PROTECTION OF PERSONAL INFORMATION ACT, COMPLIANCE MANAGEMENT PROCEDURE

BETTERCOVER CC
FSP 7081

Unit E08, Prospur Business Park.

1998/021844/23

Tel: 010 880 2732

Last update 23/4/2024

INDEX

1. INTRODUCTION

POPI introduces dedicated data protection legislation to South Africa. POPI is not exclusively an Information Technology or Legal process or security issue; it is a combination of all of these.

The **PURPOSE** of POPI is very clear: to promote the protection of personal information that is processed by the private and public sectors. POPI will place a responsibility on companies and public bodies who deal with personal information on a daily basis.

Your right to privacy (that is recognized by the Constitution of South Africa) is balanced against other needs and interest, such as economic growth.

WHAT DOES POPI DO?

POPI regulates the processing of personal information within South Africa. It is concerned with the processing of personal information.

From the 1st of July 2020, organisations will have 12 months, or one year, to comply with the conditions for the lawful processing of personal information.

Organisations, public and private, big and small, and anyone processing personal information, will have to align their processing activities to the Act. Whether such processing involves personal information of your employees, prospective employees, part-time workers, contractors, clients, members, consumers, customers or third-parties or anybody else whose personal information you collect, use, share, retain, store, archive, delete or destroy – you, as a processing entity, will have to ensure that you, or anybody that processes personal information on your behalf, complies with the Act.

2. COMPANY PRIVACY POLICY

We are committed to transparency and confidentiality relating to our clients personal and private information, which we collect and process for the purpose of providing advice and intermediary support and servicing of financial products.

We will obtain and share relevant personal information to:

- Furnish appropriate financial advice
- Determine our client's financial situation, financial product experience and financial needs and objectives
- Acquire, maintain and service any financial product
- Render appropriate intermediary and financial services

Clients information will be handled confidentially and will only be made available with client's authorization or where we are compelled by law to do so. Claim information is however shared on an industry wide basis.

3. CLIENT CONSENT TO GATHER AND KEEP INFORMATION

We are committed to:

- Obtain client's consent for the information that we keep and share.
- We have no intent to gather and keep information with the intention to sell this information to a third party for market purposes.
- We ensure that our staff within our company will be fully trained on our culture of treating your information with the uttermost confidentiality to always treat you fairly.
- We can guarantee that our organization will only disclose a client's private information to other specifically designated organizations in the scope and course and for the purpose for which it was provided for – and not to any other third party without first obtaining the clients consent thereto.
- We only intend to utilize your information for the purposes which it was obtained for and only to share your information with the insurers and underwriters that we do business with.

4. RISK MEASURES ON ELECTRONIC DATA

Unfortunately, there always exists a possible risk that client's private electronic information might be unlawfully accessed by a third party without our nor client's consent. This can expose our organization to not only to reputational damage, but we will also face enforcement action being taken against us by the Information Regulator.

Our client will be put in severe jeopardy for risks such as identity fraud and theft and access to extremely highly confidential information such as ownership of personal assets and the value thereof, security measures of such or personal medical status.

To limit the possibility of electronic information being hacked or unlawfully accessed, we have decided to implement the following measures:

- A firewall will be installed to try and limit the opportunity to hack our electronic database from a remote destination.

