PROTECTION OF PERSONAL INFORMATION POLICY

BODY STRESS RELEASE ASSOCIATION OF SOUTH AFRICA (BSRASA)
(hereinafter referred to as the "the Association")

DATE OF COMPILATION: 04/08/2026

DATE OF REVISION: 04/08/2026

Version: 01

TABLE OF CONTENTS **PAGE**

1. PREAMBLE

Chapter 3 of the Protection of Personal Information Act 4 of 2013 (POPIA) provides for the minimum conditions for the lawful processing of personal information by a responsible party. The Body Stress Release Association of South Africa (BSRASA) (hereinafter referred to as the Association) requires personal information relating to natural persons and juristic persons in order to carry out its legal, administrative, commercial, professional membership, and health and wellness sector representation functions. The manner in which such information is processed, stored, used, retained, and disclosed is determined by the Association in accordance with applicable legislation and strict corporate governance obligations. The Association acknowledges its obligations in terms of POPIA, the Promotion of Access to Information Act 2 of 2000 (PAIA), and all other legislation applicable to the lawful processing, confidentiality, retention, and protection of personal information within the voluntary professional membership and healthcare support environment. The Association recognises that member confidentiality, practitioner trust, and statutory compliance remain paramount in all processing activities undertaken by the Association. Accordingly, all processing of personal information by the Association shall be undertaken in a lawful, reasonable, confidential, and secure manner consistent with the rights of data subjects. The Association undertakes to ensure that personal information processed by it is processed lawfully, fairly, and transparently; collected for specific, explicitly defined, and lawful purposes related to promoting stress management, emotional wellbeing, education, workshops, and counselling referrals; adequate, relevant, and not excessive in relation to the purpose for which it is processed; accurate and kept up to date where reasonably practicable; retained only for as long as necessary; and protected by appropriate technical and organisational security safeguards against unauthorised access, loss, damage, destruction, or unlawful disclosure.

2. SCOPE AND APPLICATION

This Policy applies to all committee members, temporary staff, contractors, operators, practitioners, and any other persons acting on behalf of or under the instruction of the Association who process personal information in the course and scope of their duties. This Policy applies to all personal information processed by the Association in both physical and electronic form, including information relating to members, suppliers, corporate vendors, community project participants, and any other third parties whose information may be processed by the Association. Compliance with this Policy is mandatory and forms part of the governance, ethical, and compliance obligations of all persons associated with the Association.

3. DEFINITIONS

For purposes of this Policy, unless the context indicates otherwise, the following terms shall bear the meanings assigned to them under POPIA:

"**Association**" means the Body Stress Release Association of South Africa (BSRASA).

"**Data Subject**" means the person to whom personal information relates.

"**Information Officer**" means the head of the private body or any duly authorised person designated in terms of POPIA and PAIA.

"**Operator**" means a person or entity which processes personal information for the Association in terms of a contract or mandate without coming under the direct authority of the Association.

"**Personal Information**" means information relating to an identifiable, living natural person and, where applicable, an identifiable existing juristic person.

"**Processing**" means any operation or activity concerning personal information, including collection, receipt, recording, organisation, storage, updating, retrieval, dissemination, use, distribution, destruction, or deletion.

"**Record**" means any recorded information regardless of form or medium.

"**Responsible Party**" means the public or private body or any other person which determines the purpose of and means for processing personal information. For purposes of this Policy, the Association is the Responsible Party.

"**Security Compromise**" means any unauthorised access to, acquisition of, disclosure of, loss of, or damage to personal information.

"**Special Personal Information**" means personal information relating to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, criminal behaviour, or information concerning children.

4. INFORMATION OFFICER DETAILS

The Association's nominated individual act as the Information Officer in accordance with POPIA and PAIA and is responsible for overseeing the implementation, monitoring, and enforcement of this Policy and all applicable data protection obligations.

