BRITISH BEAUTY COUNCIL

British Beauty Council

Data Protection Policy

1. Interpretation

1.1 Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

privacy manager: the data privacy manager with responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.*

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of:

a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or
b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2. Introduction

2 This Data Protection Policy sets out how the British Beauty Council ("we", "our", "us", "the Company") handle the Personal Data of our members, suppliers, employees, workers, business contacts and other third parties.

2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, members or supplier contacts, shareholders, website users, or any other Data Subject.

2 This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. Data protection is the responsibility of everyone within the Company and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action.

2 This Data Protection Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the privacy manager.

3. Scope of Policy and when to seek advice on data protection compliance

3 We recognise that the correct and lawful treatment of Personal Data will maintain trust and 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 £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the UK GDPR.

3 We are all responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.3 The privacy manager is responsible for overseeing this Data Protection Policy. That post is held by Unity Stuart, and they can be reached at 07355 042657 and ea@britishbeautycouncil.com. 3

3.4 Please contact the privacy manager with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the privacy manager in the following circumstances:

(a) if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Company) (see paragraph 5.1);
(b) if you need to rely on Consent or need to capture Explicit Consent (see paragraph 6);
(c) if you need to draft Privacy Notices (see paragraph 7);
(d) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 11);
(e) if you are unsure what security or other measures you need to implement to protect Personal Data (see paragraph 12.1);
(f) if there has been a Personal Data Breach (paragraph 13);
(g) if you are unsure on what basis to transfer Personal Data outside the UK (see paragraph 14);
(h) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 15);
(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 19) or plan to use Personal Data for purposes other than for which it was collected (see paragraph 8);
(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 20);
(k) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 21); or
(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 22).

4. Personal data protection principles

4.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(b) collected only for specified, explicit and legitimate purposes (purpose limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

(d) accurate and where necessary kept up to date (accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

(g) not transferred to another country without appropriate safeguards in place (transfer limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

5. Lawfulness, fairness and transparency

5 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5 The UK GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given their Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations; and

(d) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices; or

5 You must identify and document the legal ground being relied on for each Processing activity.

6. Consent

6 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

6 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6 When processing Special Category Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

6 You will need to evidence Consent captured and keep records of all Consents, so that the Company can demonstrate compliance with Consent requirements.

7. Transparency

7.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. 5

7.2 Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and privacy manager, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

7.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7.4 If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice.

8. Purpose limitation

- Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.
- You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.
- If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the privacy manager for advice on how to do this in compliance with both the law and this Data Protection Policy.

9. Data minimisation

- Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
- You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.
- You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.
- You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

10. Accuracy

- Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
- You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. Storage limitation

- Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
- The Company will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time.
- You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.
- You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.
- You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

12. Security integrity and confidentiality

- Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.
- We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure.
- You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.
- You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

7

(c) Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

12.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

13. Reporting a Personal Data Breach

- The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.
- We have put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.
- If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the privacy manager. You should preserve all evidence relating to the potential Personal Data Breach.

14. Transfer limitation

- The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.
- You must comply with the Company's guidelines on cross-border data transfers.
- You may only transfer Personal Data outside the UK if one of the following conditions applies:
  - (a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;
  - (b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the privacy manager;
  - (c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
  - (d) the transfer is necessary for one of the other reasons set out in the UK GDPR including:
    - (i) the performance of a contract between us and the Data Subject;
    - (ii) reasons of public interest;
    - (iii) to establish, exercise or defend legal claims;
    - (iv) to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
    - (v) in some limited cases, for our legitimate interest.

15. Data Subject's rights and requests

- A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:
  - (a) withdraw Consent to Processing at any time;
  - (b) receive certain information about the Controller's Processing activities;
  - (c) request access to their Personal Data that we hold (including receiving a copy of their Personal Data);
  - (d) prevent our use of their Personal Data for direct marketing purposes;
  - (e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
  - (f) restrict Processing in specific circumstances;
  - (g) object to Processing which has been justified on the basis of our legitimate interests or in the public interest;
  - (h) request a copy of an agreement under which Personal Data is transferred outside of the UK;
  - (i) object to decisions based solely on Automated Processing, including profiling (ADM);
  - (j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
  - (k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
  - (l) make a complaint to the supervisory authority; and
  - (m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format; and
- You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).
- You must immediately forward any Data Subject request you receive to the privacy manager.

16. Accountability

16.1 The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing the privacy manager;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy or Privacy Notices;

(d) regularly training Company Personnel on the UK GDPR, this Data Protection Policy and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. Record keeping

- The UK GDPR requires us to keep full and accurate records of all our data Processing activities.
- You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.
- These records should include, at a minimum:
  - (a) the name and contact details of the Controller and the privacy manager; and
  - (b) clear descriptions of:
    - (i) the Personal Data types;
    - (ii) the Data Subject types;
    - (iii) the Processing activities;
    - (iv) the Processing purposes;
    - (v) the third-party recipients of the Personal Data;
    - (vi) the Personal Data storage locations;
    - (vii) the Personal Data transfers;
    - (viii) the Personal Data's retention period; and
- the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

18. Training and audit

- We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.
- You must undergo all mandatory data privacy-related training and ensure your team undergoes similar mandatory training.
- You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

19. Privacy by Design and Data Protection Impact Assessment (DPIA)

- We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.
- You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

(a) The state of the art. 10

(b) The cost of implementation.

(c) The nature, scope, context and purposes of Processing.

(d) The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.

19.3 The Controller must also conduct a DPIA in respect to high-risk Processing.

19.4 You should conduct a DPIA (and discuss your findings with the privacy manager) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).
(b) Automated Processing including profiling and ADM.
(c) Large-scale Processing of Special Categories of Personal Data.
(d) Large-scale, systematic monitoring of a publicly accessible area.

19.5 A DPIA must include:

(a) A description of the Processing, its purposes and the Controller's legitimate interests if appropriate.
(b) An assessment of the necessity and proportionality of the Processing in relation to its purpose.
(c) An assessment of the risk to individuals.
(d) The risk mitigation measures in place and demonstration of compliance.

20. Automated Processing (including profiling) and Automated Decision-Making

2 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:
(a) a Data Subject has Explicitly Consented;
(b) the Processing is authorised by law; or
(c) the Processing is necessary for the performance of or entering into a contract.

2 If certain types of Special Categories of Personal Data are being processed, then grounds (b) or (c) will not be allowed. However, the Special Categories of Personal Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

2 If a decision is to be based solely on Automated Processing (including profiling), then the Data Subject must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

2 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and the envisaged consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

2 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

21. Direct marketing

21.1 We are subject to certain rules and privacy laws when engaging in direct marketing to our members or prospective members (for example when sending marketing emails or making telephone sales calls). 11

21.2 For example, in a business to consumer context, a Data Subject's prior consent is generally required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing individual members known as "soft opt-in" allows an organisation to send marketing texts or emails without consent if it:

(a) Has obtained contact details in the course of a sale to that person.
(b) Is marketing similar products or services.
(c) Gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.

21.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

21.4 A Data Subject's objection to direct marketing must always be promptly honoured. If a member opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

21.5 You must comply with the Company's guidelines on direct marketing to members and you should consult the privacy manager if you are unsure regarding how to comply with either the Company's guidelines or the law.

22. Sharing Personal Data

2 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

2 You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;
(d) the transfer complies with any applicable cross-border transfer restrictions; and
(e) a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

23. Changes to this Data Protection Policy

We keep this Data Protection Policy under regular review. This version was last updated in October 2023.