Last updated 7 July 2021

**DATA PROTECTION POLICY**

1. **Introduction**

When BEN is entrusted with personal data in order to deliver our services it is our responsibility to ensure that all reasonable steps are taken to protect this data in terms of the Protection of Personal Information Act 4 of 2013 (POPIA). These guidelines are key to sharing data responsibly and to effectively navigate the changing risk environment associated with advancements in data and technology.

BEN regularly receives records from individuals which are of a personal nature. When we use this information to perform our duties we need to safeguard this information even if we just forward it to another colleague. We need to ensure that we handle the information in a responsible manner and that it relates to the function we perform as BEN.

This guideline is designed to bring awareness of the requirement of POPIA. We need to be conscious of what we are allowed to do with personal information and what not.

1. **Scope**

The purpose of this guideline is to outline how BEN employees will use personal data and what measures need to be taken to ensure safe and lawful collection and processing of data.

1. **Commencement date of the POPI Act**

The act will become fully effective as from 1 July 2021.

1. **Information officer**

The act requires BEN to register an Information officer which is the CEO of BEN.

The role of the Information officer is to encourage compliance with the provisions of the Act.

A deputy Information officer can be appointed which is the Financial Officer.

1. **Security**

BEN has established security measures to protect the integrity and confidentiality of personal information by taking appropriate, reasonable, technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information.

Each employee is responsible for the security of his/her own computer and/or mobile device.

Employees should log off when leaving their computer unattended to prevent unauthorised access.

Passwords should be used for all electronic devices and these passwords should be stored in a secure manner and changed regularly. The same password should not be used on various sites.

The rooter password should be strong and secure.

Incoming data should always be checked for viruses and extreme care should be taken when downloading external content as these may contain viruses.

When travelling need to make sure that the device is securely locked in the boot of the car and not left on the passenger seat.

1. **What is personal information?**

Personal information means information relating to an identifiable, living, natural person, and where it is applicable and identifiable, existing juristic person including, but not limited to;

* Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience belief, culture, language and birth of the person.
* Information relating to the education or the medical, financial, criminal or employment history of the person;
* Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
* the biometric information of the person (i.e. finger prints, DNA, face recognition, blood type etc.)
* the personal opinions, views or preferences of the person;
* correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
* the views or opinions of another individual about the person; and
* the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
1. **Processing of Personal Information**

Personal information may only be processed for specific, explicitly defined and legitimate reasons. It cannot be general consent. It must deal with what, why, how and where in each instance and whether the information will be shared with a third party.

Personal information must be collected directly from the data subject (the person you collect the data from).

If the personal information has been gathered from a third party, the data subject must have given his/her consent that the data can be shared.

Only information that is required for the specific purpose of which it is gathered may be stored. You may collect more information than is required for the intended purpose for future use if you obtain the necessary consent form the data subject.

Section 69 of the Act outlaws direct marketing by means of any form of electronic communication unless the data subject has given consent. Such an electronic communication includes e-mails, SMSs and automatic calling machines. A data subject can only be approached once to obtain such consent. Once such consent is refused, it’s refused forever.

Slightly different rules apply if the subject is a customer. Here the customer’s contact details should have been obtained in the context of the sale of a product or a service, the direct marketing by electronic communication can only relate to BEN’s own service or product and the data subject must have been given the right to opt out at the time that the information was collected and each time such communication is sent.

1. **Transfer and disclosure of personal data**

BEN may also provide personal data to third parties such as partners, contractors and suppliers that provide a service to BEN or to track the impact of our work.

BEN reserves the right to disclose an individual’s personal data to law enforcement agencies, regulatory bodies, government agencies and other third parties as required by law.

1. **Processing personal information of children (under 18 years)**

As a general rule, processing of personal information of a child is prohibited by POPIA unless the data processing is carried out with the prior consent of the competent person. A competent person is a person who is *legally* competent to consent to any action of decision being taken in respect of any matter concerning a child, i.e. a parent.

1. **Transfer of personal information outside the borders of South Africa**

BEN may send personal information of a data subject to a third party in another country if the data subject has given prior consent to the transfer, i.e. sending photos and/ or stories of bicycle beneficiaries to a donor.

1. **Retention period**

Once the data has been collected and processed, the personal information will not be retained for longer than is necessary for achieving the purpose for which it was collected or processed or legally required. The data will be destroyed or deleted in a responsible manner.*.*

1. **Social Media**

Social media includes Facebook, Linkedin, Twitter, Instagram, Tumblr, TikTok, other social network sites, internet postings and blogs.

This section refers to the use of social media for business purposes as well as personal use that may affect Bicycling Empowerment Network. Social media must not be used to post anything regarding an individual’s personal data, or sensitive work-related topics unless prior consent has been obtained.

1. **Website**

The privacy policy will be available on BEN’s website.

1. **Newsletter, Annual Report and other communication relating to BEN ‘s work**

BEN’s newsletter, the annual report and other communication relating to BEN’s work can only be send to people that have given prior consent to being send this. An opt-in option will be made available on the website.

