

**PRIVACY POLICY**

**CONTENTS**

1. Privacy notice
2. Data retention policy
3. Procedure for personal data breaches

**Privacy notice for NHF members**

This privacy notice explains how Amadeus Hair & Beauty Ltd looks after personal information you give us or that we learn by having you as a client and the choices you make about marketing communications you agree we may send you. This notice explains how we do this and tells you about your privacy rights and how the law protects you.

**TOPICS:**

* What information we collect about you
* How information about you will be used
* Marketing
* Employment
* How long your information will be kept for
* Where your information is kept
* Access to your information and correction
* Cookies
* Other websites
* Changes to our privacy notice
* How to contact us

**WHAT INFORMATION WE COLLECT ABOUT YOU**

We collect information about you when you book an appointment for a service or treatment, visit the salon or barbershop for a service or treatment, buy a product or apply for a job, whether contact is online, on paper, by email or over the phone.

The information you give us may include your name, address, email address, phone number, relevant history which may suggest that a service or treatment should not go ahead or certain products should not be used (eg allergies, pregnancy, skin conditions), payment and transaction information, IP address and CVs.

For clients under the age of 16, we will only keep and use their personal information with the consent of a parent, carer or guardian.

**HOW INFORMATION ABOUT YOU WILL BE USED**

In law, we are allowed to use personal information, including sharing it outside the salon/ barbershop, only if we have a proper reason to do so, for example:

* To fulfil a contract with you ie to provide the service or treatment you have requested and to communicate with you about your appointments
* When it is in our legitimate interest ie there is a business or commercial reason to do so, unless this is outweighed by your rights or interests
* When you consent to it: we will always ask for your consent to hold and use health and medical information.

We will therefore share your information with:

* Providers of our salon software system Salon Advantage

We have rigorous data protection and security policies in place with all our suppliers.

We will not share your information with any other third party without your consent except to help prevent fraud, or if required to do so by law.

**MARKETING**

We would like to send you information about products and services which may be of interest to you. We will ask for your consent to receive marketing information.

If you have consented to receiving marketing, you may opt out at a later date.

You have the right at any time to stop us from contacting you for marketing purposes or giving your information to third party suppliers of products or services. If you no longer wish to be contacted for marketing purposes, please contact Carol Knight at [info@amadeushairandbeauty.com](mailto:info@amadeushairandbeauty.com)

**EMPLOYMENT**

The information we collect about employees, the purposes it is used for and who it will be shared with is set out in our employment contracts and employee handbook.

**HOW LONG YOUR INFORMATION WILL BE KEPT FOR**

Unless you request otherwise, we will keep your information to contact you no more than three times a year for a maximum of 1 year from your last visit to the salon.

After a year we will delete all your personal information, except for your name, relevant client history (eg allergy test records which we keep for 4 years) and financial transactions (which we are obliged to keep for 6 years).

Information about unsuccessful job applicants will be deleted after four months.

See our data retention policy for further information, including employee data.

**WHERE YOUR INFORMATION IS KEPT**   
[check this with your software and website providers]

Your information is stored within the European Economic Area on secure servers provided by Salon Advantage. Any payment transactions are encrypted. Sending information via the internet is not completely secure, although we will do our best to protect your information and prevent unauthorised access.

**ACCESS TO YOUR INFORMATION AND CORRECTION**

You have the right to request a copy of the personal information that we hold about you. This will normally be free, unless we consider the request to be unfounded or excessive, in which case we may charge a fee to cover our administration costs.

If you would like a copy of some or all of your personal information, please contact Carol Knight at [info@amadeushairandbeauty.com](mailto:info@amadeushairandbeauty.com) or go to our website: <http://www.amadeushairandbeauty.com> and click on Privacy Policy

We want to make sure that your personal information is accurate and up-to-date. You may ask us to correct or remove information you think is inaccurate.

You have the right to ask us to object to our use of your personal information, or to ask us to delete, remove or stop using your personal information if there is no need for us to keep it.

**E-NEWSLETTERS**

We email e-newsletters to inform you about products, services and treatments provided by our salon. You have the opportunity to unsubscribe from e-newsletters at any time.

E-newsletters may contain subscriber tracking facilities within the actual email, for example, whether emails were opened or forwarded, which links were clicked on within the email content, the times, dates and frequency of activity. We use this information to refine future email campaigns and provide you with more relevant content based around your activity.

