Information Management policy

AME Aesthetics

|  |  |
| --- | --- |
| Date Effective: | 01/02/2022 |
| Review Date: | 01/02/2023 |
| Version No: | 1 |
| Policy Owner / Author: | Aimee Fletcher |

## Reason for Policy / Purpose of Policy

Information management is vital to the delivery of our services in an orderly, efficient, and accountable manner. Effective information management will help ensure that we have the right information at the right time to make the right decisions. It will provide evidence of what we do and why. The purpose of this policy is to ensure clients who receive treatment from AME Aesthetics are comfortable in entrusting their information to the company. This policy provides information to clients as to how their personal information is collected and used within the company.

## Policy Statement and Aims

We aim to balance our commitment to openness and transparency with our responsibility as an effective company. So, we will create and manage records efficiently, make them accessible where possible, protect and store them securely and dispose of them safely at the right time.

By following this policy, the aim is to ensure that the recording of information, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to:

• help us carry out our business.

• help us to make informed decisions.

• protect the rights of clients.

• track policy changes and development.

• make sure we comply with relevant legislation.

• provide an audit trail to meet business, regulatory and legal requirements.

• support continuity and consistency in management and administration.

• make sure we are open, transparent, and responsive.

• support research and development; and

• promote our achievements

## Scope

AME Aesthetics is committed to protecting and respecting client’s privacy. This policy sets out the basis which of any personal details we collect from clients or are provided by us will be within the General Data Protection Regulation (GDPR) guidelines.

## Definitions

Any relevant definitions, specific to this policy.

|  |  |
| --- | --- |
| **The General Data Protection Regulation (GDPR) and personal data** | The GDPR was launched in 2016, intending to provide one set of privacy laws for the European Union.  The GDPR provides guidelines for organizations and businesses regarding how they handle information that relates to the individuals with whom they interact. It has made it easier for the citizens of the European Union to understand their rights when it comes to their personal information, and it should be used.  This is important because technology is changing faster than ever, and personal data is evolving with it. The smartphone has become central to the modern world, and almost half of the world’s population has social media accounts.  This has drastically changed the nature of the personal information that we share. It now includes biometric data, like fingerprint identification and retina scans, and location data from IP addresses and Google Maps. For this reason, our personal information is more vulnerable than ever. |
| **Personal Data** | The basic definition of personal data is any information relating to an identified or identifiable natural person (data subject).  In other words, any information that obviously relates to a particular person and can be used to identify them.  The GDPR states that data is classified as “personal data” an individual can be identified directly or indirectly, using online identifiers such as their name, an identification number, IP addresses, or their location data.  And if these online identifiers give information specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.  In some circumstances, even information related to a person’s job, hair color, or political opinions could be classed as personal data. Usually, this comes down to the context in which the data was collected and whether a data subject could be directly or indirectly identifiable. |
| **Examples of personal data** | The definition of personal data is any information relating to an *“identified or identifiable natural person.”* When most people think of personal data, they think of phone numbers and addresses; however, personal data covers a range of identifiers.   * Name and surname. * Email address. * Phone number. * Home address. * Date of birth. * Race. * Gender. * Political opinions. * Credit card numbers. * Data held by a hospital or doctor. * Photograph where an individual is identifiable. * Identification card number. * A cookie ID. * Internet Protocol (IP) address * Location data (for example, the location data from a mobile phone). * The advertising identifier of your phone.   Personal data relating to GDPR does not cover:  Information about someone who is deceased.  Properly anonymized data.  Information about public authorities and companies. |
| **Data Controller** | A data controller determines the purposes and means of processing the personal data. |
| **Data Processor** | A processor is responsible for processing personal data on behalf of a controller. |
| **Data Subject** | The data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person’s physical, physiological, genetic, mental, economic, cultural, or social identity. |
| **Third-party** | As per the GDPR, "third party" means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data. |

## Procedure

At AME Aesthetics we are the data controllers. This means we decide how the client’s personal data is processed and for what purposes.

Our purposes of processing data are the following:

* Recording clients’ bookings on our secure online booking system.
* Recording clients email addresses to contact them of their appointment and to give any updates or news within the clinic.
* Recording clients contact numbers to contact them of their appointment.
* Recording clients name, date of birth as identification within medical notes.

**Clients’ data rights:**

**1. The right to be informed**We have a duty to inform you how your data will be used and to ensure that it is clear and concise, and easily accessible.

**2. The right of access**  
You have a right to understand what personal data is being processed and have access to this personal information. This is usually referred to as a Subject Access Request (SAR).

**3. The right to rectification**  
You have a right to have your personal data corrected if you believe there are inaccuracies, or it is incomplete.

**4. The right to erasure**  
You have a right to have your personal data erased, this is also known as the right to be forgotten. This broad principle gives you the right to have your personal data removed if there is no compelling justification or legislative / regulatory reason to either retain your personal data or continue processing.

**5. The right to restrict processing**  
You have a right to block or suppress processing of your personal data under certain circumstances.

**6. The right to data portability**  
You have a right to data portability, which allows you (in certain circumstances) to have your personal data ported across to another environment/organisation, in a safe and secure way.

**7. The right to object**  
You have a right to object to the processing of your personal data under certain circumstances.

**8. Rights in relation to automated decision making and profiling.**  
We do not use any automated decision making or profiling as part of our activities.  
**How to access the information we hold about you (known as a Subject Access Request)**

To make a request please contact the following via email: [aimee@ameaesthetics.com](mailto:aimee@ameaesthetics.com)

It is required to ensure that personal data that we process is:

* Relevant, adequate, and not excessive
* accurate and up to date
* not held for longer than is necessary

Complying with these obligations is important to protect individual privacy. AME Aesthetics will therefore review periodically the customer data it collects to ensure that this data is adequate and relevant to the services we provide and is not excessive. We will also make our records accordingly. All information will be disposed of securely when no longer required.

Clients are under no obligation to share personal data however failure to do so will have the following consequences of AME Aesthetics unable to carry out any treatments to the client. At AME Aesthetics we require personal data as a statutory requirement necessary to enter a contract that involves the recording and documentation of the client’s medical pathway.

## Responsibilities

At AME Aesthetics it will only be the company director (Aimee Fletcher) who will have access to personal data and will be responsible for complying with this policy and with other relevant policies and procedures relating to data handling. All information will be secured electronically on tablet that will be kept locked and secured within the premises. All data will be kept secured for three years then will be deleted once no longer required. It is the company director (Aimee Fletcher) who must comply with these policies and procedures.

## Related information

Legislation - Scottish Statutory Instrument No 182 (4) <http://www.legislation.gov.uk/ssi/2011/182/contents/made>

Legislation - Freedom of Information [www.legislation.gov.uk/asp/2002/13/contents](http://www.legislation.gov.uk/asp/2002/13/contents)

Caldicott Guardian <http://www.gov.scot/Publications/2011/01/31115153/0>

Guidance - Data protection <https://ico.org.uk/for-organisations/>

Health and Social Care Standards <http://www.newcarestandards.scot/>