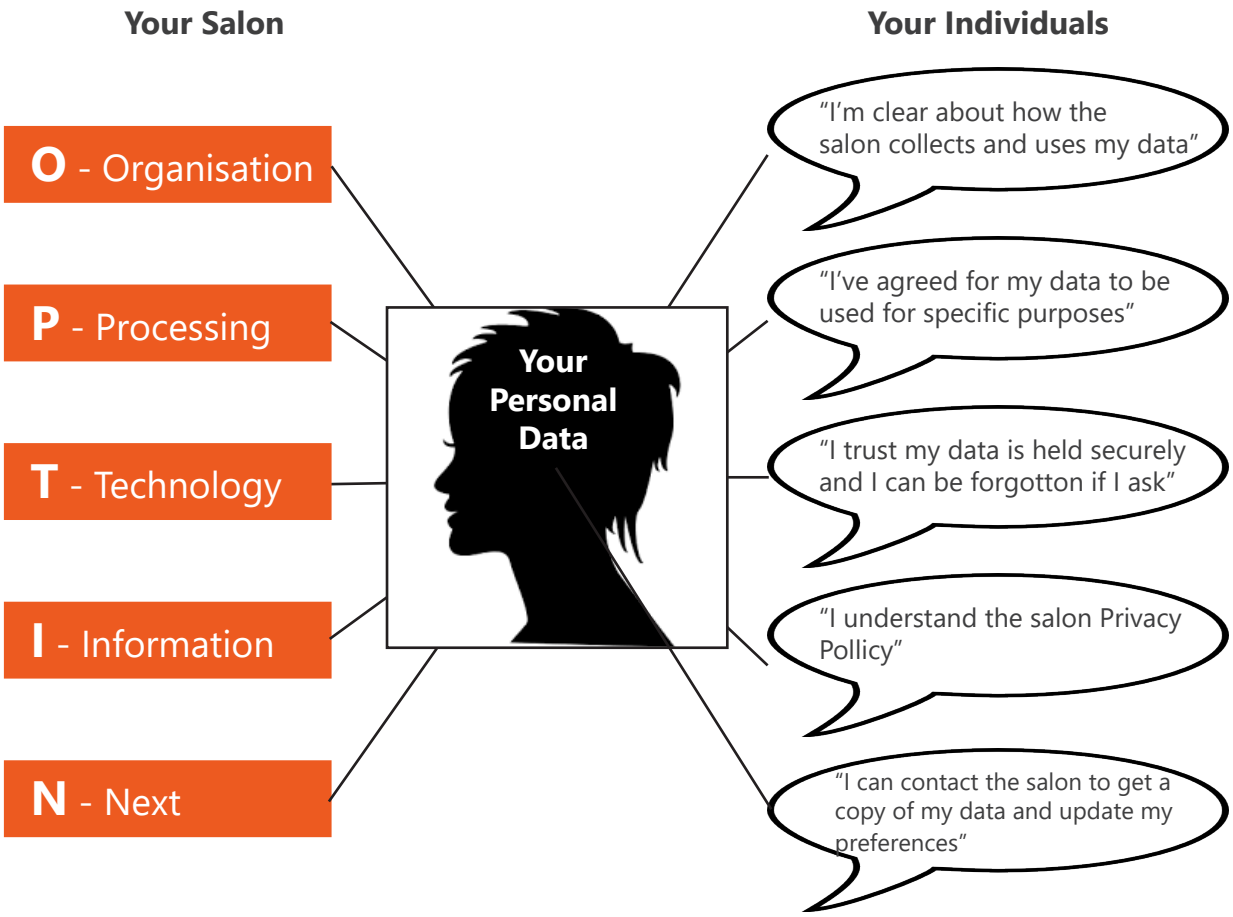
OPTIN checklist

SALON GENIUS
the smart solutions company

GDPR Checklist

This checklist sets out activities you will need to consider – and act on – by the compliance deadline of 25th May 2018. Use this to help you identify what support you may need ithin your salon.
In line with GDPR we have structured this on the **OPTIN** sequence of procedures
Remember, this is only a guide and does not constitute legal advice.