- All computers will have password protection that will be updated and changed on regular intervals.
- Appropriate anti-virus software will be installed to limit the spread of unwanted computer viruses and curb the access of information technology experts.
- Staff will be discouraged to install work e-mail address on their cellular telephones.
- Should staff conduct their work activities from premises other that the head office, access to the mainframe electronic database will be limited on their work laptops.
- Strict company policies will be implemented on the use of laptops at designations where public can have access to information that is kept on the electronic device.
- Only staff will be permitted to utilize work electronic devices and under no circumstances may any friend or relative have access to such a device.
- Back-ups will be done at regular intervals and the data that is backed-up will be stored off-site at a secure designation.
- Should an Information Technology company be utilized to back-up information, they will have to provide us with a Compliance Certificate that will guarantee the confidentiality of information.
- Laptops are portable so there is a higher risk that they can be stolen. As a consequence, it is important to take more security measures in order to protect all laptops. A simple solution is to encrypt them. In doing so, without the right password, your computer's Data is unreadable.
- Train employees on the risks imposed by cybercrime. Train your employees to develop good habits and draw their attention to behaviours that should be avoided (opening an email form or downloading an attachment from an unknown sender etc.).
- Remotely working collaborators should double their vigilance, namely with regard to emails that they receive, even if they seem to come from a known source as they might be tools of/for phishing.
- If possible, verify authenticity of messages by contacting the sender directly (in person, over the phone …)
- Do not click on any links or download attachments if you don't know the sender of the message or if you are hesitant about its content,
- Be wary of emails from people who you don't know, always try to verify information through other means.
- Make sure that your Wi-Fi connection is secure and password protected. Should it/this not be the case, everyone in your surroundings, for example your neighbours, will be able to connect to your network.
- If you work in a co-working space, do not forget to lock your screen.
- If ever old computers are replaced, the hard driver of such will first be cleared before the computer can be disposed of.
- If your computer(s) or database gets stolen, you must notify clients if their information is on that database as their information can or might be compromised.

The notification to client must provide sufficient information to allow the client(s) concerned to take protective measures.

5. RISK MEASURES ON MANUAL, HARCOPY DATA

To limit any exposure of data breaching in office as far as it relates to hardcopy files and/or documents, the following measures will be implemented:

- Under no circumstances may documentation be openly left on the desk of any staff member. If a client's file is not being utilized it will be safely stored away from public access;
- If any confidential personal information of a client is being disposed of, it must first be destroyed by means of shredding and or other measures such as burning (fire).
- Client information and files must be stored in cabinets and/or cupboards that can be locked.
- Limited access must be available to access confidential information of a client. If an employee is not actually involved with such a client, then access must be curbed.
- If data breach is suspected, surveillance must be installed.
- Restrict the duplication of documents. Photocopies will be monitored and restricted to only what is necessary.

6. *COMPLIANCE CERTIFICATES*

- We will review existing agreements from all suppliers and organizations that our company do business with. These entities must provide guarantee(s) that they hold necessary and required procedures whereby our client's information will be kept confidential.
- We understand that should we omit to do so and continue doing business with organizations that cannot or did not provide us with the required Certificate, and if private information is leaked, our company will be held accountable and liable for such loss.

7. ***STAFF AND EMPLOYMENT CONTRACTS***

- We will first obtain consent from our **STAFF** and/ or new job applicants if we intend to do reference checks and more so and in specific if we conduct credit or criminal checks.
- Confidential information of the staff compliment, such as Salary Packages, Garnishee orders, marital or health status, will only be disclosed with the relevant employee's consent.
- Information of our employees and the employment contracts, disciplinary actions and other will be kept in a safe, locked designation and only limited Human Resources individuals will have access to these records.

8. ***INTERNAL INFORMATION OFFICER***

We hereby appoint Shante' Rogers as our INTERNAL **INFORMATION OFFICER** within our organization.

The following duties are bestowed upon this officer:

