BSRAUK Data Protection Policy

Introduction

The Body Stress Release Association (UK) ("BSRAUK") is committed to conducting its business in accordance with all applicable Data Protection laws and regulations including the General Data Protection Regulation ("GDPR"). BSRAUK expects all BSRAUK Members and Third Parties to share this commitment.

As an Association that provides professional representation and membership services to Body Stress Release Practitioners, BSRAUK is registered with the Information Commissioners Office ("ICO"), ICO notification number ZA209622.

BSRAUK's reasons/purposes for processing information is as recorded in the ICO register entry:

We process personal information to enable us to provide our services as an association which includes administering membership records, promoting our services, maintaining our accounts and records, and supporting and managing our voluntary Committee members.

This Data Protection Policy ("Policy") sets out BSRAUK's responsibility and accountability regarding Data Protection; how BSRAUK meets the Principles relating to processing of personal data; and processes associated with the rights of data subjects (individuals).

Any breach of this Policy will be taken seriously and may result in disciplinary action or business sanction. Definitions of terms used within this Policy and related documents are provided in Appendix A.

1. Scope

This Policy applies to all Data Subjects' personal data stored or processed by BSRAUK. Specifically:

- As a Data Controller, this Policy applies to all personal data BSRAUK stores and processes about our members, prospective members, and other third parties.
- Where BSRAUK is deemed a Data Processor due to specific consultancy or advisory services.

2. Objectives

BSRAUK will:

- Adhere to the GDPR Principles for processing personal data, as detailed in this Policy.
- Respect and support individuals' rights concerning their personal data as detailed in GDPR.
- Ensure data protection is built in by design and default to all processes that include personal data.
- Undertake, in addition to the above, a data protection impact assessment for such processes that might have a high risk of a data breach which includes personal data.
- Consider and put in place organisational and technology measures to mitigate risks to personal data.
- Should BSRAUK transfer personal data to a third party located in a country outside of the EEA, consider their compliance with an approved transfer mechanism such as the EU-US Privacy Shield.
- Report data breaches according to the BSRAUK Data Breach Notification Process.
- Handle complaints according to the BSRAUK Complaints Process.
- Monitor and maintain records to support the accountability requirement of GDPR.
- Review and audit this Policy and supporting processes and procedures annually or as required.
- Correct any identified deficiencies in this Policy and the supporting processes and procedures within a defined and reasonable time frame.

3. Responsibility

Everyone who works for or with BSRAUK has responsibility for ensuring that personal data is collected, stored and handled appropriately. The Chair of BSRAUK is ultimately responsible for meeting BSRAUK legal Data Protection Obligations.

To ensure the understanding of responsibilities when handling personal data, BSRAUK will:

- Make all Committee members aware of their responsibilities including security measures.
- Ensure that all existing Committee members are aware of, and will adhere to, this Policy and associated documentation.
- Include GDPR readiness status as part of the selection process of new associates, sub-contractors and other third parties used as Data Processors.

4. Data Protection Principles

There are six data protection principles required by GDPR Article 5 and adhered to by BSRAUK. This section outlines the responsibilities arising from these principles and the BCMA Policy for each.

i. Lawful, Fair, and Transparent Data Processing

The requirement of this principle is that personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals. BSRAUK will maintain a register of all personal data that it stores and processes, the purpose, the lawful bases for doing so, and any personal data that is shared with third parties.

BSRAUK Privacy Notices

This information will be communicated with Data Subjects via BSRAUK Privacy Notices (an example is the one provided on the BSRAUK website) or within terms and conditions or other contracts. In all instances these will be written in concise, understandable language which is appropriate for the audience. The relevant Privacy Notice, or link to Privacy Notice, will be provided at the point of collection of personal data, or as soon as is practicably possible.

ii. Processed for Specified, Explicit and Legitimate Purposes

The requirement of this principle is that personal data is 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. BSRAUK will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned.

BSRAUK Consent Policy

Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, BSRAUK is committed to seeking such consent. Where special categories of data are stored and processed consent will always be required. There are some exceptions to this as detailed in Article 9 of GDPR. If and when BSRAUK wishes to use personal data for any reason apart from what was originally agreed under the first principle (see above), BSRAUK will seek explicit consent for the new reason(s). Consent may be withdrawn by an individual at any time. The mechanism by which this can be done will be detailed in at least the BSRAUK Privacy Notice(s). BSRAUK will record and manage consent given and withdrawn.

iii. Adequate, Relevant and Limited Data Processing

The requirement of this principle is that any personal data which is stored and processed should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. BSRAUK will identify for each Data Subject the purpose of the processing and the minimum personal data it requires for the purpose.

iv. Accuracy of Data and Keeping Data up to Date

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 it is processed) is erased or rectified without delay. BSRAUK will periodically check the accuracy of any personal data it stores and processes. Where reasonable, any rectifications identified, or notified by an individual will be undertaken as soon as is practicable.

v. Timely Processing

The requirement of this principle is that personal data is 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 GDPR in order to safeguard the rights and freedoms of individuals.

BSRAUK will identify the retention period for personal data stored and processed. Personal data will be deleted as soon as is practicable after that time.

vi. Secure Processing

This requirement is that personal data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. BSRAUK will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data.

5. Rights of Individuals

The GDPR provides eight rights for individuals. This section summarises each of these and provides the BSRAUK Process associated with each.

