DATA PROTECTION POLICY
OF
BESPOKE EXECUTOR SERVICES (PTY) LTD

CONTEXT AND OVERVIEW

Key details

- Approved by Board / Management on: 31 January 2018
- Policy became operational on: 1 February 2018
- Next review date: 1 January 2019 or should legislation change before then
- "Team" – The word "Team" will refer to BEXs Directors, Staff, Contractors, Consultants and Volunteers.

Introduction

Bespoke Executor Services (BEXs) needs to gather and use certain information from individuals to provide the services offered. Individuals are defined as and not limited to customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how the personal data must be collected, handled and stored to meet data protection standards.

Why the policy exists

This data protection policy ensures that BEXs:

- Complies with the Protection of Personal Information Act, No 4 of 2013 (POPI) and follows good practice;
- Protects the rights of staff, customers and partners;
- Is open about how it stores and processes individuals' data;
- Has measures/steps in place to guard against data breach.

Protection of Personal Information

Protection of Personal Information (POPI) Act, No 4 of 2013 describes how organisations — including BEXs must collect, handle and store personal information.

POPI was formally introduced in February 2017 and the commencement date is awaited.

These rules apply regardless of whether data is stored electronically or by any other means.

The POPI Act aims to bestow upon the data subject, as the owner of personal information, rights of protection and the ability to exercise control over:

- When and how the data subject chooses to share their information (requires their consent);
- The type and extent of information the data subject chooses to share (must be collected for valid reasons);
- Transparency and accountability on how "the data subject" data will be used (limited to the purpose) and notification if/when the data is compromised;
- Providing the data subject with access to their own information as well as the right to have their data removed and/or destroyed should they so wish;
- Who has access to the information of the data subject, i.e. there must be adequate measures and controls in place to track access and prevent unauthorised people, even within the same company, from accessing your information;
- How and where the information of the data subject is stored (there must be adequate measures and controls in place to safeguard their information to protect it from theft, or being compromised);
- The integrity and continued accuracy of the information of the data subject (i.e. the information must be captured correctly and once collected, the institution is responsible to maintain it).

Examples of "personal information" for an individual could include:

- Identity and/or passport number;
- Date of birth and age;
- Phone number/s (including mobile phone number);
- Email address;
- Online/Instant messaging identifiers;
- Physical address;
- Gender, Race and Ethnic origin;
- Photos, voice recordings, video footage (also CCTV), biometric data;
- Marital/Relationship status and Family relations;
- Criminal record;
- Private correspondence;
- Religious or philosophical beliefs including personal and political opinions;
- Employment history and salary information;
- Financial information;
- Education information;
- Physical and mental health information;
- Membership to organisations/unions.

BEXs implemented the following to ensure POPI compliance:

- Set processes with regards to the collection, recording, storing and destroying of personal information.
- Clients are fully informed of the reason for the collection of the information being requested. Our documents and communication state the purposes for the information collected.

PEOPLE, RISKS AND RESPONSIBILITIES

Policy scope

It applies to all data that BEXs holds relating to identifiable individuals, even if that information technically falls outside of the POPI Act.

Data protection risks

This policy helps to protect BEXs from 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

The team and those associated with BEXs have a responsibility for ensuring data is collected, stored and handled appropriately.

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

The **Board of Directors** is ultimately responsible for ensuring that BEXs meets its legal obligations.

- The **Board of Directors** 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 for access to personal information stored by BEXs (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

- ❖ Performing quarterly checks and scans to ensure security hardware and software is functioning properly and that “backups” are in place and updated.
- ❖ Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
- ❖ 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 must be those who need it for their work.
- ➢ Data must not be shared informally. The Team must have signed a confidentially agreement.
- ➢ BEXs will provide training to all employees to help them understand their responsibilities when handling data.
- ➢ Employees must keep all data secure, by taking sensible precautions and following the guidelines in this section / policy.
- ➢ Strong passwords must be used, and they must never be shared. See Password policy below.
- ➢ Personal data must not be disclosed to unauthorised people, either within the company or externally.
- ➢ Data must be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be destroyed by either being shredded or incinerated.
- ➢ Consultants must request help from their BEXs IT manager if they are unsure about any aspect of data protection.

DATA COLLECTION AND STORAGE

These rules describe how data is collected and where data must be safely stored. Questions about storing data safely can be directed to the IT manager.

Collection of data

Whilst POPI regulates how organisations must collect, handle and store personal information, organisations must also comply with “Know-your-customer” obligations in terms of the Financial Intelligence Centre Act 38 of 2001.

BEXs operates as follows:

- For the drafting of Wills.

  The Estate Planning Questionnaire is used to gather the information required to ensure that the will being drafted is suitable given the information being provided by the client. In order to ensure accuracy in the drafting of this document, certain personal information is called for – the client is at all times fully aware of the reasons for and the need to provide such information.

- For the administration of estates

  During the administration of the estate there will be a need to collect personal information from the heirs; at all time the heirs are fully aware of the need for the collection of this information.

- For the administration of Trusts

  During the administration of a trust there will be a need to collect personal information from the trust beneficiaries; at all time beneficiaries are fully aware of the need for the collection of this information.

.

- Drafting of Trust Deeds

  The application form is used to gather the information required to ensure that the Trust Deed drafted is suitable given the information being provided by the client. In order to ensure accuracy in the drafting of this document, certain personal information is call for – the client is at all times fully aware of the reasons for and the need to provide such information.