OVERVIEW



Revision Date: 12 April 2018 4:17 PM

ico. Information Commissioner's Office

GDPR General Data Protection Regulation

ORGANISATION

Salon understands and supports GDPR

Your Team needs to fully understand the impact and ensure resources are available to implement the changes required for GDPR compliance. It requires a new strategy. Risk needs to be managed.

Salon use plain English

Before you tick this box, just take a moment. Are your policies really easy to understand? Individuals need to be clear on what they are giving consent for and you need to ensure the language used is appropriate for your individuals, including children (if applicable). No Jargon!.

Salon have assessed and updated their Privacy Policy

You may need to take legal advice on developing a suitable Privacy Policy.

We dont need a Data Protection Officer

While you probably don't need to name a Data Protection Officer in your Privacy Policy, you do need a suitably knowledgeable person, or team of people, that individuals can contact regarding their personal data. If there is not someone with the expertise in the team, now is the time to train or recruit someone.

Salon knows which departments are affected

No matter how tidy you think your systems and processes are you will need to impact assess all departments to identify how compliant their current processes are. Now you know who is affected you can plan appropriate action.

Salon have assessed the level of risk

Breaches of key GDPR provisions could lead to fines of up to €20 million or 4% of annual turnover, whichever is greater.

We understand how we communicate with our individuals

Under GDPR, consent to use an individuals data to communicate for specific purposes will be required. You need to identify which purposes these are, whether you already have consent or whether you need to obtain it. There are certain communications – for instance, mandatory communications such as Direct Debit information – that do not need consent.

Salon have checked if regulated by PECR

You have checked whether you are liable and need to be accountable to the Privacy and Electronic Communications Regulations (PECR). Answer YES to any of the points below and you need to ensure you're up to date for these regulations as well.

- Market by phone, email, text or fax?
- Use cookies or a similar technology on your website?
- Compile a telephone directory (or a similar directory)

We have prioritised clients to convert to the right level of consent

Achieving consent from everyone on your database is an enormous task. Use this time to prioritise individuals whose consent you need immediately so that you can minimise the impact on business.

Salon can be fully accountable

The salon needs to be fully accountable. Everyone has a part to play. Your team need to understand WHY the processes and procedures are in place. Compliance needs to be business as usual. Walk the talk. Don't just pay lip service; exercise the mindset to protect individuals' personal data.

PROCESSING

Salon knows the source of all data

It is likely that data will be collected from multiple sources and may even be stored in numerous places. You need to map your inbound and outbound data flow.

Salon knows what data they are holding

Is your data categorised? Do you understand what sensitive data you hold? If not you need to pay attention to the new GDPR extended definition of sensitive data e.g. health, children. Do you have specific consent to use this data? Do you need to collect and store it? If yes, for how long? GDPR stipulates that data should only be held as long as it is needed.

Salon is transparent about the use and sharing of data

Individuals need to understand the purpose for which you have collected their data and whether you intend to share internally or externally with other businesses.

Salon can clearly demonstrate that they have consent to use this data

Individuals need to be provided with a place to provide consent for the collection and use of their personal data for the specified purpose(s), or for sharing. They must also be able to easily change or withdraw these consents and have the ability to track the history of any amendments.

Salon have processes in place to delete data

GDPR requires you to delete personal data when either you no longer need it, the purpose you collected it is no longer valid or when the individual exercises their right to erasure.

Salon has systems in place to manage a data breach

Reputations can be destroyed by a data breach. GDPR requires that the authorities are informed and where there is a high risk to their rights and freedoms the affected individuals receive communication within 72 hours. There are some exclusions, such as if the data is encrypted.

Salon can comply with an individual's right to portability

Portability of data is not a new concept but individuals have new rights. Individuals have the right to obtain their personal data and reuse it as they wish – as long as the information meets specific criteria. Organisations must be able to comply and send information in a commonly-used format within a month of it being requested.

TECHNOLOGY

Salon can provide details of all data electronically

Individuals have the right to request a copy of the information you hold about them. You need to be sure that this data is accessible and can be readily extracted for the individual.

All data is securely stored and safely encrypted

As mentioned above, if data is encrypted and unintelligible to unauthorised persons, your salon could potentially be exempt from the 72-hour requirement to notify individuals of a data breach. Of course, you would still have to notify the relevant authorities.

