DATA PROTECTION POLICY STATEMENT (TIER 1)

Introduction - Privacy and data protection as a key policy for Clients

Energize Aesthetic's commitment to protecting privacy and data protection has been adopted as a key policy which underpins both this Data Protection Policy and other associated policies used by Energize Aesthetic and its clientship.

1. Purpose of this Data Protection policy and what it covers

This policy sets out Energize Aesthetic's approach to protecting personal data and explains your rights in relation to how we may process personal data. More detail in respect of how we process and protect your data is provided below, in particular in section 5.

Energize Aesthetic ("We" in this document) is registered with the Information Commissioner's Office at the following address: 92, Dalry Road, Edinburgh, EH11 2AX. If you have any queries about anything set out in this policy or about your own rights, please write to the **GDPR Champion** at the above address .

We may update this policy from time to time in minor respects, although we will make sure that any substantial or significant changes will be notified to you directly.

2. Some Important Definitions

'We' means Energize Aesthetic
'ICO' is the Information Commissioner's Office, the body responsible for enforcing data protection legislation within the UK and the regulatory authority for the purposes of the GDPR
'Clients' mean Gym Clients
'**Personal Data**' is defined in section 3
'Processing' means all aspects of handling personal data, for example collecting, recording, keeping, storing, sharing, archiving, deleting and destroying it.
'**Data Controller**' means anyone (a person, people, public authority, agency or any other body) which, on its own or with others, decides the purposes and methods of processing personal data. We are a data controller insofar as we process personal data in the ways described in this policy.
'**Data processor'** means anyone who processes personal data under the data controller's instructions, for example a service provider. We act as a data processor in certain circumstances.
'**Subject Access Request'** is a request for personal data that an organisation may hold about an individual. This request can be extended to include the deletion, rectification and restriction of processing.

3. What is personal data?

Personal data means any information about an identified or identifiable person. For example, an individual's home address, personal (home and mobile) phone numbers and email addresses, occupation, and so on can all be defined as personal data.

Some categories of personal data are recognised as being particularly sensitive ("sensitive personal data"). These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic and biometric information, and data concerning a person's sex life or sexual orientation.

4. How does data protection apply to Clients?

Data protection legislation applies to all data controllers regardless of whether they are charities or small organisations. It applies to Clients in the same way as it does to other organisations.

5. What type of personal data do we collect and why?

5.1 Clients

Our business is about Aesthetics. We may hold personal data (including sensitive personal data) about clients on our clientship systems. We believe it is important to be open and transparent about how we will use your personal data. Information we may hold about you includes the following:

- name and contact details
- age/date of birth
- details of any health conditions
- photograph

We need this information to communicate with you. We also have a responsibility to keep information about you, both during your clientship and afterwards (also to help us if you leave or re-join).

Much of this information is collected from the member joining forms

5.2 Employees (past, present and future)

As an employer, we need to keep information relating to each member of staff who has a contract with us. This will include the pre-employment stage, references, and records relating to the time they worked for us, including probationary, appraisal and disciplinary information.

We also hold information that allows us to pay salaries and work with other payroll and pension providers. Information we may hold about staff includes the following:

- name and contact details
- length and periods of service (and absence from service)
- details of training you receive
- details of your experience, qualifications, occupation, skills
- details of next of kin
- age/date of birth
- details of any health conditions
- details of disclosure checks if applicable
- staff id badges
- details of any dependents
- information that allows us to pay salaries and work with other payroll and pension providers references, and records relating to the time they worked for ENERGIZE AESTHETIC, probationary, appraisal and disciplinary information.

Much of this information will be taken from the job application form.

5.3 Trustees and clients of the governance structure

For the clients of Energize Aesthetic's Board of Directors, we may hold the type of information as set out in 5.1 and also including the following:

- CVs
- Related party information

5.4 Potential customer lists

We benefit from holding lists about potential customers. We may hold the type of information as set out in 5.1.

