# General recommendations to employers to ensure POPI compliance

In light of the duties imposed on employers, it is recommended that the following steps be taken to ensure compliance with POPI:

* Employers should ensure that their staff, especially those who process employee information on a regular basis such as Human Resources and IT officials, are aware of the duties imposed on employers by POPI.
* A data privacy policy should be drawn up and the employer should ensure that all employees are made familiar with its contents. The policy should include protocols enabling employees to lodge complaints against processing.

From a contractual perspective, employment contracts should also be worded broadly when requiring the employee to provide consent to processing so as to cater to the broad definition of 'processing' in POPI. Employment contracts should incorporate sufficient information relevant to the processing so that it can be said an employee gave informed consent.

Employers should take care when processing 'special personal information' such as ethnicity and trade union membership. Employers must ensure that proper security safeguards are in place to protect personal information from unauthorised access or deletion. Employers must ensure they comply with POPI regarding the transfer of personal information to third parties in foreign countries. Legal research must be done to determine whether the country which the information is transferred to has promulgated privacy protection legislation similar to POPI.

Tavcor Motor Group (Pty) Ltd POPI – Employee and Employer Annexure

The employee must take note of the following impact in terms of information, personal information and all business information, in terms of the Protection of Personal Information Act.

The purpose of POPI is to give effect to the constitutional right to privacy, by introducing measures to ensure the personal information of 'data subjects' (such as employees) is safeguarded when it is processed by 'responsible parties' (i.e. employers). POPIA provides conditions for the lawful processing of personal information. The Employer commits to comply with these principles whenever the personal information of employees is collected, stored or used.

Similarly, the employee must understand the same principles apply in terms of information of the business and customer information. The employee must adhere to the compliance of POPI and the subsequent POPI policy of the employer.

# Processing of information

## Accountability

The employer will process the information in line with the eight conditions set out in POPI. The effect is given to such conditions at the time that the purpose and method of processing have been determined, as well as during the processing itself. The Information officer and deputy information officers will ensure compliance with these conditions and deal with complaints from employees who seek to enforce POPI.

## Limitations on processing

The personal information processed by an employer must also be adequate, relevant, and not excessive, relative to the purpose for which the processing was undertaken. The necessary consent will be obtained from the employee in this regard.

In terms of the employment contract, the employee is made aware of the legal obligations of the employers in terms of the Basic Conditions of Employment Act 75 of 1997, as amended ("BCEA"), and the Labour Relations Act 66 of 1995, as amended ("LRA").

## Purpose specification

The employer collects personal information, it does so for specific, explicitly defined, and lawful purposes related to the function of the employer.

Personal information will be retained for as long as a law or code of conduct determined by the Information Regulator provides. In the absence of a law or code of conduct, the retention period must be long enough to afford the employee a reasonable opportunity to request access to the records.

## Further processing limitation

If an employer wishes to process information more than once, the subsequent processing must also comply with the conditions set out in POPIA and be compatible with the original purposes for which it was collected. An example would be where the employer has collected the email addresses of employees then makes it available to them by emailing the mailing list to each employee. Making it available would constitute 'processing' and would have to comply with the initial purpose for which the emails were collected.

## Information quality

An employer must take reasonable practical steps to ensure that the personal information is complete, accurate, not misleading, and updated where necessary. The employer must have regard to the purpose for which personal information is collected or further processed.

## Openness

An employer must maintain documentation of all processing. A particularly onerous duty placed on the employer is that before processing, it must take reasonable practical steps to ensure that the employee is aware of an array of facts. Such details would have to include what information is being collected, the purpose of such collection, and who will have access to the information.

If the employer intends to transfer the information to a country outside South Africa, then the employee must be notified as such. The employee must also be informed of his or her right to access the information and the right to rectify it; as well as the right to object to the processing of personal information. Similarly, an employee must be informed of the right to lodge a complaint to the Information Regulator and the contact details thereof. It is recommended that all the information above be incorporated into the employment contract to cater for information that the employer knows or predicts will be processed.

## Security safeguards

An employer must secure the integrity and confidentiality of personal information in its possession or under its control. This must be achieved by taking appropriate and reasonable technical and organisational measures to prevent loss, damage, or unlawful access or processing of personal information.

The employer must take reasonable measures to identify all reasonably foreseeable internal and external security risks and establish appropriate safeguards. The employer must have due regard to generally accepted information security practices and procedures which may apply to it generally, or be required in terms of a specific industry or professional rules and regulations. All employers should ensure they have updated anti-virus software and firewalls for the protection of digitally-stored personal information.

Ideally, backups should be made on a remote server so as to be prepared for the accidental deletion or local hard drive failure. Regular IT maintenance is also recommended. Physical records must only be accessible by authorised personnel and should be kept in a secure location. Where there are reasonable grounds to believe that the personal information of an employee has been accessed or acquired by any unauthorised person, the employer must notify the Information Regulator and the employee as soon as possible.

## Employee participation

An employee has the right to request access to the record of his or her personal information held by the employer. The record must be provided within a reasonable time, manner and form and may be at a prescribed fee. The employee has a right to request that the record be corrected or deleted if this is warranted. If an employer receives such a request but refuses to comply, then it must provide the employee with a notification to that effect. It must also attach an indication to the record that a particular request was made but was not executed.