

A man and a woman are smiling and looking at a tablet together. The man is on the left, wearing a white shirt, and the woman is on the right, wearing a black top with a white collar and a pink long-sleeved shirt. They are both looking at a blue tablet held by the man. The background is a soft, out-of-focus grey.

GDPR

Your guide to data protection law



Supporting the hair, beauty
and barbering industries



How the NHF can help

Check out the NHF's other guides on all aspects of running a hair, barbering or beauty business at www.nhf.info/nhf-guides.

NHF Guides

- Absence management
- Allergy alert testing
- Apprenticeships
- Becoming a training provider
- Business finance
- Card payment processing
- Careers
- Chair renting
- Client experience
- Complaints
- Employing people
- Franchising
- GDPR
- Health and safety (part of kit)
- Hiring a manager
- Managing performance
- Marketing your salon
- Minimum wages
- Pensions
- Prices, wages and profit
- Recruitment
- Salon fit-out
- Salon software
- Self-employment
- Selling your business
- Start-up guide (updated)

Important information

The information contained within this document is for information and guidance purposes only and must not be used as a substitute for seeking legal or professional advice. The information is correct at the time of writing.

This guide covers:

THE BASICS

- What is GDPR?
- What is personal data?
- What is the ICO?
- Does my business need to register with the ICO?
- Information audit
- Accountability

GDPR AND CLIENT DATA: MARKETING

- Using data for marketing
- What is PECR?
- What is the Telephone Preference Service (TPS)?
- What does this mean for marketing?
- A lawful reason to use data
- What does consent mean?
- Best practice: double opt-in
- Children and GDPR
- Data clear-outs
- Making everything crystal clear
- Identifying who you are
- Making it easy to opt out
- Keeping clear records
- Clients' rights
- What about existing mailing lists?
- Template consent forms
- Complying with the TPS
- Loyalty schemes and GDPR
- Leaflet drops
- Staff training
- Cookies

GDPR AND EMPLOYEE DATA

- Getting organised
- GDPR rules on staff data
- Employment contracts

- Keeping your employees informed
- The 'right to be forgotten'
- Job applicants and GDPR
- Self-employed chair and room renters

SPECIAL CATEGORY DATA: A SPECIAL CASE

- Additional safeguards

PRIVACY NOTICE

- Privacy notice and GDPR

SALON SOFTWARE

- Salon software and GDPR

CCTV

- Make sure you stay within the law

KEEPING FINANCIAL RECORDS

- How long should financial records be kept?

WHEN THINGS GO WRONG

- Personal data breaches – what to do

TEMPLATES

- Information audit
- Consent for marketing
- Privacy notice
- Data retention policy
- Consent for special category data eg allergy records, medical conditions
- Consent for children under 16
- Response to receipt of consent forms
- Data breach procedure

LEGAL HELPLINE

- Help with GDPR

CHECKLIST



The basics

WHAT IS GDPR?

GDPR stands for **General Data Protection Regulation**.

GDPR replaced the Data Protection Act 1998 (DPA) on 25 May 2018.

Under GDPR you will have to comply with stricter rules in relation to the personal data you collect and use. This includes both electronic *and* paper records.

There will be financial penalties if you don't comply with GDPR so make sure your hair/beauty salon or barbershop stays within the law.

WHAT IS PERSONAL DATA?

Personal data is any information that can be used to identify a living person, either on its own or in combination – for example, a name *and* an email address.

Personal data includes:

- A photo.
- Name.
- Address.
- Phone numbers.
- Email address.
- Personal information such as medical details.
- Computer IP address ('IP' stands for 'Internet Protocol' and may reveal an individual's geographical location).

These are some of the main examples, but the list is not exhaustive. GDPR applies to all personal data relating to clients, employees, ex-employees and job applicants.

WHAT IS THE ICO?

ICO stands for Information Commissioner's Office.

It is the UK's independent authority responsible for upholding information rights in the public interest.

Find out more: ico.org.uk

DOES MY BUSINESS NEED TO REGISTER WITH THE ICO?

Yes. Under GDPR you will need to be registered on the new ICO registration scheme.

If you are already registered with the ICO under the old data protection laws, the ICO should transfer you to GDPR when your registration is due for renewal.