5.5 Customers and visitors

We also hold personal data from customers and visitors to gym. We may hold the type of information as set out in 5.1 and also including the following:

- purchase history
- taxpayer and payment details

Much of this information is taken from online registration forms.

5.6 CCTV

Our gym operates a CCTV network to help prevent and detect crime and safeguard (protect) people and others. If we can identify somebody from a CCTV image, the image must be processed as personal data.

6. Conditions for collecting personal data

6.1 Keeping to the law

We must keep to the law when processing personal data. To achieve this, we have to meet at least one of the following conditions:

- you have to give (or have given) your permission for us to use your information for one or more specific purposes
- we need to process the information to meet the terms of any contract you have entered into
- processing the information is necessary to keep to our legal obligations as data controller
- processing the information is necessary to protect your vital interests
- processing the information is necessary for tasks in the public interest or for us as the data controller to carry out our responsibilities
- processing the information is necessary for our legitimate interests (see below)

Also, information must be:

- processed fairly and lawfully
- collected for specified, clear and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- processed securely

6.2 Information that we share

We may have to share your personal data within appropriate levels of the Energize Aesthetic, . We do not share personal data with companies, organisations and people outside the Organisation, unless one of the following applies;

- We have clear permission from you to do so.
- If we have to supply information to others (for example payroll providers) for processing on our behalf. We do this if we are asked and to make sure that they are keeping to the GDPR and have appropriate confidentiality and security measures in place.
- For safeguarding young people or for other legal reasons.

7. Keeping personal data secure

Everyone who handles personal data (including staff, clients, volunteers, payroll and pension providers) must make sure it is held securely to protect against unlawful or unauthorised processing and accidental loss or damage. We take appropriate steps to make sure we keep all personal data secure, and we make all of our staff aware of these steps, including keeping to our internal

information and computing technology (ICT) policy. In most cases, personal data must be stored in appropriate systems and encrypted when taken off-site. The following is general guidance for everyone working within Clients, including staff.

- You must only store personal data on networks, drives or files that are password protected and regularly backed up.
- You should have proper entry-control systems in place, and you should report any stranger seen in entry-controlled areas.
- You should keep paper records containing personal data secure. If you need to move paper records, you should do this strictly in line with data protection rules and procedures.
- You should not download personal data to mobile devices such as laptops and USB sticks unless absolutely necessary. Access to this information must be password protected and the information should be deleted immediately after use.
- You must keep all personal data secure when travelling.
- Personal data relating to clients and volunteers should usually only be stored on the clientship database or other specific databases which have appropriate security in place.
- When sending larger amounts of personal data by post, you should use registered mail or a courier. Memory sticks should be encrypted.
- When sending personal data by email this must be appropriately authenticated and password protected. Do not send financial or sensitive information by email unless it is encrypted.
- You should not share your passwords with anyone.
- Different rights of access should be allocated to users depending on their need to access personal or confidential information. You should not have access to personal or confidential information unless you need it to carry out your role.
- Before sharing personal data with other people or organisations, you must ensure that they are GDPR compliant.
- In the event that you detect or suspect a breach you should follow your defined breach response process.

All staff undertake regular training to ensure that they are aware of the above rules

8. Responsibilities

We expect our staff, managers, directors, clients and any providers we use (for example payroll or pension providers) to keep to the guidelines as set out in our Data Policy and under ICO and GDPR guidance when they are using or processing personal data and other confidential or sensitive information. This is set out more clearly below.

8.1 Board of Directors

Our Board of Directorsd has overall responsibility for Energize Aesthetic and for making sure that we keep to legal requirements, including data protection legislation. Our General Manager and senior team are responsible for making sure we keep to these requirements across Energize Aesthetic.

8.2 Data protection officer (DPO) or equivalent role holder

Energize Aesthetic has externally appointed a DPO to ensure the organisation is monitoring compliance with GDPR and other Data Protection laws, our data protection policies, awareness- raising, training, and audits. Local Clients Units should consider appointing their own DPO. The data protection officer is responsible for:

- making sure that this data protection policy is up to date
- advising you on data protection issues
- dealing with complaints about how we use personal and sensitive personal data reporting to the ICO if we do not keep to any regulations or legislation

8.3 Staff

All staff have a responsibility to keep to the requirements of this data protection policy and our related procedures and processes. Managers are responsible for making sure that staff within their teams are aware of and keep to this. If you become aware of a data protection issue you must report it promptly to the data protection officer or equivalent role holder.

