British College of Aesthetic Medicine

Data Protection Policy – GDPR Compliant

1. Introduction

This Policy sets out the obligations of BACD ta The British College of Aesthetic Medicine ("the Organisation") regarding data protection and the rights of clients, members, business contractors, customers, suppliers, patients and other business contacts ("data subjects") in respect of their personal data under the General Data Protection Regulation (Regulation (EU) 2016/679) ("the Regulation").
The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Organisation, its employees, agents, contractors, or other parties working on behalf of the Organisation.

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the Regulation.

The Organisation is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Please contact the DPO with any questions about the operation of this Policy or the Regulation or if you have any concerns that this Policy is not being or has not been followed.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes

for which it is processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

g) only be transferred to another country with appropriate safeguards being in place.

h) made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data.

3. Data Processing

The Regulation restricts actions regarding personal data to specified lawful purposes. Data processing must be lawful, fair and transparent. These restrictions are not intended to prevent processing but ensure that personal data is processed fairly and without adversely affecting the data subject.

The Regulation allows processing for specific purposes and data processing is lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The legal ground must be identified and documented for each processing activity.

4. Purpose Limitation

4.1 Personal data is collected only for specified, explicit and legitimate purposes. It is not further processed in any manner incompatible with those purposes.

4.2 The Organisation collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data

subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, information transferred from regulators, inspectors, assessors, appraisers, patients, medical or healthcare professionals or members of the public).

4.3 The Organisation only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. Adequate, Relevant and Limited Data Processing

The Organisation will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up to Date

The Organisation shall ensure that all personal data collected and processed is kept accurate, complete, up-to-date and relevant to the purpose for which it is collected. The accuracy of data shall be checked when it is collected and at annual intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Storage Limitation

The Organisation shall not keep personal data in an identifiable form for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay unless a law requires such data to be kept for a minimum period of time.

8. Security of Persona Data

The Organisation shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

9. Record Keeping

Accurate organisational records reflecting the processing of personal data including records of data subjects' consent and procedures for obtaining consent are maintained. These records shall include:

9.1 The Organisation's data protection officer is Dr Philip Dobson secretary@bcam.ac.uk.

9.2 The Organisation shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the Organisation, its data protection officer, and any applicable third-party data controllers;

b) Details of the types of personal data collected, held, and processed by the

Organisation; and the categories of data subject to which that personal data relates;

c) The purposes for which personal data is processed;
d) Personal data storage locations
e) Details (and categories) of any third parties that will receive personal data from the Organisation;
f) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
g) Personal data retention periods; and
h) Detailed descriptions of all technical and organisational measures taken by the Organisation to ensure the security of personal data.

10. Privacy Impact Assessments

The Organisation shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Organisation's data protection officer and shall address the following areas of importance:

10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
10.2 Details of the legitimate interests being pursued by the Organisation;
10.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
10.4 An assessment of the risks posed to individual data subjects; and
10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;
b) The right of access;
c) The right to rectification;
d) The right to erasure (also known as the 'right to be forgotten');
e) The right to restrict processing;
f) The right to data portability;
g) The right to object;
h) Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed

12.1 The Organisation shall ensure that the following information is provided to every data subject when personal data is collected:

a) Details of the Organisation including, but not limited to, the identity of its Data Protection Officer;
b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
c) Where applicable, the legitimate interests upon which the Organisation is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
e) Where the personal data is to be transferred to one or more third parties, details of those parties;
f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers);
g) Details of the length of time the personal data will be held by the Organisation (or, where there is no predetermined period, details of how that length of time will be determined);
h) Details of the data subject's rights under the Regulation;
i) Details of the data subject's right to withdraw their consent to the Organisation's processing of their personal data at any time;
j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);
k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;
12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) If the personal data is used to communicate with the data subject, at the time of the first communication; or
b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
c) In any event, not more than one month after the time at which the Organisation obtains the personal data.

13. Data Subject Access

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Organisation holds about them. The Organisation is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).
13.2 All subject access requests received must be forwarded to the Organisation's data protection officer using the details provided in 9.1 above.
13.3 The Organisation does not charge a fee for the handling of normal SARs. The Organisation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. **Rectification of Personal Data**

14.1 If a data subject informs the Organisation that personal data held by the Organisation is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. **Right to Erasure of Personal Data - "right to be forgotten"**

15.1 Data subjects may request that the Organisation erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Organisation to hold that personal data with respect to the purpose for which it was originally collected or processed;
b) The data subject wishes to withdraw their consent to the Organisation holding and processing their personal data;
c) The data subject objects to the Organisation holding and processing their personal data (and there is no overriding legitimate interest to allow the Organisation to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);
d) The personal data has been processed unlawfully;
e) The personal data needs to be erased in order for the Organisation to comply with a particular legal obligation

15.2 Unless the Organisation has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**

16.1 Data subjects may request that the Organisation ceases processing the personal data it holds about them. If a data subject makes such a request, the Organisation shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. **Automated Processing**

The Organisation does not process personal data using automated means.

