Protection of Personal Information Act 2013 (POPIA)

Proudly SA Checklist

1. Appointment of Information Officer/s for Protection of Personal Information Act 4 of 2013

2. Training/assisting the processors and communication to stakeholders

2.1 Identified all the third parties who have a stakeholder interest in the personal information held by Proudly SA

2.2 Identified the means by which each of the third-party stakeholders has/will be informed and engaged to comply with the POPI Act

2.3 Governing bodies responsible to address the relationships referred to, and in each case, there was an employee tasked to communicate on behalf of Proudly SA

2.4 Conduct training as necessary, and keep a training roster

3. Personal data of the data subject managed according to POPIA

3.1 Processing of information [collection, use and destruction]: Listed of all the details collected regarding the data subject i.e. anything personal (person or company) that can go on a spreadsheet

3.2 Listed the channels through which, as well as the means by which information is collected

3.3 Listed the reasons why data is collected from every single group of data subjects

3.4 Listed Proudly SA's internal data processors

3.5 Listed Proudly SA's external data processors

3.6 Listed storage facilities

3.7 Listed the individuals who have access to the personal information of the data subject

3.8 Listed the actual data that will be collected from data subjects

3.9 Confirm that all data subjects consented to the processing of personal information in writing (see Consent form)

3.10 Confirm that Proudly SA has a legitimate mutually agreed upon necessary need and interest for the processing of all personal information of every data subject (also see Consent form)

4. Strategic Risk and Impact Mitigation

4.1 Individuals associated with Proudly SA who influences the personal information of the data subject, is listed and instructed to safeguard the personal information

4.2 Proudly SA acknowledges that the personal information of data subjects needs to be protected. As such, Proudly SA vows to engage in a risk impact assessment to protect the personal information of the data subject, described in in terms of high, medium and low (in order to identify priorities in the risk mitigation strategy)

4.3 Following 4.2, the following information is recorded and managed by the Information officer:

- an inventory of all data subjects types and their personal information
- data subject consent and instruction to:
  - hold data and reason for data held;
  - use data and reason for data used;
  - destroy data and reason for the destruction;
  - including a time frame on all of the above
- the identities of the data processors/operators
- how the data flows into and through Proudly SA to date of destruction
- how access control is addressed
- reasons for holding subject data
- the purpose for holding subject data

The Information officer identified the probability factor of risks for the data subject and actively and annually manage the risks.

5. Data Mapping

Proudly SA commits to identify risks for the data subject and fully address identified risks.

5.1 Compiled a list of every single party related to Proudly SA in terms of roles and responsibilities for each

5.2 Compiled a list of every single third-party institution involved with Proudly SA in terms of submissions and registrations for Directors and Shareholders

5.3 Compiled a list of registers and documents pertaining to the transactions relevant to the subject

5.4 Hardware and Software used

6. Employee Memorandum

6.1 Proudly SA provides the Employee with a work infrastructure which the Employee agrees to use responsibly.

6.2 Labour laws and practical arrangements require that Proudly SA collect personal information from the Employee, which herewith consents to the collection, dissemination and destruction of the personal information. Limited information is required.

6.3 Employees commit to fully and always abide by all applicable laws. All information processed on electronic devices are to be work related. All electronic information processed in work time is owned by Proudly SA. Company-employee arrangements include Information Technology related matters.

6.4 The Employee understands that Proudly SA makes use of a work infrastructure and third-party service providers and the Employee consents to the processing of the Employee's personal information by these third-party service providers.

6.5 Employees are individuals and delineated to engage in work related activities. Employees are restricted to attend to their own personal information and may under no circumstances process the personal information of other employees or third parties without fully complying to the applicable laws, of which the POPI Act is foremost.

6.6 All personal information of all third parties are strictly private and confidential and not to be processed by employees unless consented to by Proudly SA in writing.

7. Privacy Policy

7.1 The below will be added to Proudly SA contracts, website etc.

For the POPI Act, Proudly SA is deemed to be an organization that engages in all aspects of business. It follows that personal information could be processed in some of the following categories:

1. Employees
2. Clients
3. Vendors
4. Stakeholders, i.e. shareholders
5. Governing bodies, i.e. directors
6. Statutory bodies, i.e. SARS
7. Public viewers, i.e. websites
8. Hostile invaders i.e. hackers

7.2 A list of the processors, persons privy to the processing is enlisted for the specific information that is required.

7.3 Proudly SA vows to protect the information as prescribed by the POPI Act. As far as Proudly SA understands, all personal information is private and attended to according to the POPI Act.

7.4 Proudly SA will at all times measure the risk of breach of the POPI Act and actively manage same on a daily basis.

8. Processing of Personal Information

Proudly SA processors of information commit to secure data subjects' consent to process information. Data subjects fall into the following main categories: employees, members, vendors (to Proudly SA), etc.

8.1 Operators are an important category of processor, as recorded "Data Processors". A record of what information is shared, for what purpose and for how long, as well as that they acknowledge that they have sufficient security measures in place to prevent a breach on their watch is kept. Furthermore, responsible/relevant parties agree to notify the Information Officer immediately of any breach/compromise in security of any of the data subjects.

8.2 Compiled a list of data subjects. All individual contracts involve the data subject's allowed time frame and the purpose of the processing. These aspects are addressed in terms of the

scope and processing of personal information of the data subjects as information is recorded in filing systems.

8.3 Listed the responsible parties that instruct on all processing of information

8.4 Confidentiality agreements will be signed by all data processors (template already created)

8.5 Listed the software employed to mitigate the risks associated with the Act.

9. Data Protection Policy (available in company policy documents and website)

9.1 Proudly SA commits to continually uphold that the person responsible for instructing the Information Technology contractors to Proudly SA, is the person responsible for the processing of the information or has received a mandate to do so.