If you do not keep to this data protection policy and its associated policies and procedures, we may take disciplinary action against you.

8.4 Clients

We expect you to keep to data protection legislation and this data protection policy, and to follow the relevant rules set out in our Policy, Organisation and Rules (POR).

As part of your data protection duties, you should report urgently any instance where the rules on how we handle personal data are broken (or might be broken).

9. Data Retention

We may keep information for different periods of time for different purposes as required by law or best practice. Individual departments include these time periods in their processes. We make sure we store this in line with our Data Retention Policy.

As far as clientship information is concerned, to make sure of continuity (for example if you leave and then re-join), we keep your clientship information throughout your clientship and after it ends, and we make sure we store it securely.

Only those staff who need clientship information to carry out their role have access to that information.

10. Rights to accessing and updating personal data

Under data protection law, individuals have a number of rights in relation to their personal data.

(a) The right to information: As a data controller, we must give you a certain amount of information about how we collect and process information about you. This information needs to be concise, transparent, understandable and accessible.

(b) The right of subject access: If you want a copy of the personal data we hold about you, you have the right to make a subject access request (SAR) and get a copy of that information within 30 days.

(c) The right to rectification: You have the right to ask us, as data controller, to correct mistakes in the personal data we hold about you.

(d) The right to erasure (right to be forgotten): You can ask us to delete your personal data if it is no longer needed for its original purpose, or if you have given us permission to process it and you withdraw that permission (or where there is no other lawful basis for processing it).

(e) The right to restrict processing: In certain circumstances where, for lawful or legitimate purposes we cannot delete your relevant personal information or if you do not want us to delete it, we can continue to store it for restricted purposes. This is an absolute right unless we have a lawful purpose to have it that overwrites your rights.

(f) The obligation to notify relevant third parties: If we have shared information with other people or organisations, and you then ask us to do either (c), (d) or (e) above, as data controller we must tell the other person or organisation (unless this is impossible or involves effort that is out of proportion to the matter).

(g) The right to data portability: This allows you to transfer your personal data from one data controller to another.

(h) The right to object: You have a right to object to us processing your personal data for certain reasons, as well as the right to object to processing carried out for profiling or direct marketing.

(i) The right to not be evaluated on the basis of automatic processing: You have the right not to be affected by decisions based only on automated processing which may significantly affect you.

(j) The right to bring class actions: You have the right to be collectively represented by not-for-profit organisations.

11. Subject access requests

You are entitled to ask us, in writing, for a copy of the personal data we hold about you. This is known as a subject access request (SAR). In line with legislation, we will not charge a fee for this information and will respond to your request within one month. This is unless this is not possible or deemed excessive, in which case we will contact you within the month of making the SAR.

12. Further information and contacts

Subject access requests

Subject access requests for data held by Energize Aesthetic should be made to our team at office@energizeaesthetic.co.uk or by writing to:

Energize Aesthetic 92 Dalry Road Edinburgh EH11 9AX

Please note, Subject Access Requests for data held should be made directly to the address above.

Contact the Information Commissioner's Office

Appendix - Index of related policies and procedures

Privacy Statement

Energize Aesthetic collects personal data in order to carry out its business. As a clientship organisation we hold data on clients and also staff and others, such as customers and donors. We take the issue of privacy very seriously and are committed to protecting and respecting your privacy in compliance with data protection law. This includes when you use our online services and this privacy statement should also be read alongside our website terms and conditions.

1. The information we collect

Clientship Data

When a member registers with Energize Aesthetic we ask for their name, email address and postcode. We will also capture the IP address at the time of registration. We also maintain an ongoing record of clients' activities.