Salon can fulfil the 'right to be forgotten'

You need to demonstrate the capability to completely erase all personal information, from every department, spreadsheet and system. Under GDPR, an individual has the right to be forgotten. You also need to inform any external parties, where this personal data has been shared to do the same.

All new technology has privacy by design built-in

Whether you are upgrading existing systems, or specifying new systems, privacy should be built in by design. Then you are sure that the privacy of your individuals is assured.

Salon keeps technology updated

It is a requirement under GDPR that service and security updates are kept up-to-date on technological equipment that is used to process personal data.

INFORMATION

Salon have updated all our permission statements

Your permission statements and Privacy Policies need to be specific and relevant to your alon. You will need to seek explicit consent and only collect data for legitimate purposes.

Individuals can easily find out what information the salon hold on them

This is the acid test on compliance. Can you easily tell an individual what information you hold, how it was obtained, when it was consented and, if they request it, that you can delete their personal data from all your systems?

Salon can verify individual's ages and identify children for specific consent

The regulations raise the age of consent for collecting an individual's data from 13 to 16 years old. If your salon collects data from children, you will need a process in place to verify an individual's age, identify children and seek parental or guardian consent for use of their data.

Salon have developed template responses

Use the time before May 2018 to create template responses to individual's requests for example a subject access request. This serves two purposes. To prepare your team to ensure they know what to send, and that all of the individuals' requirements are met.

Salon know what additional information is required to adhere to GDPR

Because of the Data Protection Act there will already be consent in place for some – if not all – data. However, there will be gaps. Gaps could include being able to erase data, timestamp when consent was obtained, or obtain specific consent for particular purposes.

NEXT

Salon have tested an individual's experience when requesting consent

Many salons are concerned about the impact on individuals when requesting consent. Use this time to trial new approaches. To monitor impact and identify how to make consent business as usual in engaging and building trust with your individuals.

Individuals can access their own data and update their preferences

GDPR is citizen centric. This puts the individual in control of how their data is used. Where individuals can give or withdraw permission easily. Where transparency is absolute.

Salon can put it right when we've got it wrong

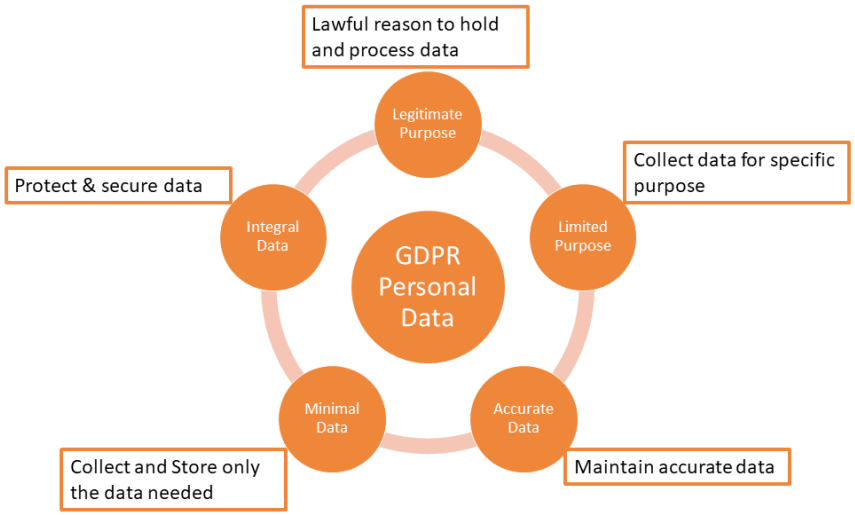
If an individual knows that information you have is incorrect, you must be able to update their information, and record additional information, if that is required. It's formally called the right to rectification.

Salon marketing that uses data are fully aware of policies, procedures and the new GDPR regulations

Training can easily be overlooked but ignorance is no defence. Every person who has access to data – and / or who uses data as part of their role – needs to be fully aware of the new legislation, the policies and procedures of your own organisation and that consent is a new route to engagement with your individuals and service users.

Data Protection Registration

If you handle personal information about individuals, you have obligations to protect that information under the Data Protection Act. Follow this link to Registration Self-assessment.



Useful Links

Information Commissioner

General Data Protection Regulation

Guide to Privacy and Electronic Comminications Regulation

www. salongenius.com