1. **WhatsApp Groups**

The administrator of a BEN related WhatsApp group should notify the group that each participant can refuse consent of being part of a WhatsApp group by leaving the group. Should a person elect to remain in the group then it will be accepted that the person has consented to being part of the group and that this person’s personal information (cell phone number and name) is noticeable to any other person in that group. Should a person want to make use of another person’s personal information in the group then prior consent needs to be obtained.

1. **Security breaches**

In case of a security breach you must report this immediately to the CEO of BEN who is also the Information Officer.

Provide as much information as possible about the security breach, i.e. What type of data was involved, when and how did the security breach happen, how many individuals personal data are likely to be affected by the breach.

Some examples of security breaches:

Theft or loss of data or equipment (laptops, mobile phones memory sticks) on which data is stored, unauthorised access, use of uncontrolled or unauthorised media, hackings

1. **Personal data accuracy**

BEN should ensure that the personal data of a data subject is accurate and any inaccuracies should be corrected across all the systems.

1. **Personal data access**

Data subjects are entitled to ask BEN for a copy of their personal data to correct, erase or restrict its processing. Data subjects may also withdraw consent previously given. Where BEN requires personal data to comply with legal or contractual obligations, then provision of such data is mandatory.

1. **Data protection and disciplinary action**

Any misuse of personal information should be reported to the CEO and if any individual contravenes this policy then disciplinary action may be taken.

1. **Review of this policy**

This policy is reviewed by the Information Officer on a regular basis.

1. **Areas where the act has and impact on BEN and need to be addressed are**

 Staff (permanent, temporary, volunteers and interns)

Each staff member needs to give permission that his/her information can be used and that this information can be shared with third parties, both inside and outside of South Africa.

Each employment contract will now also include a clause regarding the employee’s obligation to acknowledge and protect the integrity of personal information of the organisation and data privacy and report any breaches in security.

Existing contracts without the personal information protection clauses will be updated with an additional Protection of Personal Information agreement and need to be signed by the employee and annexed to the existing contract.

* 1. BEN collects and processes employee personal information to**;**
* process salaries and salary related statutory returns;
* confirm information on resumes, curriculum vitae and covering letters;
* provide reference letters
* provide training, performance evaluation and disciplinary records
* manage employee
* include in fundraising proposals
* use on our website, in the media, for videos and to share on social media and other electronic platforms to promote the work of BEN

**21.2** BEN collects and processes Director’s personal information to;

* to perform Company Secretarial duties in house and by the Auditors
* include in fundraising proposals
* advertise
* process statutory returns
* use on our website, in the media, for videos and to share on social media and other electronic platforms to promote the work of BEN

**21.3** BEN collects and processes Partner personal information to;

* include in fundraising proposals
* advertise
* use on our website, in the media, for videos and to share on social media and other electronic platforms to promote the work of BEN

**21.4** BEN collects and processes Donor personal information to;

* include in fundraising proposals
* advertise
* use on our website, in the media, for videos and to share on social media and other electronic platforms to promote the work of BEN

 **21.5** BEN collects and processes Beneficiary or Customer personal information to;

* conclude a sale, donation or service from the customer or beneficiary
* include in fundraising proposals
* track the impact of our work
* advertise
* use on our website, in the media, for videos and to share on social media and other electronic platforms to promote the work of BEN.

When BEN distributes bicycles or provides services then prior consent should be obtained from the recipients for the use of their private information. This can be part of a Memorandum of Understanding.

1. **BEN holds the following personal information:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of Personal Information** | **Permanent Employees** | **Temporary****Employees** | **Interns and****Volunteers** | **Directors** |
| Names | X | X | X | X |
| Address | X | X | X | X |
| Telephone numbers | X | X | X | X |
| ID number | X | X | X | X |
| Date of birth | X | X | X | X |
| Race | X | X | X | X |
| Sex | X | X | X | X |
| Age | X | X | X | X |
| Marital Status | X |  |  |  |
| Pregnancy | X |  |  |  |
| Banking and salary details | X | X | X |  |
| Mental or Physical health | X |  |  |  |
| Education | X |  |  |  |
| Employment history | X |  |  |  |
| Training, performance and disciplinary information | X |  |  |  |
| Images/Videos | X | X | X | X |
| Information about criminal offences or convictions | X |  |  |  |

Continued:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of Personal Information** | **Customers**  | **Partners** | **Donors** | **Beneficiaries (not covered by MOU) & Trainees** |
| Names | X | X | X | X |
| Address | X | X | X | X |
| Telephone numbers | X | X | X | X |
| ID number |  | X |  | X |
| Date of birth |  | X |  | X |
| Race |  | X |  | X |
| Gender |  | X |  | X |
| Age |  |  |  | X |
| Marital Status |  |  |  |  |
| Pregnancy |  |  |  |  |
| Banking and salary details |  | X |  |  |
| Mental or Physical health |  |  |  |  |
| Education |  | X |  |  |
| Employment history |  | X |  |  |
| Training, performance and disciplinary information |  |  |  |  |
| Images/Videos | X | X | X | X |
| Information about criminal offences or convictions |  | X |  |  |