WARNING: always deal directly with the ICO. Don't deal with any other organisations that offer to 'register' you. They may be bogus and will charge more than the ICO fee.

The ICO's helpline number is 0303 123 1113.

INFORMATION AUDIT

As a starting point, you will need to carry out an information audit. Set out clearly and in detail:

- The type of personal data you hold (both computer and paper records).
- Who gave you the information or where you got it from.
- Why you need the information and what you do with it.
- Who you share the information with.

For example, a typical salon or barbershop will hold:


- Staff details, including contact details, salary, next of kin info, relevant medical information, CVs and job applications.
- Clients' names, addresses, contact details, allergy tests, and any relevant medical notes etc.

ACCOUNTABILITY

Accountability is a key aspect of GDPR. This means you must keep clear records of all your activities in relation to your collection and use of personal data. For example:

- Why you collect it.
- How you collect it.
- How you store it and keep it secure.
- How you use the information.
- Who has opted out of receiving marketing messages from you.
- Who has opted in.
- How and when they opted in or out.
- Requests from individuals to see/ amend/transfer data and how you responded.
- Any breaches that occur and the actions you took in response.





GDPR and client data: marketing

THE GOOD NEWS

GDPR says you can use personal data to carry out direct marketing activities. But read on to find out what you must do to stay within the law.

Under GDPR, you must comply with strict rules about contacting clients with marketing messages. As part of this you will also have to comply with:

- the existing Privacy and Electronic Communications Regulations (PECR): and
- the Telephone Preference Service.

WHAT IS PECR?

PECR stands for Privacy and Electronic Communications Regulations.

PECR sets out rules that cover marketing by phone, email, text and fax.

PECR does not cover sending marketing messages by post, but this is covered by GDPR and similar rules apply.

WHAT IS THE TELEPHONE PREFERENCE SERVICE?

The **Telephone Preference Service (TPS)** is a free official service. Anyone can register with the TPS if they do not want to receive unsolicited sales or marketing calls.

WHAT DOES THIS MEAN FOR MY MARKETING ACTIVITY?

The following guidelines will ensure you stay within the law in relation to GDPR, PECR and the TPS.

A LAWFUL REASON TO USE PERSONAL DATA FOR MARKETING

Under GDPR, you must have a **specific lawful reason** for collecting and using people's data to carry out marketing activity.

There are six lawful reasons given in GDPR but often the safest one to rely on and the one NHF recommends you focus on is **consent**.

WHAT DOES CONSENT MEAN?

Your clients must actively agree to receive marketing information from you. This means they must **opt in** - not be given the opportunity to opt out. A decision to opt in must be informed, clear, specific and unambiguous.

You can no longer provide a box that is already ticked and expect clients to 'untick' it if they wish to opt out. This is not acceptable practice under GDPR.

The best way to get consent is to ask your clients to tick opt-in boxes confirming they are happy to receive marketing calls, texts or emails from you. (See the consent template.)

BEST PRACTICE: DOUBLE OPT-IN

Send a confirmation email to everyone who opts in to receiving your marketing messages. In this email you can thank them for opting in, explain the benefits (for example, that they will receive special offers and birthday vouchers), and clearly state that they are free to opt out at any time. Explain that each of your marketing messages will include clear instructions for opting out.

It's also good practice to provide a link to your privacy notice which will explain how you collect and use personal data and what rights individuals have.

HEALTH AND MEDICAL DATA

This is 'special category data' under GDPR and its use is more tightly controlled. Health and medical data includes, for example, allergy test records or client consultation records. You must have consent to use and keep this data.

GDPR AND CHILDREN

Under GDPR, children and young people under 16 are a special case: you must obtain consent from a parent or guardian to keep and use personal data about under-16s. Make a separate list of all your clients who are under-16s.

HAVE A CLEAR-OUT OF UNNECESSARY DATA

Before you start getting consent from clients, go through your database and delete information you no longer need. A good cut-off point is 12 months. If you haven't seen a client for this long, you're less likely to get a positive response from them and their details may well be out of date.

But there is some information you will need to keep for more than 12 months, for example, allergy test records (4 years) or financial transactions (6 years). Keep just enough information to be able to find the records you may need, and delete all other personal information.

Repeat the clear-out regularly (at least once a year) so your client database is always as up-to-date and accurate as possible.



