1. Introduction

1.1 Data Categories

Aesthetic Response specialises in providing call response and appointment making services for the aesthetic procedures market and as such, needs to gather and use certain information about individuals.

These include:-

- ◦ The General Public
  ◦ Patients (new, existing, former)
  ◦ Callers (individual seeking advice and information)
  ◦ Next of kin (new, existing)
  ◦ Guardians (new, existing)

- B2B Clients, Contacts, Partners
  ◦ Clinics and Practitioners (set-ups, existing, former)
  ◦ General Practitioners (Gps)
  ◦ Private Hospitals
  ◦ Training Providers

- Employees
  ◦ All staff (current, former)
  ◦ Candidates (recruitment)

- Suppliers
  ◦ Hardware and software
  ◦ IT consultancy
  ◦ HR Services
  ◦ Accounting Services
  ◦ Other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

1.2 Why this policy exists

This data protection policy ensures Aesthetic Response:

• Complies with data protection law and is GDPR compliant;

• Protects the rights of staff, clients, B2B contacts and partners and the general public;

• Is open about how it stores and processes individuals' data;

• Protects itself from the risks of a data breach.

1.3 Data protection law

The Data Protection Act 1998 describes how organisations — including Aesthetic Response must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

2 People, risks and responsibilities

2.1 Policy scope

This policy applies to:

• The head office of Aesthetic Response;

• All staff of Aesthetic Response;

• Partners – Clinics and Practitioners;

• All contractors, suppliers and other people working on behalf of Aesthetic Response.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 such as information included in the new GDPR legislation which will be introduced in May 2018.

This can include:

2.2 Patients

• Basic Contact Details: name, sex, address, postcode, home telephone number, mobile telephone number, date of birth, email address, company.

Note: some patients are 'well known' and have a high public profile

• Enquiry type.

• GP Details: practice, GP name, address, telephone number.

• Procedure: i.e. treatment details, health issues.

• Call Notes: free text box recording comments and data pertinent for each call.

Note: personal data recorded can include sensitive information on treatments and health conditions and post treatment concerns.

• Credit card details.

2.3 Clinics and Practitioners

• Clinic Details: clinic name, address, postcode, main clinic telephone number, procedures, clinic opening hours, clinic policies.

• Clinic Admin Staff: name, position, telephone number, mobile number, email, working days/hours, other information.

• Consultant Details: practitioner name, qualifications, memberships, emergency contact details, consultant profile, consultations, usual clinic days.

• Other Details: cosmeceutical products, anecdotal notes.

• Clinic Payments and Finance: bank account name, bank account number, bank sort code.

2.4 Employees

• Basic Contact Details: name, address, postcode, telephone number, mobile telephone number, date of birth, personal email address.

• Person to be notified in an emergency: name, address, post code, telephone number, mobile telephone number.

• Bank Details: name of bank, bank address, account number, sort code.

• Tax and PAYE: National Insurance Number, P45/46/60s.

• Personnel Records: contract, 1-2-1's, appraisals, training, annual leave, pensions, expenses, absence, performance, disciplinary.

• Recruitment records: interview notes, CVs, application form, references.

2.5 Suppliers

• Business Contact Details: name, address, postcode, telephone number, mobile telephone number (includes multi-sites).

• Supplier contracts and SLA's.

• Supplier products, services and price list.

2.6 Children

- As a processor, AR collect children's data only for appointment booking and treatments and do not use their personal data in the context of commercial internet services such as social networking.
- There is a mandatory box which must be ticked by the person completing the online form on the AR website to inform that they are 16 years and over
- As controllers the clinics sets the age when a child can give their own consent to processing their information at 16. If a child is younger, then clinics require to get consent from a person holding 'parental responsibility'. Guardian consent must be verifiable before any processing of personal information is undertaken'

3. Data protection risks

This policy helps to protect Aesthetic Response from data security risks, including:

• Breaches of confidentiality. For instance, information being given out inappropriately;

• Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them;

• Reputation damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

4. Responsibilities

Everyone who works for, or with, Aesthetic Response has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team member that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The Board of Directors is ultimately responsible for ensuring that Aesthetic Response meets its legal obligations.

