Annexure A – POPI Checklist

This checklist should assist companies to assess their compliance with POPI.

# Audit: Review the process / forms etc. which your organisation uses to collect, record, disseminate and destroy personal information. It is important to review the entire process before starting.

**Specifically Review the following:**

* **Recruitment process:** How does the company receive, store and communicate information regarding candidates and for how long does the information get stored? Do you have the necessary consent from the candidate to retain the information if they are not successful in their request for employment
* **New employee take on process:** Does the company have clauses in Employee contracts explaining why specific personal information is required and does the Employee consent to this? In what manner is the information obtained, and how is this information then stored? Is the information stored in a secure environment?
* **Software security:** Is the software package used that manages Payroll / HR data from a reputable company? Is password complexity monitored? For what period of time are passwords valid?
* **Database storage**: Is your solution hosted in house or on the cloud? If in house, does your company have sufficient IT security protocols in place and are they monitored and evaluated on a periodic basis? If cloud based systems are used, have you reviewed your suppliers security certificate of compliance and gained and understanding of where is the data and system software is physically located? Are there regular backups taking place and are they tested frequently?
* **Information dissemination**: How does the HR/Payroll Department handle movement of personal information? Are the Employees aware and have they given consent that the company records and retains this information.

# Purpose: Define the purpose of information gathering and processing.

Personal Information can only be gathered for specific and openly defined, lawful purposes related to a function or process within the company.

# Ask the following questions:

* 1. Why am I collecting the information – i.e. is it to be compliant with SARS, the Dept. of Labour, etc.?
	2. Has the employee consented?
	3. In what manner will this information be used – i.e. to ensure that a correct Tax Certificate is submitted to SARS every six months?
	4. Is this collection of specific data lawful?
	5. Does this information relate directly to a function/process within the organisation?

# Limit Considerations: Information collected must be lawful, adequate, and relevant to the purpose for which it is processed.

**Ask the following questions:**

* 1. Is this information relevant? i.e. Surname vs Religion?
	2. Are there any other processes that require this information? i.e. Medical Aid Recons
	3. Is it a legal requirement to keep this information? i.e. IRP5s
	4. Have you validated that the information is correct?

# Inform the Employee: The Employee must be informed that his/her information is being captured, retained and processed and exactly what the information will be used for.

**Ensure you have the following in place:**

* A clause in your employment contract specifically pertaining to the storage, processing and use of personal information.
* The Employees’ consent to do so.

# Procedures: Procedures for processing information must be in line with POPI Ask the following questions:

* 1. How is information received from third parties – how do I know it is accurate?
	2. How is information communicated to third parties – how do I ensure that I only provide that which is needed, and do I know what they are going to do with the data?
	3. Has the Employee consented to the dissemination on his/her information between the company and these third parties?
	4. Is the information secure while in “transit” – how do I know this?
	5. Was the information initially collected for this purpose?

# Employee Requests: Information must be available to Employees. Employees have the right to at any point in time request a list of information and third parties that may have access to their information.

1. **Corporate Governance Officer: Appoint a Corporate Governance officer.**

You need an internal champion – i.e. someone who responsible / accountable and constantly reviews what data you have, what data you need, how will you get the data without infringing on someone’s privacy, and how will you manage the data.

# That person also needs to establish a policy re:

* 1. At what point does the data / information become obsolete.
	2. How does one delete / destroy redundant information.
	3. How does one archive and then subsequently retrieve data / information.