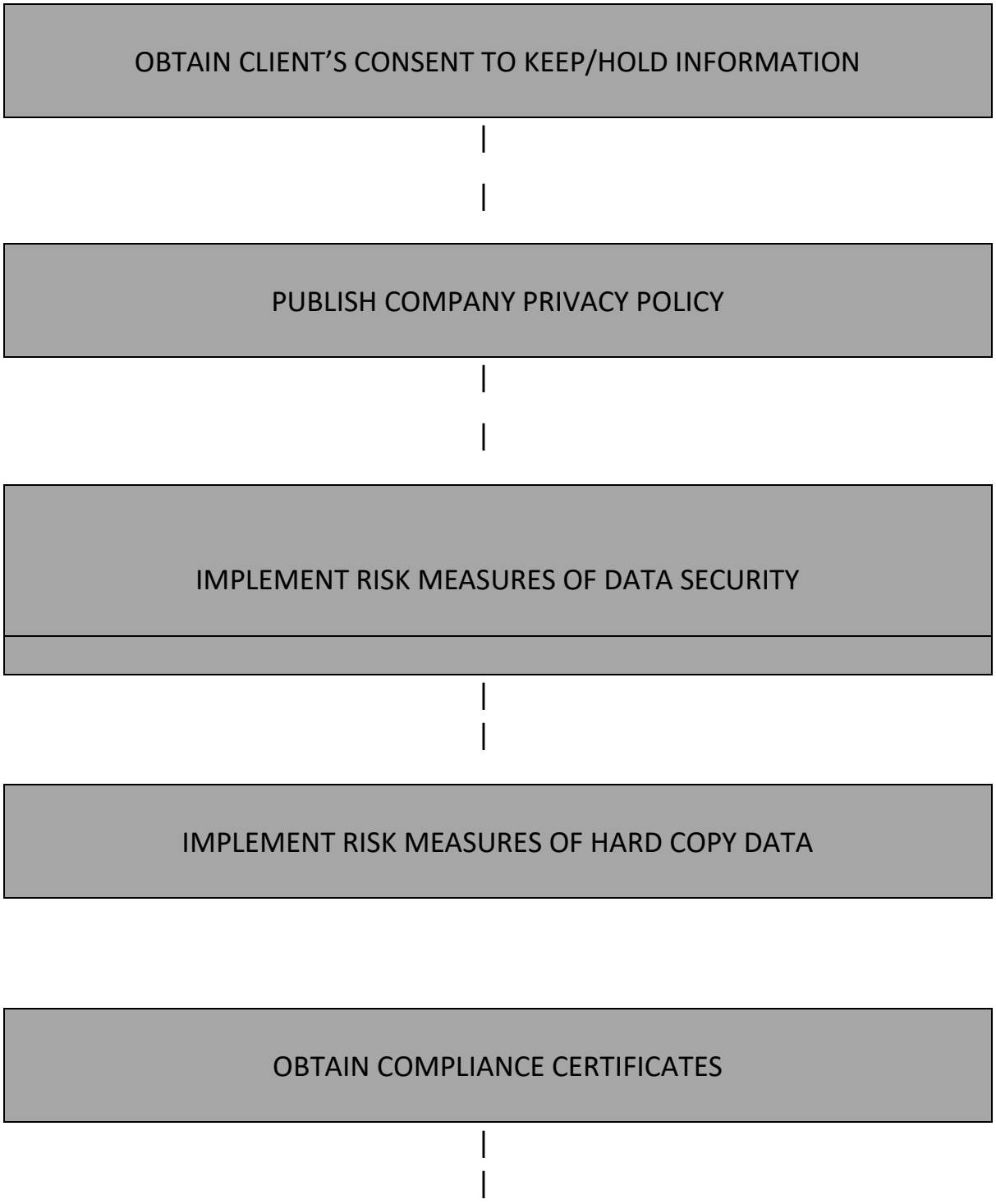
- Comply with legislative requirements.
- Updating and revision of this procedure.
- Staff training on the contents of this procedure.
- Ensure implementation of the measures listed herein.
- Continuous monitoring of possible breaches.
- The function of the Information Officer would be *inter alia* to correspond with the Information Regulator in instances of contravention of legislation.
- The Information Officer can delegate his/her responsibility to a Deputy Information Officer; last-mentioned must be registered with the Information Regulator.
- Enforcement action will be against the designated Information Officer/deputy and one can be imprisoned up to 10 years should you be found guilty of an offence.