**WE DO NOT USE COOKIES ON OUR WEBSITE.**

**OTHER WEBSITES**

Our website includes links to other websites. This privacy notice only applies to this website so when you link to other websites you should read their own privacy notices.

**CHANGES TO OUR PRIVACY NOTICE**

We keep our privacy notice under regular review and we will place any updates on this webpage. This privacy notice was last updated on 7th May 2018.

**HOW TO CONTACT US**

Please contact us if you have any questions about our privacy notice or information we hold about you:

* By email [info@amadeushairandbeauty.com](mailto:info@amadeushairandbeauty.com)
* Or write to us at: Amadeus Hair & Beauty Ltd, 6 Elizabeth Parade, Tudor Drive, Yateley, Hampshire GU46 6BY

You also have the right to complain to the Information Commissioner’s Office. Find out on their website how to report a concern:

[www.ico.org.uk/concerns/handling](http://www.ico.org.uk/concerns/handling)

**Response to consent**

At Amadeus Hair & Beauty td we want to manage the personal information we hold about you in a way you’re completely happy with. You have agreed to us collecting and holding certain information about you, so we thought you’d appreciate a quick summary of what you have consented to.

Please let us know if you have any questions or you want to make changes.

Thank you for consenting to the following:

* Providing health information to ensure we know about any conditions such as allergies, skin conditions, pregnancy which indicate that particular services / treatments / products should not be used for you
* Allowing us to keep that information for 4 years
* Providing consent for us to hold information about a child or young person under 16
* Receiving messages about special offers, birthday treats, new products or loyalty scheme rewards by email and/or text message

You can opt out of marketing messages from us at any time. Contact Carol Knight For a copy of our privacy notice, [info@amadeushairandbeauty.com](mailto:info@amadeushairandbeauty.com)

Or click on the link at: <http://www.amadeushairandbeauty.com>

**Data retention policy**

This policy sets out what information Amadeus Hair & Beauty Ltd holds, how long we hold it for and when it will be deleted.

It also covers the procedure to follow regarding data requests.

* Information held by us
* How long is personal data held for?
* Where is personal data held?
* How is personal data deleted?
* Access to personal information, correction and deletion

**INFORMATION HELD BY US**

We hold personal information about:

* Clients
* Former clients and prospective clients
* Employees
* Job applicants

We also hold information about financial transactions relating to these eg services or treatments provided, products bought, payroll information.

**HOW LONG IS PERSONAL DATA HELD FOR?**

We aim not to hold personal data longer than necessary.

Unless requested by an individual, the following types of data will be held for the periods shown below, after which it will be securely deleted or destroyed:

|  |  |
| --- | --- |
| **TYPE OF INFORMATION** | **RETENTION PERIOD** |
| Client general records | 12 months |
| Client health records | 4 years |
| Financial transactions, invoices and supplier details | 6 years |
| Employee records, contracts of employment, changes to terms and conditions, annual leave, training records | While employment continues and up to 6 years after employment ends |
| Payroll and wage records including PAYE, income tax, national insurance, sick pay, redundancy payments | 6 years from the financial year-end in which payments were made |
| Maternity records | 3 years after the end of the tax year in which the maternity pay period ends |
| Job applications (unsuccessful) | 4 months after notifying unsuccessful candidates |
| Emails | One year from the end of the month in which they were received or sent unless a longer period is relevant as above. Emails to and from ex-employees or contractors will be deleted within 2 weeks of them leaving unless these form part of the employment record – see above. |

**WHERE IS PERSONAL DATA HELD?**

Personal data about clients, financial transactions and employees are held on our secure salon software system which is backed up every day or held in secure electronic files electronically which can be accessed only by the Manager & Salon Owner.

Paper records are held in a locked cabinet.

**HOW IS PERSONAL DATA DELETED?**

Personal data is permanently deleted in accordance with the retention periods listed above from:

* Salon software system
* Electronic files
* Emails
* Paper records, which are securely shredded.

**ACCESS TO PERSONAL INFORMATION, CORRECTION AND DELETION**

See our privacy notice at <http://www.amadeushairandbeauty.com>

or email [info@amadeushairandbeauty.com](mailto:info@amadeushairandbeauty.com)

All requests for access to personal information will be handled by The Owner.

Responses to requests will be made within 30 days.