The Information Officer's details are as follows:

CONTACT DETAILS	
Name of Association	Body Stress Release Association of South Africa (BSRASA)
Designated contact person	Ingeborg Muhsfeldt (Information Officer)
Physical address	4 Forest Road, George, 6530
Contact number	083 660 0780
Email address	chairperson.sa@bodystressrelease.com

5. DATA SUBJECT RIGHTS

Data subjects have the right to be notified that their personal information is being collected by the Association and, where required by law, to be notified in the event of a security compromise affecting their personal information. Data subjects have the right to establish whether the Association holds personal information relating to them and to request access to such information in accordance with applicable legislation and the Association's PAIA Manual. Data subjects may request the correction, deletion, destruction, or updating of personal information that is inaccurate, irrelevant, excessive, incomplete, misleading, out of date, or unlawfully obtained. Data subjects may object to the processing of their personal information on reasonable grounds relating to their particular situation, subject to any statutory obligations, legitimate interests, legal proceedings, or regulatory record-keeping rules applicable to the Association. Data subjects have the right to object to the processing of personal information for purposes of direct marketing by means of unsolicited electronic communications. Data subjects may lodge complaints with the Information Regulator in relation to any alleged infringement of their rights under POPIA. The exercise of certain rights by data subjects may be limited where records are protected by professional confidentiality, non-disclosure agreements, ongoing legal proceedings, statutory obligations, or any lawful grounds for refusal recognised under applicable legislation.

6. LAWFUL BASIS FOR PROCESSING

The Association processes personal information only where permitted under POPIA. This includes processing that is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party, such as membership agreements. Processing is also conducted where it complies with an obligation imposed by law on the Association or protects a legitimate interest of the data subject. Furthermore, processing is permitted when necessary for pursuing the legitimate interests of the Association or of a third party to whom the information is supplied. This includes verifying professional credentials, maintaining the public practitioner directory, managing educational quality, and protecting the integrity of the Body Stress Release profession. Where required by law or where no other lawful basis exists, the Association will obtain the explicit and informed consent of the data subject prior to processing their personal information.

7. PURPOSE OF PROCESSING PERSONAL INFORMATION

The Association processes personal information for purposes related to advancing the Body Stress Release profession within the health and wellness sector, including managing professional memberships. The Association also processes personal information for operational management, which includes managing community support, public awareness programmes, educational workshops, counselling referrals, and related health and wellness activities. Furthermore, the Association processes personal information for administrative and security functions, procurement, vendor vetting, accounting, taxation, recruitment, payroll administration, internal administration, website support, information technology security, fraud prevention, risk management, and the exercise or protection of legal rights. The Association undertakes not to process personal information for any purpose that is incompatible with the original purpose for which the information was collected, unless such processing is permitted by law.

8. CATEGORIES OF DATA SUBJECTS AND PERSONAL INFORMATION

The Association may process personal information relating to various categories of data subjects, including registered Body Stress Release practitioners, prospective practitioners, student practitioners, voluntary members, educational instructors, committee members, vendors, creditors, debtors, website users, community project participants, and any other third parties whose information is processed in the ordinary course of business. The personal information processed by the Association includes identifiers such as names, identity numbers, passport numbers, and professional registration numbers. It also includes contact information such as physical addresses, postal addresses, telephone numbers, and email addresses. Financial records processed include banking details, membership fee statements, tax invoices, and financial administration records. Professional details processed include employment history, training records, practitioner qualifications, continuing professional development logs, and disciplinary tracking records. Digital data and other categories processed include electronic communications, website cookies, and any other information necessary for lawful wellness association operations.

9. PROCESSING OF SPECIAL PERSONAL INFORMATION

The Association may process special personal information where such processing is permitted under POPIA and necessary for lawful purposes, such as when the data subject has consented, or when it is required for the establishment, exercise, or defence of a legal right. Due to the educational, regulatory, and public-facing nature of the health and wellness environment, the Association may process special personal information relating to health logs or physical metrics managed during training modules or wellness workshops. It may also process biometric data for automated access controls to electronic testing platforms or physical administration centres. Furthermore, the Association may process information concerning criminal behaviour or legal infractions for mandatory practitioner vetting and public safety screening, as well as demographic data such as race or ethnic origin explicitly collected for statutory transformation, national skills development, or industry reporting. The Association implements strict technical safeguards and confidentiality measures in relation to all special personal information processed by it.