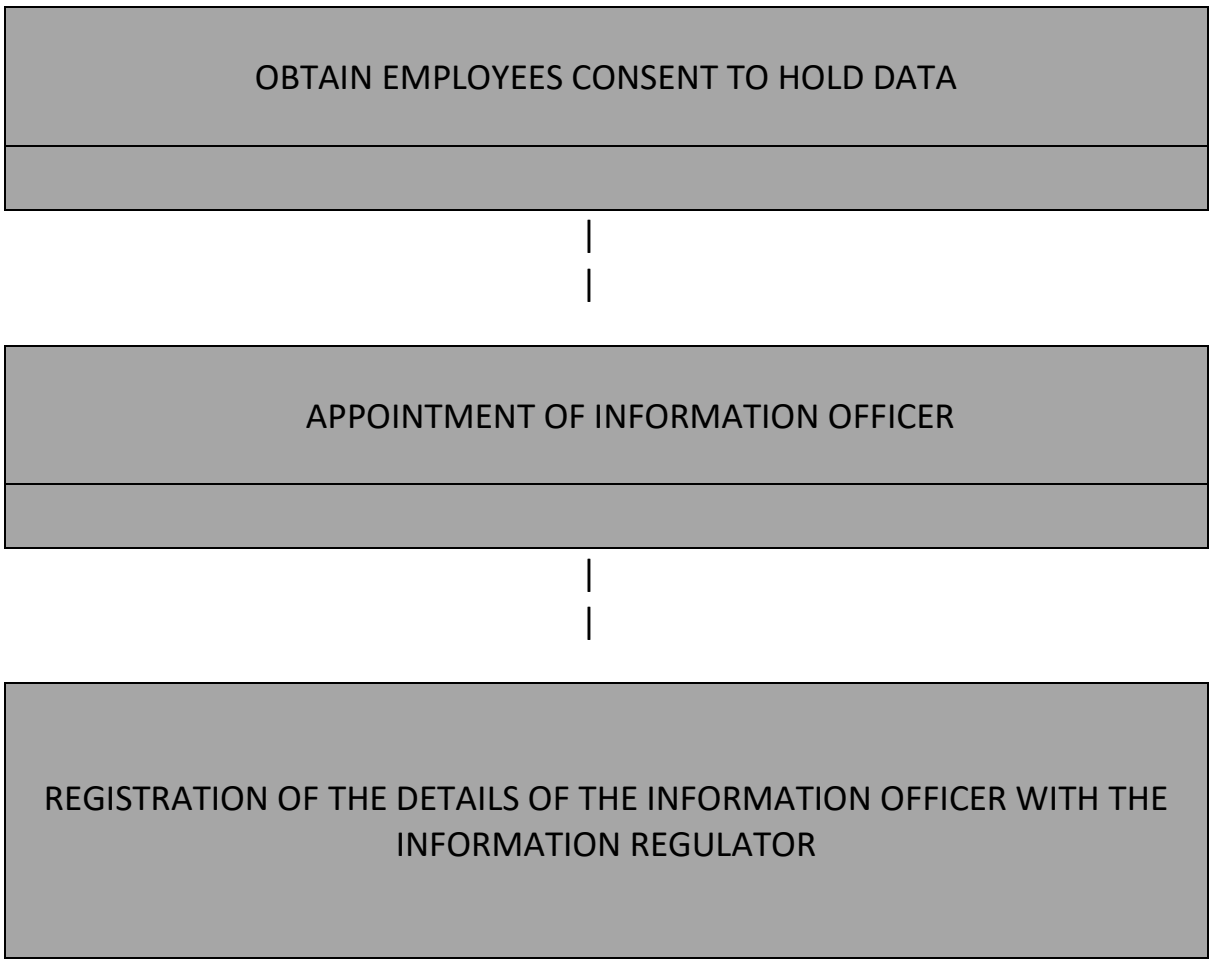
The appointed Officer's details will be registered with the Information Regulator within 5 days of appointment.

The Information Regulator (South Africa)
33 Hoofd Street
Forum III, 3rd Floor Braampark
P.O Box 31533
Braamfontein, Johannesburg, 2017
Mr Marks Thibela
Chief Executive Officer
Tel No. +27 (0) 10 023 5207, Cell No. +27 (0) 82 746 4173
inforeg@justice.gov.za

9. FLOW CHART OF IMPLEMENTATION PROCESS

FINAL DATE FOR FULL IMPLEMENTATION: 30 JUNE 2021




OBTAIN EMPLOYEES CONSENT TO HOLD DATA
APPOINTMENT OF INFORMATION OFFICER
REGISTRATION OF THE DETAILS OF THE INFORMATION OFFICER WITH THE INFORMATION REGULATOR