National Sea Rescue Institute of South Africa "NPC"

Registration No 1967/013618/08

"the Institute"

Data Protection Policy

Approved: 2017
Reviewed: July 2018

NSRI Data protection policy

Context and overview

Key details

- Policy prepared by: Ben McCune

Introduction

National Sea Rescue Institute needs to gather and use certain information about donors and volunteers.

These can include donors, suppliers, volunteers, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures NSRI:

- Complies with data protection law and follow good practice
- Protects the rights of staff, donors and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Protection of Personal Information Act (the POPI Act) describes how organisations — including NSRI— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The POPI Act is underpinned by eight important principles. These say that personal data must follow the principles outlined below:

- The processing of information is limited which means that personal information must be obtained in a lawful and fair manner.
- The information can only be used for the specified purpose it was originally obtained for.

- The Act limits the further processing of personal information. If the processing takes place for purposes beyond the original scope that was agreed to by the data subject, the processing is prohibited.
- The person who processes the information must ensure the quality of the information by taking reasonable steps to ensure that the information is complete, not misleading, up to date and accurate.
- The person processing the personal information should have a degree of openness. The data subject and the Information Regulator must be notified that data is being processed.
- The person processing data must ensure that the proper security safeguards and measures to safeguard against loss, damage, destruction and unauthorised or unlawful access or processing of the information, has been put in place.
- The data subject must be able to participate. The data subject must be able to access the personal information that a responsible party has on them and must be able to correct the information.
- The person processing the data is accountable to ensure that the measures that give effect to these principles are complied with when processing personal information.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of National Sea Rescue Institute of South Africa (NSRI)
- All stations of NSRI
- All staff and volunteers of NSRI
- All contractors, suppliers and other people working on behalf of NSRI

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any information relating to individuals

Data protection risks

This policy helps to protect NSRI from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.

- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with NSRI has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that NSRI meets its legal obligations.
- The **Information Officer** is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data NSRI holds about them (also called ‘subject access requests’).
    - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
- The **IT Manager** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- The **Marketing Manager** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **NSRI will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

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

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

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**.
- Employees 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 employees.
- If data is **stored on removable media** (like a CD or DVD), 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.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- 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 NSRI 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, employees 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.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the Republic.**
- Employees **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 NSRI 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 NSRI should put into ensuring its accuracy.

It is the responsibility of all employees 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.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests

All donors who are the subject of personal data held by NSRI 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 company is **meeting its data protection obligations**.

If a donor contacts the NSRI requesting this information, this is called a subject access request.

Subject access requests from donors should be made by email, addressed to the data controller at it@searescue.org.za The data controller can supply a standard request form.

The data controller 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, NSRI will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

NSRI aims to ensure that donors are aware that their data is being processed, and that they understand:

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

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.