10. SHARING PERSONAL INFORMATION

The Association may share personal information with third parties where such disclosure is necessary for lawful business, educational, regulatory, operational, or legal purposes. Information may be shared with the public via the public-facing online directory to allow clients to verify registered, active Body Stress Release practitioners. It may also be shared with service providers such as external educational institutions, independent examiners, auditors, accounting firms, and underwriters. For technology and logistical infrastructure, data may be shared with information technology providers, secure cloud storage companies, and logistics or courier services. Finally, information may be disclosed to law enforcement bodies, legal counsel, or statutory regulators where disclosure is necessary for compliance or the protection of professional interests. The Association will take reasonable steps to ensure that recipients of personal information implement appropriate technical and organisational safeguards to protect such information and maintain confidentiality.

11. OPERATORS AND THIRD-PARTY SERVICE PROVIDERS

Where the Association appoints operators or third-party service providers to process personal information on its behalf, it will ensure that appropriate written agreements are concluded with such parties in accordance with POPIA. Operators and service providers processing personal information on behalf of the Association shall be required to process such information only in accordance with the Association's explicit instructions. They must also maintain stringent security safeguards, enforce absolute data confidentiality, and comply with all applicable legal requirements relating to the protection of personal information. The Association will conduct reasonable due diligence and operational audits in relation to operators and service providers to ensure compliance with applicable security, data privacy, and professional standards.

12. CROSS-BORDER FLOW OF PERSONAL INFORMATION

The Association may transfer personal information to recipients located outside the Republic of South Africa where such transfer is necessary for international professional profiling, global wellness affiliation, operational, legal, technological, or training purposes. Cross-border transfers may occur through the use of cloud storage platforms, membership management systems, electronic communication platforms, international banking networks, or engagements with foreign Body Stress Release affiliate bodies. The Association will take reasonable steps to ensure that any cross-border transfer of personal information complies with Section 72 of POPIA and that the foreign recipient is subject to laws, agreements, binding corporate rules, or other safeguards providing an adequate level of protection substantially similar to that provided under POPIA.

13. DESCRIPTION OF SECURITY MEASURES

The Association implements stringent technical and organisational measures to protect the confidentiality, integrity, and availability of personal information in its possession or under its control. Physical membership records and high-security data documents are stored in access-controlled facilities protected by locks, filing cabinets, and monitored administrative offices. Electronic records, practitioner databases, and educational tracking networks are protected through multi-factor authentication, enterprise password controls, advanced encryption technologies, firewalls, anti-malware systems, network segregation, secure off-site cloud backups, and endpoint protection. The Association implements audit logging, secure electronic disposal procedures, email security protocols, role-based access controls, and active cybersecurity monitoring to reduce foreseeable internal and external security risks. The Information Officer conducts periodic risk assessments, security reviews, and compliance evaluations to identify and address potential vulnerabilities.

14. ACCESS CONTROL AND REMOTE WORKING

The Association implements strict role-based access controls to ensure that access to personal information, membership rosters, and training records is limited to authorised persons who require such access for legitimate administrative, educational, or operational purposes. Committee members, and authorised users accessing Association networks remotely are required to use association-approved, secure digital devices, connect via secure Virtual Private Networks, comply with multi-factor authentication requirements, and maintain absolute confidentiality regarding visible records. The use of personal devices, public unencrypted networks, removable storage devices such as USB

flash drives, or unauthorised software for processing personal information is strictly restricted or prohibited to protect the security and integrity of Association information.

15. RETENTION AND DESTRUCTION OF RECORDS

The Association retains personal information only for as long as reasonably necessary to fulfil the purpose for which the information was collected and processed, unless a longer retention period is required or permitted by law. The Association retains records for statutory and operational periods, which includes professional registration records tracking historical practitioner certification and membership status. It also retains financial records for a minimum of seven years for accounting vouchers, membership invoices, and taxation data. Educational documentations are retained to satisfy obligations, student academic histories, and grading manifests, while legal records are kept for active or anticipated disciplinary proceedings or ongoing legal claims. Where personal information is no longer required, the Association will take reasonable steps to securely destroy, shred, incinerate, delete, or permanently de-identify such information in a manner that prevents unauthorised access, recovery, or reconstruction.