MAKE EVERYTHING CRYSTAL CLEAR

GDPR says that all communications about GDPR must be written in plain language that is easy to understand.

BE CLEAR ABOUT WHO YOUR MARKETING MESSAGES ARE FROM

All your marketing messages must clearly state that they are from you. Always include the name of your business, where it is located and contact details.

MAKE IT EASY FOR PEOPLE TO OPT OUT OF YOUR MARKETING MESSAGES

Remember: you must only send marketing messages to people who have given their consent to receive them.

All your marketing messages must then include a simple and straightforward way to opt out of receiving further messages. This makes it easy for people to change their mind about receiving marketing messages.

This is one of the requirements of GDPR which says that people have the absolute right to opt out of receiving marketing messages at any time.

KEEP CLEAR RECORDS

You must keep proof that an individual has opted in as well as a record of who has opted out and which type of messages they have opted out of.

Keep clear records of:

- Who has consented to receiving marketing messages.
- How they consented.

- Which method of communication they have consented to: Emails? Texts? Phone calls?
- Which types of marketing message they have consented to:
 - Newsletters?
 - Special offers?
 - Birthday greetings/vouchers?
 - Loyalty scheme/rewards?
 - Seasonal greetings? For example, special messages and offers at Christmas or Easter.

Keep a record of how and when individuals withdraw their consent.

Your software system or manual records must store this information in an easily accessible way so you can easily find it if needed.

This documentation is a new requirement under GDPR.

DON'T USE THE DATA FOR ANY OTHER PURPOSE

Once you have received consent to use an individual's contact details to send them marketing messages, you must not use the information for any other purpose unless you have specific and documented permission from them to do so.

INDIVIDUAL RIGHTS

You must provide clients with a 'privacy notice' (see our template) which includes your purposes for processing their personal information, how long you'll keep it and who it will be shared with.

They have the right to:

- See the information you hold about them, which you must provide promptly (usually within one month) and free of charge.
- Have incorrect data corrected.
- Have the use of their data restricted if they wish.
- Have their information deleted (the 'right to be forgotten') unless you have a good reason for not doing so (for example, ongoing legal action).

RENEW CONSENT EVERY TWO YEARS

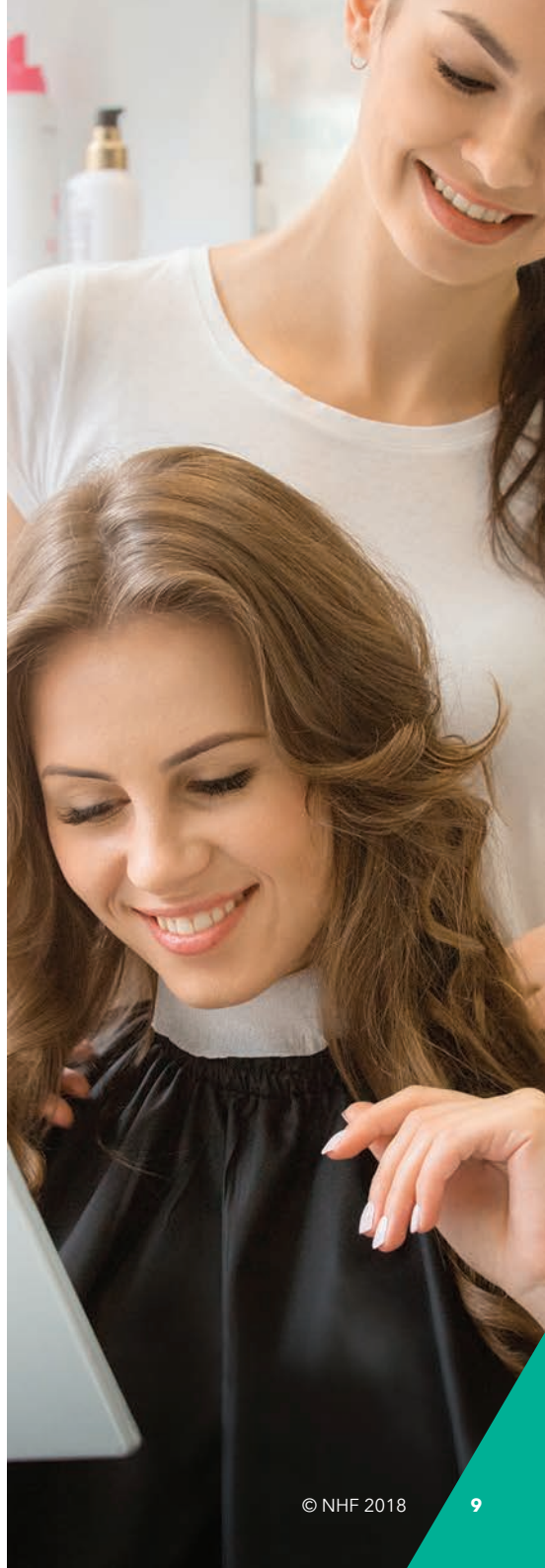
It's good practice to renew consent every two years. This creates an ongoing process of trust with your clients.

