SHINE
HAIRDRESSING

Procedure for personal data breaches

This procedure is to be followed if there is a breach of personal data. The person responsible for managing the process is Leigh Anthony, Company Director with Helene Rolfe who would deal with breaches if that first person is absent.

All decisions on whether or not to notify the Information Commisioner's Office (ICO) or individuals affected will be counter-signed by the Company Director Leigh Anthony.

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 cases.

Appendix A – risk assessment template for personal data breaches

COMPLETING THE RISK ASSESSMENT TEMPLATE

Step 1

Provide brief details of the personal data breach, when it happened, how it happened and who has been affected.

Step 2

List all the possible adverse consequences of the data which has been lost, altered or access by an unauthorised person.

Step 3

How likely are those adverse consequences to occur?

Low likelihood - 1 point Medium likelihood - 2 points High likelihood - 3 points

Step 4

How serious would those adverse consequences be if they did occur?

Low impact - 1 point Medium impact - 2 points High impact - 3 points

Step 5

Produce an overall score by multiplying the points in columns 2 and 3 eg if a negative consequence is unlikely (1 point) but if it happened the impact would be high (3 points), the overall score will be 3.

Anything scoring 6 points or more must be reported to the ICO and to the individuals concerned.

What happened? When did it happen? How did it happen? Who has been affected?

List all the possible consequences of the data being lost, altered or accessed by an unauthorised person	**How likely is it there will be negative consequences?** 1, 2, 3 points	**How severe would negative consequences be?** 1, 2, 3 points	**Combined**
1			

2			
3			
4			
5			

Continue on another sheet if necessary

Form completed by .....