Storage of data

BEXs receives data either in paper format or electronic format.

Data received for the:

- Drafting of Wills:

- ❖ The information is scanned and saved on OneDrive in the specific folder created for the client under Wills drafted.
- ❖ If BEXs is requested to retain the original Will in safe custody the documents received are kept with the original Will in a folder in our safe.
- ❖ If BEXs is not requested to retain the original Will in safe custody, all hard copies of personal information are destroyed by either being shredded or incinerated.
- ❖ Upon notification that BEXs is no longer the executor, the electronic file is deleted.

➢ Administration of estates

- ❖ The information is scanned and saved on OneDrive in the specific folder created for the Estate.
- ❖ The paper documents are placed in a documents folder of the estate file, which is created for each estate.
- ❖ The files are locked away in a cupboard which restricts access.
- ❖ Once the estate if finalized, the original documents collected of the deceased is returned to the heirs and the paper file will be kept in storage for a period of 5 years, where after the paper file will be destroyed by way of shredding or incineration.
- ❖ The file on OneDrive will be kept for record purposes, should we receive enquiries in future.

➢ Administration of Trusts

- ❖ The information is scanned and saved on OneDrive in the specific folder created for the Trust.
- ❖ The paper documents are placed in a documents folder of the trust file, which is created for each trust.
- ❖ The files are locked away in a cupboard which restricts unauthorised access.
- ❖ Once the trust is terminated, the paper file will be kept in storage for a period of 5 years, where after the paper file will be destroyed by either being shredded or incinerated.
- ❖ The file on OneDrive will be kept for record purposes, should we receive enquiries in future.

➢ Drafting of Trust Deeds

- ❖ If BEXs is to be appointed as Trustees:

  The same process will be following as stated above for the administration of Trusts.

- ❖ If BEXs is not appointed as Trustees:

  - The information received is scanned and saved on OneDrive in the specific folder created for the client under Trust Deeds Drafted.
  - Once the Trust Deed is registered, all documents with regards to the trusts will be returned to the Trustees.
  - The information on OneDrive will be kept for records purposes should we receive enquiries in future.

Operating systems and software used by BEXS

BEXs uses Windows 7 & 10 Professional as their operating system. With the operating system comes OneDrive which is a Microsoft cloud storage facility.

BEXs make currently use of the following software:

- Microsoft Office 365
- Legal Ease

All data is stored on OneDrive. Backups of the Legal Ease system are performed monthly and evidence of the success of this recorded for good governance purposes. Data stored in the cloud is protected by the cloud provider, Microsoft in this case.

The following measures have been implemented to prevent unlawful access to personal information held by BEXs staff.

- The laptops of BEXs staff enjoy BitLocker encryption.
- Anti-virus software, Firewall and Network protection is installed on all laptops.

Data recovery plan is in place and tested yearly.

General guidelines with regards to the storage of data.

When information is received in paper format, it is scanned and stored in the applicable folder of BEXs on OneDrive.

When data is stored on paper, it must be kept in a secure place to prevent unlawful access.

BEXs further adheres to the following when data that is usually stored electronically, has been printed:

- When not required, the paper or files must be kept in a locked drawer or filing cabinet.
- Employees must make sure paper and printouts are not left where unauthorised people could see them, like a printer.
- Data printouts must 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 is protected by strong passwords that are changed regularly and never shared between employees. Currently passwords are changed every 30 days.
- No data is stored on removable media (like a CD or DVD.
- Data must only be stored on designated drives and servers and must only be uploaded to the approved cloud computing services of BEXs.

- Servers, if applicable, containing personal data must be sited in a secure location, away from general office space.

- Data must never be saved directly to laptops or other mobile devices like tablets or smart phones.

DATA USE

Personal data is of no value to BEXs 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 must ensure the screens of their computers are always locked when left unattended.

- BEXs employees and consultants are not allowed to access data from unsecure sites such as free Wi-fi zones, internet cafes etc.

- Personal data must not be shared informally

- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

- Employees must not save copies of personal data to their own computers. Always access and update the central copy of any data.

DATA ACCURACY

The POPI act requires BEXs to take reasonable steps to ensure data is kept accurate and up to date.

Given the nature of the services provided by BEXs accurate information is vital and given this, BEXs is vigilant on ensuring 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.

SUBJECT ACCESS REQUESTS

Should BEXs be storing personal data, the data subject will be 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 an individual contact the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the IT Manager admin@bexs.co.za. The IT manager will aim to provide the relevant data within 14 days.

The IT Manager 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, BEXs 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

BEXs 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

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

This is available on request. A version of this statement is also available on the company's website.

PASSWORD POLICY

This policy applies to:

- All staff, consultants and volunteers of BEXs;
- All contractors and other people working on behalf of BEXs.

All devices where data is stored electronically whether it is a Personal computer, laptop, tablet, iPad, cellphone should be password protected and additional fingerprint protection is encouraged.

The following is the standard required at BEXs with regards to passwords:

- The password must be changed every 30 days;
- The password must be a complex password, at least 6 characters long and consist of an uppercase and lowercase letter, a number and a special character.
- The password must not be written down and no person must have access to the password. Staff are encouraged to make use of “Key pass” to store important passwords.