WHAT ABOUT EXISTING CLIENTS? IS CONSENT NEEDED?

You will not need to get new consent to send out marketing messages and newsletters etc to existing clients **if the following conditions are met:**

- You collected their contact information as part of providing a service or product to them.
- You are marketing only for similar purposes.
- Every marketing message you send them includes a clear and easy way to opt out of receiving further marketing messages.

If you are in any doubt you should ask for fresh consent to make sure you are complying with the law. See our 'consent for marketing' template.





PASSING CLIENT DATA ON

We strongly recommend that you don't pass your clients' details onto third parties without a very good reason and with great care as explained below.

If you do share personal data with anyone else, you will need to explain who you will be sharing data with and for what purpose, and you will need your clients' specific permission to do so. You should also agree in writing with the third party that they will comply with GDPR in the way you require them to.

TELEPHONE PREFERENCE SERVICE

Don't forget: you must also comply with the rules of the Telephone Preference Service (TPS).

The law says you must not telephone clients who are registered with the TPS.

You can check if any of your clients' telephone numbers are on the register here: <http://www.tpsonline.org.uk/tps/registered.php>

The TPS service includes mobile telephone numbers. However, registration of a mobile number will not automatically prevent text messages. This means you must get specific permission to send text messages.

LOYALTY SCHEMES AND MARKETING

As loyalty schemes are part of your marketing activities, you will need consent from clients for this purpose. See our 'consent for marketing' template. t

LEAFLET DROPS

You can carry on doing local leaflet drops to advertise your business. This is allowed under GDPR as you are not targeting a particular individual.

IF YOU PAY FOR MARKETING SERVICES

If you pay someone else to do your marketing you are jointly responsible for complying with data protection laws.

Remember: if your business breaks the rules, action would normally be taken against you first – not the person/company who is doing your marketing work.

MAKE SURE YOUR STAFF UNDERSTAND AND COMPLY

You must ensure that all your staff understand the importance of complying with GDPR and what they will need to do. Make sure they read and understand your privacy notice and the consequences of not complying with GDPR.

Remember – they may have to answer clients' questions about why they are being contacted for consent, so make sure they can provide a short and straightforward answer.

You will need to keep records of the GDPR training you have provided to your employees.

COOKIES

Under GDPR, cookies* can be defined as personal data. This means that GDPR rules apply.

To comply, ensure that when people visit your website for the first time, cookies will be blocked until they:

- agree to cookies being set; or
- understand that taking certain actions on your website will result in cookies being set.

** Cookies are text files that can, for example, tailor the content that is shown and record how long visitors spend on a site and which links they click.*



GDPR and employee data

GET ORGANISED

It's important to get organised. Put together a list of all the personal data you hold about:

- Current employees.
- Past employees.
- Job applicants who were not offered jobs.

Remember to include everything, for example:

- Contact details including phone numbers, address, email address etc.
- Bank account details.
- Next of kin details.
- Medical information.
- CVs and related job application information.
- Photographs.

GDPR RULES ON EMPLOYEE DATA

GDPR requirements include:

- You will need a specific lawful reason to hold and use personal data about your staff. Employment law obligations and the fact that you have a contract with an employee are both valid reasons which apply to employee data.
- Personal data about your staff must be collected and used for employment related purposes – and not used for any other purpose.
- It must be kept securely - password protected or under lock and key if paper-based.
- You must hold only the information you need.