4.1 The Compliance Director, is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies, in line with an agreed schedule;
- Arranging data protection training and advice for the people covered by this policy;
- Handling data protection questions from staff and anyone else covered by this policy;
- Dealing with requests from individuals to see the data Aesthetic Response holds about them (also called 'subject access requests');
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data;
- Maintain, update and review privacy notice to ensure compliance with GDPR implementation.

4.2 The IT Systems Manager is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- Performing regular checks and scans to ensure security hardware and software is functioning properly;
- Evaluating any third-party services the company is considering using to store or process data.

4.3 The Commercial Director is responsible for:

- Ensuring that personal data provided by clinics and practitioners for the purposes of Direct Marketing, only includes contact details of individuals who have opted-in and given their consent for their personal data to be used in this way;
- To check, before each promotion or marketing campaign that personal data for Direct Marketing purposes has been supplied by Clinics and Practitioners who have signed the AR Service agreement;
- Approving any data protection statements attached to communications such as emails and letters;
- Addressing any data protection queries from journalists or media outlets like newspapers;
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

4.4 General staff guidelines

• The only people able to access data covered by this policy should be those who need it for their work.

• Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

• Aesthetic Response will provide training to all employees to help them understand their responsibilities when handling data.

• Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

• In particular, strong passwords must be used and they should never be shared.

• Personal data should not be disclosed to unauthorised people, either within the company or externally.

• Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

• Employees should request help from their line manager or the Compliance Director if they are unsure about any aspect of data protection.

5. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Compliance Director.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

Any written information should be stored in a securely locked cabinet every evening, at the end of each call handler's shift. When any written note becomes obsolete this should be placed in the locked waste disposal to be collected by a 3rd party contractor for shredding.

Hard copy patient enquiry forms received directly via client enquiry email addresses should be filed daily in a working folder. Outside office hours, this folder should be securely locked in its allocated cabinet.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

• When not required, the paper or files should be kept in a locked drawer or filing cabinet;

• Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer;
• Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
• Data should be protected by strong passwords that are changed regularly and never shared between employees;
• If data is stored on removable media it should be encrypted and be kept locked away securely when not being used;
• Data should only be stored on designated drives and servers, and should only be uploaded to Aesthetic Response internal storage;
• Servers containing personal data should be sited in a secure location, away from general office space, accessible by authorised personnel only;
• Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures;
• Data should never be saved directly to laptops or other mobile devices like tablets or smart phones;
• All servers and computers containing data should be protected by approved security software and a firewall.

5.1 Data use

Personal data is of no value to Aesthetic Response unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:
•When working with personal data, employees should ensure the screens of their computers are always locked when left unattended;
• Personal data should not be shared informally;
• Personal data should never be transferred outside of the European Economic Area;
• Employees should not save copies of personal data to their own computers;
• Always access and update the central copy of any data;

5.2 Data accuracy

The law requires Aesthetic Response to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Aesthetic Response should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

• Data will be held in as few places as necessary. Employees should not create any unnecessary additional data sets;
• Employees should take every opportunity to ensure data is updated. For instance, by confirming a patient's details when they call;
• Aesthetic Response should make it easy for data subjects to update the information Aesthetic Response holds about them;
• Data should be updated as inaccuracies are discovered. For instance, if a client can no longer be reached on their stored telephone number, it should be removed from the database;
• It is the Commercial Directors responsibility to ensure marketing databases are updated when clients change, delete their details or withdraw consent.

6. Subject access requests

All individuals who are the subject of personal data held by Aesthetic Response are entitled to:
• Ask what information the company holds about them and why;
• Ask how to gain access to it;
• Be informed how to keep it up to date;
• Be informed how the company is meeting its data protection obligations.

Aesthetic Response aims to ensure that individuals are aware that their data is being processed, and they understand they have:
• The right to be informed;
• The right of access;
• The right to rectification;
• The right to erasure;
• The right to restrict processing;

• The right to data portability;

• The right to object;

• The right not to be subject to automated decision making including profiling.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Compliance Director at data@aestheticresponse.co.uk. The Compliance Director can supply a standard request form, although individuals do not have to use this.