9.2 Proudly SA addressed all security on all personal information. Personal information is at least secure, but not limited to, in the following areas:

1. On end-points;
2. Data in transit;
3. Data stored in cloud;
4. In terms of antivirus, malware, Trojans, worms, phishing employed etc.

9.3 All Proudly SA officials, employees, vendors and members/clients are appropriately informed of measures taken to protect personal information and the processing of personal information. Unauthorized persons have no access to personal information and all persons who do have access, have minimum appropriate access to personal information.

9.4 Those who hold or process information consent to full surveillance of processing of personal information and consented to personal accountability for such processing. All operators and processors committed to protect personal information and to procure instruction from the responsible party on deemed processing.

9.5 Proudly SA procured the commitment of all operators and processors of personal information to employ maximum security and secrecy on all personal information, and to personally assume the responsibility to employ measures to protect personal information on all electronic equipment.

9.6 Devices, where applicable, are always kept on the processor's person. Neither the device nor any information on the device is ever given to third parties who do not hold the written consent of the data subject. Business data will always be kept separate from personal data – i.e., personal information.

9.7 Data is encrypted in order to safeguard data against unauthorized exposure to third parties. Data pertains to non-electronic files, end-point data, data in transit and hosted or cloud data. Least number of security codes are kept by least number of employees. The data specialist appointed by Proudly SA will take into account all risk factors and address same to the satisfaction of the POPI Act. Where possible, the number of data storages is maximized.

9.8 Proudly SA has done a risk and impact assessment on all cloud computing and is satisfied that its cloud computing adheres to the requirements of the POPI Act.

9.9 All non-electronic personal information is kept safe and rules and regulations are applicable to access of filing facilities and office spaces. Risk is reduced to the minimum on all aspects of processing personal information in that information is held behind the maximum practical guarded physical barriers as the environment allows.

9.10 All handlers of physical security acknowledged that they are responsible for compliance and undertake to ensure full compliance to the POPI Act. All personal information will always be kept and attended to in a secure manner.

9.11 Personal information is only used for the purpose obtained as instructed by the data subject.

10. Incident Management (Data Breach Incident Plan)

10.1 Proudly SA has approved procedures to manage incidents that may have an impact on the POPI Act. Roles and responsibilities are known to all responsible operators and data processors, and ready to be implemented when incidents occur.

10.2 All heads of department are in full control of all personal data and vowed to keep personal data safe and secure. Steps have been taken to reduce incidents and to increase the speed in which incidents are attended to. Operators and processors of personal information are forewarned to report incidents as soon as possible and managers are forewarned to attend to reports as soon as possible.

10.3 The data breach action plan includes:

1. All parties related to the incident will assist one another to attend to a breach as soon as possible with maximum allowed force.
2. When an incident occurs, the incident, in compliance with the POPI Act will not be discussed with anyone but the employee's direct manager.

3. Managers may only discuss incidents with the CEO.
4. The CEO may only discuss the matter with the board of directors, whereafter the board will direct the CEO.
5. Once a breach is confirmed, the CEO will communicate, as prescribed by the POPI Act, with the affected data subject, the Regulator and with those who may be influenced by the breach.
6. The following will be documented:
    a. All risks, incidents, and threats.
    b. All responses to the above.
    c. Number of data subjects involved, with their contact details
    d. Details of the breach, i.e. time, place, format of data, size of breach, reasons and possible consequences, etc.
    e. An action plan to remedy the breach with the roles and responsibilities of all parties related to the matter.
    f. Proudly SA has forms and written procedures for all steps related to the stages of breach.

11. Personal Information Management

The data subject remains the owner of his or its personal information. The data subject is the sole stakeholder of his or her or its personal information and Proudly SA acknowledges the latter facts.

11.1 Proudly SA logs all consents obtained from the data subject in a central register. The data subject consents contain the following:

1. The initial consent allowing Proudly SA to hold the specific personal information;
2. Ongoing consents detailing the confirmation and changes to the personal information;
3. Confirmation to data subject of his right to access to the personal information;
4. The purpose for which personal information is held by Proudly SA;
5. Who in Proudly SA would receive and hold the personal information;
6. The length of time which the personal information will be held;
7. When or in what event the personal information will be destroyed.

8. Agreement on identity of third parties to whom the data subject ceded rights above.

11.2 Proudly SA holds request and consent forms for data subject enquiries and instructions, and will provide these to the data subject or third party who holds instructions on behalf of data subject. Refer to Consent form.

12. Customer and Supplier Consent & Update for the Protection of Personal Information Act 2013

The Protection of Personal Information Act 4 of 2013 (POPIA) protects information personal to individuals and businesses (Data Subjects). The owner of information is the data subject. All other relevant parties are deemed to be processors of personal information. POPIA requires Data Subjects to instruct processors on the obtaining, use, purpose of use and destruction of personal information.

12.1 Consent form templates are designed and sent to new recruits and renewing members in terms of consent and instruction on personal data.

13. Access Management Registration Control

13.1 Proudly SA must always record changes in access granted to information systems through hardware and software for internal and external users through a set-up access change form that has been designed).

13.2 Listed all IT requirements pertaining to access status change of information and agreement with the user is concluded.

14. Promotion of Access to Information Act 2 of 2002 Manual (PAIA Manual) and Promotion of Access to Information Act: Section 51 Manual – Updated

[UPDATED: 18 August 2018]