BSRA Data protection policy

Context and Overview

Key Details

- Policy prepared by: Professor Lorna Harries (BSRA secretary)
- Approved by BSRA trustees on
- To be reviewed annually

Introduction

The BSRA needs to collect information on past and previous members, as well as on grantholders, grant applicants, trustees and members of the lay and scientific advisory panels

This policy describes how data are collected, stored and accessed to meet the BSRA's data protection standards and UK law.

This data protection policy ensures the BSRA

- Complies with Data protection laws
- Protects the rights of individuals
- Is open and transparent about the data it collects and stores
- Protects itself from the risks of a data breach.

Data protection law

The data protection act describes how organisations must collect, handle and store personal information about its members and people connected with it.

These rules apply regardless of whether the data are electronic, paper or in any other format.

To comply with the law, the BSRA will ensure that data collected from individuals is collected and used fairly, stored safely and not disclosed unlawfully.

Data protection law states that personal data must be

- Processed lawfully and fairly
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and up to date
- Held for only as long as necessary
- Processed in accordance with the rights of individuals
- Protected in appropriate ways
- Not be transferred to any other party without consent

People, risks and responsibilities

This policy applies to

- The trustees/executive committee members of the BSRA
- The lay advisory board of the BSRA
- The scientific advisory board of the BSRA
- The membership of the BSRA

It applies to all data held by the BSRA on individuals, even if said data lies outside the requirements of the data protection act. This may include

- Names of individuals
- Postal addresses of individuals
- Email addresses of individuals
- Telephone numbers of individuals
- Other data on individuals (e.g. grant applications and associated data)

Data Protection risks

- **Breaches of confidentiality** – e.g. information being given out inappropriately
- **Failing to offer choice** – e.g. individuals not being given a choice over whether data are collected and stored on them
- **Reputational damage** – e.g. should data be accessed illegally by outside parties.

Responsibilities

Everyone involved with the BSRA has some responsibility for ensuring data are collected, handled and stored safely.

These people or groups have key areas of responsibility

- The **trustees** of the BSRA will be legally responsible for ensuring that the BSRA operates within data protection law.
- The **Scientific Advisory Board** are responsible for ensuring that data on grant applications and applicants are stored appropriately
- The **Lay Advisory Board** are responsible for ensuring that data on grant applications and applicants are stored appropriately

The BSRA Member Secretary and deputy secretary are responsible for:

- Keeping the trustees, the lay advisory board and the scientific advisory board up to data of the requirements of the data protection act.
- Reviewing all data protection policies and documents annually
- Handling data protection questions from people connected with the BSRA
- Dealing with requests from individuals to see their personal data

- Where necessary, working with other staff to ensure they understand and conform to data protection law as it applies to the BSRA

The communications officer is responsible for

- Ensuring all systems used to collect or store data conform to acceptable security standards
- Performing regular checks to ensure security systems are performing as needed
- Evaluating any third party solutions for data storage (e.g. The Cloud, Dropbox) to ensure they meet the necessary standard.
- Approving any data protection statements attached to emails or newsletters
- Dealing with questions from journalists regarding the BSRA's data protection policy

General BSRA data protection guidelines

- The only people who have access to data should be those who need it to fulfil their roles
- Data should not be shared informally. People requiring access to data should formally request it from the membership secretary.
- The BSRA will provide guidance on data protection to all people who may need to access data
- People with access to data should take care to maintain the security of those data by following good security procedures.
- Where appropriate, strong passwords must be used and these must not be publicised.
- Personal data should not be disclosed to unauthorised people, whether within or without the BSRA
- Data should be regularly reviewed and updated. If no longer necessary, it should be destroyed.
- Individuals should request help if they are unsure of data protection requirements.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Secretary or the Deputy Secretary.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Individuals should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between individuals.

- If data is stored on removable media (like external hard drives), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to [company name] unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, individuals should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data should never be transferred outside of the trustees of the BSRA
- Individuals should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires the BSRA to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the BSRA should put into ensuring its accuracy.

It is the responsibility of all individuals who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Individuals should take every opportunity to ensure data is updated.
- The BSRA will make it easy for data subjects to update the information that the BSRA holds about them
- Data should be updated as inaccuracies are discovered. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by the BSRA are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the BSRA is meeting its data protection obligations.

If an individual contacts the BSRA requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the secretary at secretary@bsra.org.uk.

The BSRA will aim to provide the relevant data within 14 days.

The BSRA will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the BSRA will disclose requested data. However, the BSRA will ensure the request is legitimate, seeking assistance from the board and taking legal advice where necessary.

Providing information

The BSRA aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights