Data Usage Policy POPI ACT – HRP019

General
Data Security and Privacy of personal data is one of the most important issues affecting the Company's daily operation. This policy outlines the basis of data maintenance and control, and it is a requirement that the policy be always complied with. Each employee will be required to sign the policy and hand back to HR before access to any personal data, or client data is allowed.

Background:

With the introduction of the POPI Act in South Africa and similar Acts in Europe called GDPR, it is extremely important for businesses that work with personal data be protected from being prosecuted for misuse of Personal information.

The POPI Act does not stop you from processing and does not require you to get consent from data subjects to process their personal information. Whoever decides to process personal information is responsible for complying with the conditions.

There are 8 key conditions that are introduced by the POPI act. Any entity (both natural and juristic persons) that processes, stores or controls personal information must comply with these key conditions of the POPI act.

1.You are accountable, no excuses.
The responsible party will be held accountable for the management and implementation of the items mentioned above.

2.Limitations on how you may process Personal data.
Personal information must be processed in accordance with the law. It must be managed and stored in a secure and careful manner and may not intrude on the privacy of the person whose information is being processed.

3.Don't over process the personal data.
Information may not be processed beyond the initial purpose, why it was collected, that would make it incompatible with the original purpose.

4.All information must have a reason.
The information must only be collected for a specific reason, which is properly and clearly defined and must be for legitimate purposes. The information may not be kept for longer than needed. Data cannot be kept indefinitely if it is not being used anymore.

5.Make sure the data is accurate.
The person collecting the data must take steps to ensure that the data is complete, accurate, up to date, and not misleading in any way.

6.Security is most important.
You are required to ensure the integrity of the data as well as protecting it from unauthorized access in your organization and from external parties.

7.Right to know how much and what.
Details of what data and information is being collected must be made available to the person requesting the information, free of charge. They must understand what data is being collected, why such data is being collected, how it is stored, where it is stored and that they have the right to request that it be discarded after its initial purpose has been met.

8.Be honest about your intent.
Personal information may only be collected by someone who has given notice to or disclosed the requirements, the purpose of, and the reason to the person concerned. Consent should be obtained.

Some of the sensitive data that is considered under POPI as being Personal Information:

- Race / nationality / ethnic / social origin / colour
- Gender / sex
- Pregnancy
- Marital status
- Sexual orientation
- Age
- Physical or mental health / well-being / disability
- Religion / conscience / belief
- Culture/language
- Birth

This is extended by any educational, medical, criminal, employment, or financial information.

Basic rules to always ensure compliance.

- Usernames and passwords may never to be shared with any other party.
- All access to data much be done with own personal user account.
- Auditing needs to be in place to track access to any systems that contain personal data.
- Password complexities need to comply with the minimum security accepted by the international standard applied by the industry.
- No data can be moved form a Production system to a local machine for processing. If this is needed the data need to be obfuscated or encrypted.
- If data is place on a personal computer/workstation, the data must be destroyed once the work activity is concluded. The data may not be kept for longer than 30 days on a local personal or work-related workstation.
- No Personal data me by copied.
- No personal data may not be printed out and left unprotected in any location (If this is a need, the printed material needs to be secured with limited access
- When working on a computer while there is visible personal data on the screen, the computer may not be left unattended with out a Locked screen saver with a Password protection that comply with the minimum password complexity.
- If data has sent to a customer, external party, or 3rd party, there needs to be a record of the request to send the data.
- All data being transferred needs to be compressed and protected with a password so the data inside cannot be access by unapproved parties.
- When a request for data extraction is received the user must confirm and get approval from a direct line manager before supplying the extracted data to the requesting party
- Based on the restrictions identified by the POPI Act of South Africa all users/employees need to understand the limitations placed on them and the business. All details about the POPI Act can be read here https://popia.co.za/
- If an Employee has any doubt about the process, they are following it needs to be raised with the direct line manager at any time.

Acceptance of Policy and compliance:

I _____ with ID number/Passport _____hereby accept the data protection policy as listed here in and agree to all the conditions listed in the policy document. I will not copy and/or share any personal data with an unauthorized party.

Signature: _____

Name: _____

Date: _____