18. **Objections to Personal Data Processing**

18.1 Data subjects have the right to object to the Organisation processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

18.2 Where a data subject objects to the Organisation processing their personal data based on its legitimate interests, the Organisation shall cease such processing forthwith, unless it can be demonstrated that the Organisation's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the Organisation processing their personal data for direct marketing purposes, the Organisation shall cease such processing forthwith.

18.4 Where a data subject objects to the Organisation processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Organisation is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

18.5 The Organisation shall not be obliged to comply with a request for erasure where and to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by law to which the data controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
c) for reasons of public interest in the area of public health.
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as it would seriously impair the achievement of the objective of the processing.

19. **Automated Decision-Making**

The Organisation does not use personal date in any automated decision-making processes.

20. **Profiling**

The Organisation does not use personal data for profiling purposes.

21. **Personal Data**

The following personal data may be collected, held, and processed by the Organisation:

a) Basic contact data including title, name, address, date of birth, email and telephone numbers, this data is collected, held and processed in order to communicate with the data subject, to enable the establishment or continuation of a business relationship, education and training, financial and billing purposes and to ensure accurate handling of data both internally and in communication with other organisations;

b) Professional registration numbers and details of registrations, places and scope of work, insurance and indemnity arrangements, CV details, trade union membership, passport data and other identification data, dates for appraisals, revalidations, details of appraisal and revalidation information, this data is collected, held and processed in order to establish identity, facilitate management and administration of the appraisal and revalidation system and to enable efficient and accurate communication with regulators, appraisers, designated bodies and the data subject;

c) Patient data such as name address, date of birth, contact details and including special category personal data including medical history, medications, details of tests and investigations, ethnic origin, sexual orientation, marital status, family, biometric data, this information may be collected, held and processed in order to provide medical care to the data subject and where necessary may be shared with other healthcare providers involved in the delivery of care to the patient;

d) Client data including details of directors and employees including details of past employment, GP details, home address, personal and professional references, criminal record checks, past registrations with regulators, this data may be collected, held and processed in order to provide advice on and prepare documentation and investigations by healthcare regulators

22. Data Protection Measures

The Organisation shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) All emails containing personal data must be encrypted;

b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.

c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

g) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail;

h) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Organisation requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer.

i) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Organisation or not, without the authorisation of the Data Protection Officer;

k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

l) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

m) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Organisation or otherwise without the formal written approval of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given.

n) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Organisation where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Organisation that all suitable technical and organisational measures have been taken);

o) All personal data stored electronically should be backed up daily with backups stored onsite and offsite. All backups should be encrypted;

p) All electronic copies of personal data should be stored securely using passwords;

q) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;

r) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Organisation, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

s) No personal data shall be stored for marketing purposes without the express written consent of the data subject.

23. Organisational Measures

The Organisation shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the Organisation shall be made fully aware of both their individual responsibilities and the Organisation's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, agents, sub-contractors, or other parties working on behalf of the Organisation that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Organisation;

c) All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be appropriately trained to do so;

d) All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data shall be

regularly evaluated and reviewed;

g) All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

h) All agents, contractors, or other parties working on behalf of the Organisation handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Organisation arising out of this Policy and the Regulation;

i) Where any agent, contractor or other party working on behalf of the Organisation handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. Transferring Personal Data to a Country Outside the EEA

24.1 The Organisation may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) The transfer is made with the informed consent of the relevant data subject(s);

d) The transfer is necessary for the performance of a contract between the data subject and the Organisation (or for pre-contractual steps taken at the request of the data subject);

e) The transfer is necessary for important public interest reasons;

f) The transfer is necessary for the conduct of legal claims;

g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. Data Breach Notification

25.1 All personal data breaches must be reported immediately to the Organisation's Data Protection Officer.

25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of

confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

25.4 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;
b) The categories and approximate number of personal data records concerned;
c) The name and contact details of the Organisation's Data Protection Officer (or other contact point where more information can be obtained);
d) The likely consequences of the breach;
e) Details of the measures taken, or proposed to be taken, by the Organisation to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. Implementation of Policy

This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Adopted by the Board on …… (Date)

_____

Chairman