Making a request for personal data is free unless a reasonable cost is to be charged where requests are unfounded or excessive or repetitive in character.

Subject Access requests are dealt with without undue delay and the Compliance Director will co-ordinate, gather and dispatch the requested data within one month.

The Compliance Director may contact the Data Subject to be sure we have enough information to be sure of the requester's identity and ask further questions to ensure we have all the information from the requester to find what they want.

Before providing a copy of the information in a permanent form (unless the individual agrees otherwise), the Compliance Director will take into account:

- If the information will be changed between receiving the request and sending the response;
- Does it include information about other people? If so, the response will disclose as much information as possible by redacting the references to other people;
- if all the information that the requester wants is exempt from subject access;
- If a request is refused or to be charged, Aesthetic Response will tell the individual why, within one month, informing them they have the right to raise this with the Compliance Director in the first instance and then to a supervisory authority and pursue a judicial remedy.

6.1 Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Aesthetic Response will disclose requested data. However, the Compliance Director will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

6.2 Providing information

Aesthetic Response has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the company's website.

Requests from individuals relating to their personal data should be made by email, addressed to the Compliance Director at data@aestheticresponse.co.uk who can supply a standard request form, although individuals do not have to use this.

Requests for rectifying, objecting, erasing, restricting processing (including profiling), obtaining personal information in a portable format will not be charged unless requests are unfounded or excessive or repetitive in character.

7. Deleting Personal Data

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Therefore, Aesthetic Response comply with the DPA, in particular the fifth data protection principle, when archiving or deleting personal information.

7.1 Physical and Equipment Security

Regarding secure disposal or re-use of equipment, Aesthetic Response adhere to the policies below:

- Hard disks are cleared of all software and all organizational information prior to disposal or re-use, as set out below.
- The Compliance Director is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through her office.
- A log is retained showing what media were destroyed, disposed of, and when. The asset inventory is adjusted once the asset has been disposed of.

- Equipment with memory devices is 'wiped'/sanitised and then may be sold or given to employees or others. If necessary, the device(s) are put beyond practical use.
- Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.
- Portable or removable storage media of any description are destroyed prior to disposal.
- All media are disposed of in line with WEEE regulations on disposal of computer equipment, through the Aesthetic Response's approved contractor. The contractor is a licensed waste carrier and relevant Waste Transfer Notes are retained by the Compliance Director for a minimum of two years.
- Documents containing confidential information which are to be destroyed are shredded by their owners or disposed of as confidential waste. The contractor employed is a registered waste carrier and provides Certificates of Destruction where appropriate and Waste Transfer notes which are retained by the Compliance Director for a minimum of two years.

8. Data Subjects Complaints Process

Complaints raised by Data Subjects at any time relating to issues such as Aesthetic Response:-

- Not keeping information secure;
- Holding information that is inaccurate;
- Incorrectly disclosing information about them;
- Keeping information about you for longer than is necessary;
- Has collected information for one reason and is now using it for something else; or
- Has sent you someone else's personal information.

Complaints should be made by email, addressed to the Compliance Director at data@aestheticresponse.co.uk. The Compliance Director can supply a Data Subject Complaints form, although individuals do not have to use this.

The Compliance Director will contact the Data Subject to validate the complainant's identity and ask further questions to ensure we fully understand the complaint.

Before providing a full response, the Compliance Director will take into account:

- If the information will be changed between receiving the request and sending the response;
- Does it include information about other people? . If so, the response will disclose as much information as possible by redacting the references to other people;
- If the complaint is valid.

The Compliance Director will try to remedy the situation within 30 days.

If the Data Subject is not satisfied with the response given regarding their complaint, they can submit details of the complaint to the Aesthetic Response Commercial Director for further investigation

Throughout the complaint the Data Subject will be informed that they have the right to at any time to pursue their complaint with a statuary body and be provided with ICO helpline telephone number 0303 123 1113 and URL https://ico.org.uk/global/contact-us/helpline/ for the ICO helpline or chat line.

9. Providing Data

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Aesthetic Response or Aesthetic Response holds, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance.

Aesthetic Response will whenever possible, utilise file standards that allow for easy reuse, encompassed by a "structured, commonly used, machine-readable" Open Standard.

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on website.