Where BSRAUK is deemed to be a Data Processor, BSRAUK will engage with the Data Controller(s) on how requests from individuals will be fulfilled. When an individual makes a request regarding any of these rights then, before any action is taken concerning the request, BSRAUK will check that:

- The request is reasonable.

- Their identity is confirmed.
- There is no impact on other individuals' personal data and their rights.
- There is no legal, regulatory or contractual requirement to retain the data in its current form.

i. Right to be Informed

Keeping Data Subjects informed. The Right to be Informed encompasses BSRAUK's obligation to provide 'fair processing information', typically through a Privacy Notice. It emphasises the need for transparency about how we use personal data.

BSRAUK Process

The BSRAUK process regarding this Right is covered in the sections BSRAUK Privacy Notices and BCMA Consent Policy earlier in this document.

ii. Right of Access

Individuals have the right to access their personal data and supplementary information. The Right of Access allows individuals to be aware of and verify the lawfulness of the processing. Details of who to contact to exercise this right are provided in BSRAUK Privacy Notice.

BSRAUK Process

The process from receipt of a subject access request through to response is detailed in the BSRAUK Access Request Procedure.

iii. Right to Rectification

The GDPR gives individuals the right to have their personal data rectified. Personal data can be rectified if it is inaccurate or incomplete. Details of who to contact to exercise this right are provided in the BSRAUK Privacy Notice.

BSRAUK Process

After completing the checks detailed at the top of this section, BSRAUK will amend the relevant data as soon as is reasonably possible. An email will be sent to the requesting individual to confirm, and act as a record of, the completion of the request.

iv. Right to Erasure

Erasure of personal data. The Right to Erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is that an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing.

BSRAUK Process

After completing the checks detailed at the top of this section, BSRAUK will delete the relevant data as soon as is reasonably possible. An email will be sent to the requesting individual to confirm, and act as a record of, the completion of the request.

v. Right to Restrict Processing

Restriction of personal data processing. Individuals have a right to 'block' or suppress processing of their personal data. When processing is restricted, BSRAUK is permitted to store the personal data, but not further process it.
BSRAUK can retain just enough information about the individual to ensure that the restriction is respected in future.

BSRAUK Process

After completing the checks detailed at the top of this section, BSRAUK will not process the requesting individual's personal data until notified. An email will be sent to the requesting individual to confirm, and act as a record of this.

vi. Right to Data Portability

The Right to Data Portability allows individuals to obtain and reuse their personal data for their own purposes.
It allows them to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. It enables consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.

BSRAUK Process

BSRAUK holds only basic personal data. As such there is no data that falls under this Right.

vii. Right to Object

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).
- Direct marketing (including profiling).
- Processing for purposes of scientific/historical research and statistics.

Details of who to contact to exercise this right and how to complain are provided in the BSRAUK Privacy Notice.

viii. Rights Related to Automated Decision Making Including Profiling

Companies can only carry out this type of decision-making where the decision is:

- Necessary for the entry into or performance of a contract; or
- Authorised by Union or Member state law applicable to the controller; or
- Based on the individual's explicit consent.

BSRAUK Process

No automated decision making (or profiling) is undertaken by BSRAUK either directly or on behalf of third parties. Should it ever be, then a process will be put in place and this Policy document updated.

Appendix A: Definitions

Requirement	Definition
Personal Data	Any information relating to an identified or identifiable person where that person can be identified, directly or indirectly, by reference to an identifier such as a name or to one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that person.
Special Categories of Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation.
Child	The GDPR defines a child as anyone under the age of 16 years old. This may be lowered to 13 by Member State law as within the UK. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained.
Data Protection Impact Assessments	An assessment undertaken prior to the processing of the impact of the envisaged processing operations, where such processing uses new technology and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of persons, on the protection of personal data.
Data Controller	Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.
Data Processor	Natural or legal person, public authority, agency or body which processes personal data on behalf of the Data Controller.
Third Party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Filing Systems	Any structured set of personal data which are accessible according to the specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, agrees to the processing of personal data relating to him or her.
Data Subject	An identified or identifiable natural (living) person.
Profiling (Automated Processing)	This is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Supervisory Authority	An independent public authority which is established by the UK responsible for monitoring the application of the Regulation. Within the UK this is the Information Commissioner's Office.
Information Notice or Privacy Notice	A notice given to the data subject, in writing or other means including orally and by electronic means, which sets out in a concise, transparent and intelligible and easily accessible way using clear and plain language the following information: • Identity and contact details of the controller. • Purposes of processing and legal basis for processing. • Recipients or categories of recipients of the personal data. • Details of data transfers outside the EU, including how the data will be protected. • The retention period for the data, or if not possible to give, the criteria used to set this. • That the person has the right to access and port data, to rectify, erase and restrict his or her personal data, to object to processing and, if processing is based on consent, to withdraw consent. • That the person can complain to the supervisory authority. • Whether there is a legal or contractual requirement to provide the data and the consequences of not providing the data. • If there will be any automated decision taking including information about the logic involved and the significance and consequences of the processing for the person.
Encryption	The process of encoding personal data in such a way that only authorised parties can access it.
Breach register	A register documenting any personal data breaches, comprising the facts relating to the breach, its effects and the remedial action taken.
Template letters	Letters containing standard wording to be used with additional wording added specific to the information being provided in the letter.
Access Request Timescale	Information must be provided without delay and at the latest within one month of receipt.