We have security measures in place to protect our customer database. Access to the clientship database is restricted. However, it is the responsibility of each member to:

- keep their password secret
- protect against unauthorised access to your personal details
- to log off from any service when not using it, and

We need to make clients aware of this when they register with us as should you request at a later stage that we remove all your data, we will not be able to comply with this request.

2. Sharing information

We will not share your data with third parties without your permission.

3. Advertising

Our website or other publications may include advertising for other businesses as part of our operation. We may use, and provide to third parties, your contact details but only if you have given explicit consent for us to do so.

4. Legal Jurisdiction

All personal data and details held on and processed by computers situated in the United Kingdom.

5. Further Clients related information

We will, as part of our normal operation, communicate information to clients which is relevant to their role in Clients. In addition our website sends out emails with information to our clients. However, clients can decide which emails they wish to receive as they register.

6. Disclosure of data by law or order of a Court

We may be required to communicate the personal data we hold on a member to a third party if required by law, e.g. regulation or statute or by order of a court.

7. Data Protection legislation

Energize Aesthetic adheres to the key principles set out in current data protection legislation.

You can obtain more information about data protection legislation from the Information Commissioner's Office or if you wish to make a complaint about how we handle your data you can contact them here.

8. Use of Cookies

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site.

The table below explains the cookies we use and why.

Cookie	Name	Purpose	More information
Google Analytics	_utma _utmb _utmc _utmz	These cookies are used to collect information about how visitors use our site. We use the information to put reports together and to help us improve the site. The cookies collect information in an anonymous form, including information about the number of visitors to the site, where visitors have come to the site from, and the pages they visited.	Click here for an overview of privacy at Google.
Module cookies	Module_layout1 module_layout2 module_layout3 module_open	These cookies are used to store your personal homepage layout of our home page.	We are working towards developing a new system that will remove the need for this cookie.
Session cookies	res_width res_height PHPSESSID	These cookies make the most effective use of your screen resolution for user logged-in areas. Session cookies only	These cookies are essential for running the site and member areas.

		last as long as your browser is open.	
Style cookies	style	These cookies decide your default font size for our website. (You can increase or decrease the font size on the main menu of your website.)	We are working towards developing a new system that will remove the need for this cookie.

9. Google Analytics

Visitors to this website who have javascript enabled are tracked using Google Analytics. Google Analytics collects the following types of information from users:

- Type of user agent (web browser) used, software manufacture and version number.
- Type of operating system.
- Screen colours (colour processing ability of the user's screen) Javascript support
- Flash version
- Screen resolution
- Network location and IP address
- Can include country, city, state, region, county or any other geographical data
- Hostname
- Bandwidth (internet connection speed)
- Time of visit
- Pages visited
- Time spent on each page of the website
- Referring site statistics
- The website (URI) the user came through in order to arrive at this website (example: clicking on a hyperlink from Yahoo.com that took the user to this website)
- Search engine query used (example: typing in a phrase into a search engine like Google, and clicking on a link from that search engine)

This data is only used to optimise our website for our visitors.

This data does not include any personalised identification information such as:

Names

Phone numbers

Email addresses

Mailing addresses

Bank account numbers

Credit card information

We may amend this policy at any time in response to your feedback, new or altered systems and procedures, Internet best practices and UK and European law.

10. Contacting us

If you want to contact us to raise any questions about this privacy statement or any general matters relating to Energize Aesthetic, you can contact us using this email office@energizeaesthetic.co.uk or at the following address.; Energize Aesthetic, 92 Dalry Road, Edinburgh EH11 2AX

Alternatively, if your query relates specifically to data protection you can contact the Data Protection Officer at office@energizeaesthetic.co.uk

Document Owner and Approval

The Data Protection Officer / GDPR Owner is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all clients of staff on the *shared drive* and is published *on our web site*.

This policy was approved by the Board on *07.12.20* and is issued on a version controlled basis under the signature of the General Manager.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Stephen Day	07.12.20
2	Final Version	Stephen Day	07.12.20