- You must hold information only for as long as you need it.
- You must delete personal data about an individual at their request unless you have a good reason for not doing so.
- Your employees are entitled to see and correct personal data held about them.
- You cannot charge a fee for providing this information and must respond to requests within one month.

This should be included in your privacy notice (see our template).

EMPLOYMENT CONTRACTS

The stricter data protection rules under GDPR also apply to the wording in employment contracts, which the NHF offers free of charge to Members.

A privacy notice to be given to existing and new employees with an amended contract is available from May 2018.

KEEP YOUR EMPLOYEES INFORMED

Let your employees know what their rights are under GDPR. Similarly to your clients, employees have the right to:

- See the data you hold about them.
- Know how personal data about them will be used.
- Have incorrect data corrected.
- Have their information deleted (the 'right to be forgotten') – but only in certain circumstances.



YOUR EMPLOYEES’ ‘RIGHT TO BE FORGOTTEN’

There is a valid reason to keep employment related data for all current staff. However, individuals can ask for their personal data to be deleted from your systems and paperwork – but only if there is no compelling reason for you to keep it.

You can refuse to delete personal data, for example, if you need it to defend a legal claim or deal with queries from HMRC.

But otherwise, if you have no good reason to keep personal data about individuals – for example, information provided by job applicants (see page 14 for more on job applicants), or information about ex-employees – it is a good idea to delete it from your systems. You can make it clear in your privacy notice (see page 15) that you will promptly and securely delete personal data that you no longer need.

You can follow the guidelines below:

TYPE OF INFORMATION	HOW LONG TO KEEP IT
Employee records, contracts of employment, changes to terms and conditions, annual leave, training records	While employment continues and up to six years after employment ends
Payroll and wage records including PAYE, income tax, national insurance, sick pay, redundancy payments	Six years from the financial year-end in which payments were made
Maternity records	Three years after the end of the tax year in which the maternity pay period ends
Emails	One year from the end of the month in which they were received or sent from your email accounts. Delete emails to and from ex-employees or contractors within two weeks after they leave unless this forms part of the employment record – see above.



JOB APPLICANTS AND GDPR

When you receive job applications include in your acknowledgement confirmation that all information received from unsuccessful applicants will be deleted from your records – CVs, covering letters, emails and email addresses automatically captured by your system. You should make sure this is done within four months of notifying the applicant that they have been unsuccessful.

Here is some suggested wording:

To respect your privacy and comply with GDPR (General Data Protection Regulation) it is our policy to delete from our systems all information we receive about candidates who are not selected for this position. This will be carried out within four months following our feedback to unsuccessful applicants.

If you want to keep CVs for future consideration, you must ask for specific consent to do so. Specify how long you will keep the information before deleting it from your electronic and/or paper records.

SELF-EMPLOYED CHAIR AND ROOM RENTERS

Chair and room renters are each responsible for maintaining their own client database and for making sure they comply with GDPR. This is because they are running their own self-employed business which is separate to the salon or barbershop they are working in.



Special category data: a special case

ADDITIONAL SAFEGUARDS

GDPR says that special category data must be treated with particular care. The definition of special category data includes information about a person's physical or mental health or condition.

This will apply to:

- Information you hold about employees' physical or mental health.
- Information you hold about clients in relation to allergy testing and physical conditions which may mean they can't have certain beauty or cosmetic treatments.

SPECIAL CATEGORY DATA: COMPLYING WITH GDPR

As explained above, you must have a specific lawful reason for collecting and using personal data.

For special category data, you will also need to specify a second lawful reason. For example:

- The individual has given you specific consent to process data about their physical and mental condition.
- You must process the information to comply with employment law.

It is possible the standard GDPR reason and the special category data reason are broadly the same (eg consent). However special category data reasons are very specific and detailed and we recommend you check the ICO guidance on this.

Remember: as part of GDPR you must keep a record of the lawful reasons you are using to process sensitive personal data.

Privacy notice

PRIVACY NOTICE AND GDPR

Your privacy notice should include:

- What information (personal data) you collect.
- Why you collect it.
- How it is used.
- Who it will be shared with.
- When and why it will be deleted.
- What you will not use personal data for.
- What rights clients, employees, ex-employees and job applicants have.
- How personal data is kept secure (for example, password-protected online; under lock and key for paperwork).
- Who individuals can make a complaint to. (They should complain to you first. If they are not satisfied by your response, explain that their next step is to contact the ICO.)