16. SECURITY COMPROMISES AND INCIDENT REPORTING

Any actual or suspected unauthorised access to, disclosure of, loss of, theft of, or damage to personal information must immediately be reported to the Information Officer. The Association will investigate all reported incidents, activate its data breach response protocol, and take reasonable steps to contain, assess, and mitigate the effects of any security compromise. Where required by law, the Association will notify the Information Regulator and affected data subjects of any security compromise in accordance with Section 22 of POPIA. The Association maintains an incident register detailing all security incidents, forensic investigations, remedial measures, and regulatory notifications for governance and auditing purposes.

17. COMMITTEE RESPONSIBILITIES

All Committee members, training instructors, and onsite contractors of the Association owe a strict duty of care to protect all personal information processed during the course of their duties. The Committee may only access, retrieve, or process personal information, including member files, student records, financial logs, that is directly relevant and strictly required to perform their specific workplace tasks. The Committee must ensure that all data captured during member onboarding or registration logging is accurate, complete, and kept up to date. Committee members operating within administrative offices or training facilities must maintain a strict clean-desk environment, ensuring that physical records like training scores or shipment manifests are never left unattended and are securely locked away when not in use. Digital workstations must be kept secure at all times through mandatory multi-factor authentication, and sharing system passwords or user credentials is explicitly forbidden. The Committee members are strictly prohibited from downloading, copying, or exporting any data or personal information onto personal electronic devices, unapproved public networks, or unauthorised removable storage media. It is a mandatory requirement for all members to immediately report any actual, suspected, or accidental data breach, lost corporate device, or cybersecurity incident directly to the Information Officer without delay. Any non-compliance with these data protection directives will be treated as a severe breach of organisational policy, exposing the committee member to internal disciplinary proceedings up to and including summary dismissal or

removal from the association's governance boards, as well as potential civil or criminal prosecution under POPIA.

18. TRAINING AND COMPLIANCE MONITORING

The Association will conduct continuous internal awareness campaigns and data protection training sessions to ensure that all committee members remain fully informed of their legal responsibilities under POPIA, PAIA, and this Policy. The Information Officer shall actively monitor compliance across all operational sectors, which includes carrying out periodic, unannounced audits of physical record-keeping facilities, digital system access records, and employee processing practices. Any systematic operational gaps or compliance vulnerabilities identified during these monitoring processes will be swiftly addressed with targeted operational amendments, software updates, or supplementary training as deemed necessary by management.

19. OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

Data subjects have a statutory right to object to the processing of their personal information on reasonable grounds relating to their specific situation, provided such processing is carried out based on the legitimate interests of the Association or a third party, or for direct marketing purposes. Any data subject who wishes to object to the processing of their personal information must submit their formal request in writing to the Information Officer using the prescribed regulatory form established under POPIA (Form 1). Upon receiving a valid objection, the Association will immediately cease processing the affected personal information, unless the Association is legally obligated to continue processing by law, statutory record-keeping regulations, or to establish, exercise, or defend an active legal claim.

20. REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION

Data subjects may formally request the Association to correct, update, delete, or destroy any personal information in its possession or under its control that is inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or obtained unlawfully. Requests for the correction or deletion of personal information must be submitted in writing to the Information Officer using the prescribed regulatory form established under POPIA (Form 2). The Association will take all reasonable and legally required steps to verify the accuracy of the information and execute the requested change without delay, except where the Association is restricted from deleting such data due to overarching statutory retention periods or active regulatory investigation timelines.

21. GOVERNANCE AND REVIEW

This Policy is subject to formal approval by the Executive Committee of the Association and shall be formally reviewed at least annually, or more frequently as necessitated by amendments to South African privacy laws, technological advancements, or critical changes to the Association's operational infrastructure. The version of this Policy published on the Association's official corporate portal or displayed at administrative facilities shall be deemed to be the version currently in force. The Information Officer holds ultimate organisational responsibility for ensuring that all business practices, vendor agreements, and operational standard operating procedures align seamlessly with this Policy.

Issued by

Ingeborg Muhsfeldt
Information Officer