All information relating to the individual will be compiled into a report and collected from:

* Salon software system
* Financial transactions
* Emails
* Other electronic records
* Paper records (where applicable)

**Procedure for personal data breaches**

**Adapt for your salon where shown with square brackets**

This procedure is to be followed if there is a breach of personal data. The person responsible for managing the process is Carol Knight or Charisse Hardy.

All decisions on whether or not to notify the Information Commissioner’s Office (ICO) or individuals affected will be counter-signed by Carol Knight, salon owner.

This procedure covers:

* What is a personal data breach?
* What must be recorded?
* Assessing the likelihood and severity of the adverse consequences of the breach
* When do breaches have to be reported to the ICO?
* What must be reported to the ICO?
* How to report a breach to the ICO
* Telling individuals affected about a breach
* What are the consequences of failing to notify the ICO?

**WHAT IS A PERSONAL DATA BREACH?**

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data.

Examples include:

* access by an unauthorised third party
* deliberate or accidental action by a data controller (the salon or barbershop) or a data processor (third party supplier, who must inform you without undue delay as soon as they become aware of it)
* sending personal data to an incorrect recipient
* computer or data storage devices containing personal data being lost or stolen
* alteration of personal data without permission
* loss of availability of personal data (ie data is made unavailable and this unavailability has a significant negative effect on individuals)

**WHAT MUST BE RECORDED?**

All breaches must be recorded, whether or not they need to be reported to the ICO. If you decide not to report a breach, you must be able to justify this decision and it must therefore be documented.

Record:

* The facts relating to the breach
* Its effects
* Remedial actions taken
* What caused the breach and how a recurrence could be prevented

**ASSESSING THE LIKELIHOOD AND SEVERITY OF THE NEGATIVE CONSEQUENCES OF THE BREACH**

Use the template in Appendix A to help answer the following questions:

* What is the likelihood and severity of the resulting risk to people’s rights and freedoms?
* What are the potential negative consequences to the individuals concerned?
* How serious and substantial are the consequences? Don’t forget this can include emotional distress, as well as financial, physical or material damage.

If there is a high risk of negatively affecting individuals’ rights and freedoms (scoring 6 or more points on the risk assessment template at Appendix 1), then it must be reported to the ICO. This includes personal data breaches notified to you by third party data processors.

You may also need to notify third parties such as the police, insurers, banks or credit card companies who could help to reduce the risk of financial loss to individuals.

**WHEN DO BREACHES HAVE TO BE REPORTED TO THE ICO?**

Breaches which are likely to result in a high risk of negatively affecting individuals’ rights and freedoms must be reported **no later than 72 hours** after you first become aware of it. If you take longer than this, the reasons for delay must be documented.

**WHAT MUST BE REPORTED TO THE ICO?**

A description of the nature of the personal data breach including:

* The categories and approximate number of individuals concerned and the categories and approximate numbers of personal data records concerned (which may be the same number)
* The name and contact details of the person who can provide more information if required
* The likely consequences of the personal data breach
* The measures taken, or proposed to be taken, to deal with the personal data breach including measures taken to mitigate any possible negative effects

The information can be provided in phases if it is not all available within 72 hours, as long as this is still done without undue further delay and you tell the ICO when to expect further information from you.

You must prioritise the investigation, give it adequate resources and deal with it urgently.

**HOW TO REPORT A BREACH TO THE ICO**

The section of the ICO website on reporting breaches has not yet been updated for GDPR. However, the following contact details are provided:

Data breaches : Call 0303 123 1113

Open Monday to Friday between 9am and 5pm, closed after 1pm on Wednesdays for staff training.

**TELLING INDIVIDUALS AFFECTED ABOUT A BREACH**

If the breach is likely to result in a high risk to the rights and freedoms of individuals (scoring 6 or more on the more points on the risk assessment template at Appendix 1), you must inform the individuals affected as soon as possible.

One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

You need to tell individuals:

* The nature of the personal data breach
* The name and contact details of the person who can provide them with more information
* The measures taken or proposed to be taken to deal with the personal data breach and the measures taken to mitigate any possible adverse effects

If you decide not to notify individuals, you still need to notify the ICO unless you can show that the breach is unlikely to result in risks to rights and freedoms. The ICO has the power to make you inform individuals if they consider there is a high risk. The decision-making process must be documented.

**WHAT ARE THE CONSEQUENCES OF FAILING TO NOTIFY THE ICO?**

A fine of up to 10 million euros or 2% of your turnover or a fine of up to 20 million euros or 4% of your turnover in the most severe case.