Your privacy notice must be written in plain, easy-to-understand language. Make sure it's readable on different devices including mobile phones.

Provide easy access for your clients via your website and a link in marketing messages. Make sure all your staff see it and have easy access to it too.

See our 'privacy notice' template.

If you have a separate data protection policy or any other related policies, you must make sure they all comply with GDPR.



Salon software

SALON SOFTWARE AND GDPR

Many salons and barbershops keep personal data about their staff and clients on salon software. In addition, salon software is often used to send out automated marketing messages. You will need to be clear about what personal data it stores, how the system uses it and how it is kept secure.

Most software systems can be set up to control who has access to different types of data and will already offer GDPR-compliant features such as secure storage and automatic backup.

Your software supplier should be ready and able to offer updates and general advice to ensure your hair/beauty salon or barbershop complies with GDPR. For example, ask your supplier if they will be updating your salon software so it can:

- Record individual client's marketing preferences.
- Offer fast and easy unsubscribe methods.
- Store your privacy notice and provide easy access for staff and clients.
- Respond quickly to individuals' requests to see, amend and/or transfer their data.
- Automatically delete client records after a fixed amount of time set by you.

CCTV and Wi-Fi

MAKE SURE YOU STAY WITHIN THE LAW

If you use CCTV in or outside your business premises you are monitoring and/or recording the activities of individuals. This means you are processing personal data and must follow the same strict rules that apply to the processing of any personal data. For example, individuals will have the right to see footage and you must not keep any recorded information for longer than is necessary.

If you provide free guest Wi-Fi to clients the terms and conditions need to be very clear on what data you are collecting, the reasons why and how you intend to use the data. If you intend to use the data for marketing purposes you must get opt-in consent.



When things go wrong

PERSONAL DATA BREACHES - WHAT TO DO

What is a data breach?

This means the loss, or unauthorised alteration or sharing of any of the personal data you hold about individuals. This can be deliberate or accidental. For example:

- Sharing information with someone who is not authorised to see it.
- Being 'hacked' by someone who gains unauthorised access to your computer system.
- The loss of devices such as laptops, tablets, phones or memory sticks that hold or give access to personal data.

What should you do?

You must make a record of:

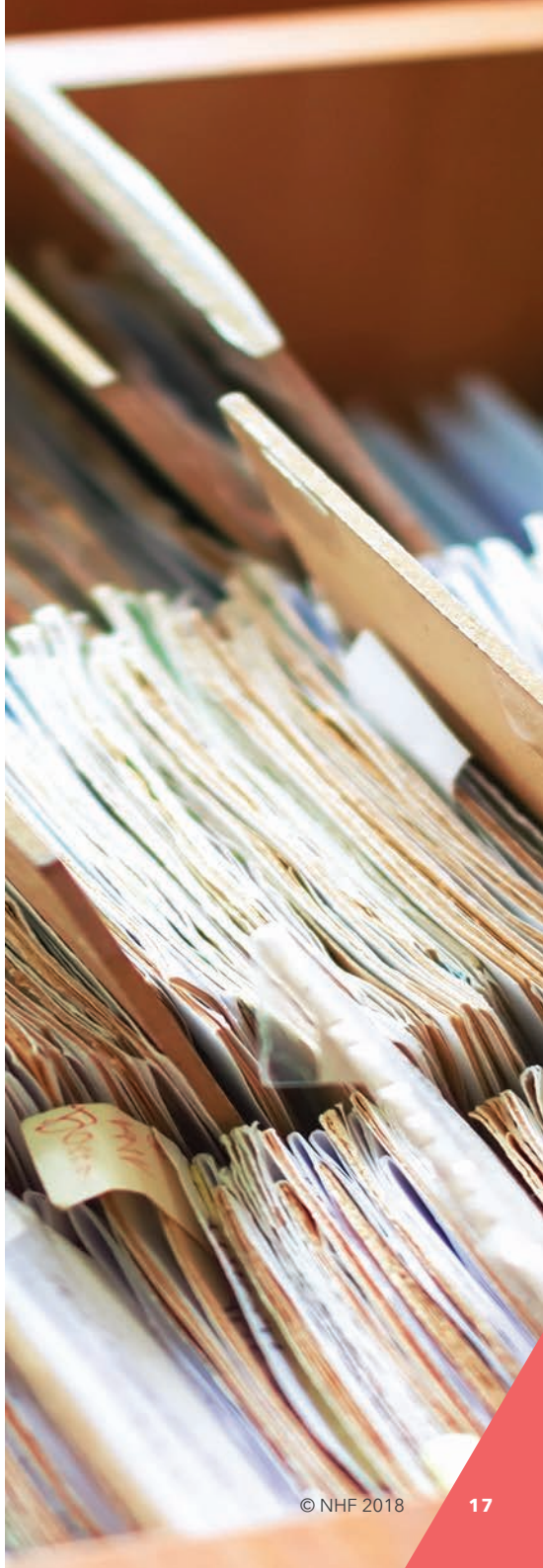
- What happened and the cause of the breach.
- The effects of the breach.
- What you did to put things right.
- How you will prevent it happening again.

What else to you need to do?

If the breach is very serious and may place individuals at risk, for example, the possibility of financial loss or severe emotional distress, you must:

- Report it to the ICO within 72 hours (Telephone 0303 123 1113).
- Tell the individuals concerned what has happened as soon as possible.

If you fail to report serious breaches to the ICO you could be fined up to twenty million euros or 4% of your turnover.





Templates

NHF Members can use our free ready-to-use templates to help make complying with GDPR as straightforward as possible:

- information audit
- privacy notice
- data retention policy
- data breach procedure
- consents for marketing, special category data and children
- response to receipt of consent forms

Every business is different, so you can adapt the templates to make sure you cover all the personal information you hold, how you use it, and who you share it with.

Free legal helpline and GDPR advice for NHF Members

The NHF understands the legal and commercial complexities of running your own hair, beauty or barber business and offers Members a free 24/7, 365 days a year legal helpline for employment and HR issues including GDPR.

This indispensable legal backup provides NHF Members with sound and practical advice on how to deal with a range of common employment issues, from contracts, apprenticeship agreements, absence and holidays, to redundancy, managing staff performance and maternity arrangements.

Join us today.

Checklist

THE BASICS

The following checklist is a quick summary of what you need to do about GDPR.

- Make sure you're registered with the ICO (helpline: **0303 123 1113**).
- Carry out a thorough information audit.
- Keep clear records of all your activity in relation to collecting, keeping and processing personal data.
- Ensure electronic data is password-protected and keep paper records under lock and key.
- Don't keep client or employee information for longer than you need to.
- Create a privacy notice that sets out in plain language how you comply with GDPR.

MARKETING

- Understand and comply with GDPR rules.
- Understand and comply with the Privacy and Electronic Communications Regulations (PECR) and Telephone Preference Service.
- Ensure you have consent from individuals to send marketing messages to them.
- Make it easy for individuals to opt out of your marketing messages.
- Ensure all your marketing messages clearly state they are from you and include contact details.
- Make sure your staff understand and comply with GDPR – keep records of GDPR staff training.

- Clients have the right to see and correct the data you hold about them. You must also delete their data on request unless there is a good reason not to do so.

EMPLOYEES

- Use NHF employee contracts to ensure you are complying with GDPR.
- Make sure your employees know how their personal data is used and what their rights are under GDPR.
- Inform unsuccessful job applicants that you will be deleting their personal data from your records (and make sure you do so).

MISCELLANEOUS

- **Special category data** (for example, allergy records and medical information) must be treated as a special case – you will need two lawful reasons to collect and store sensitive personal data.
- Make sure your **salon software** complies with GDPR – ask your supplier.
- **CCTV** recordings of individual activity must be treated as personal data. Be clear what data you are collecting for **guest Wi-Fi access**.
- Keep **financial records** for no longer than you need to.
- Take appropriate action if there is a **data breach**.
- Use the NHF suite of templates – information audit, privacy notice, data retention policy, data breach procedure, consents for marketing, special category data and children.



NHF, One Abbey Court, Fraser Road, Priory Business Park, Bedford MK44 3WH.

Phone: 01234 831965 | **Email:** enquiries@nhf.info | **Web:** www.nhf.info

