

POPIA Explained – Part 16

By Lize de la Harpe, legal adviser

In the last edition we discussed enforcement of the act as well as offences, penalties and administrative fines.

In this edition we will focus on POPIA in the workplace.

Recap on the role players

In the first edition we discussed the various role players in terms of POPIA, being the data subject, responsible party and operator.

Section 1 defines a “responsible party” as a public or private body which, alone or in conjunction with others, determines the purpose of and means for processing personal information. Put simply: it’s the person/entity who decides what personal information must be processed and how it is processed. As such, the term includes employers.

The “data subject” refers to the person to whom the *personal information* relates. *Personal information* refers to information relating to an identifiable, living natural person or juristic person. The term data subject will as such include applicants (*and former applicants, whether successful or unsuccessful*), former or current employees, contractors and casual workers (hereafter simply referred to as “employees”).

Personal Information of employees

As discussed before, the act applies to any personal information entered into any record by a responsible party. As stated above, employees qualify as data subjects – and as such, the act applies (with the same exceptions) to all employee records containing personal information as held by an employer.

(*PS: As discussed in Part 11 – retention of records – the term “record” includes any recorded personal information regardless of form or medium that’s in the possession or under the control of the responsible party, whether or not it was created by a responsible party and

regardless of when it came into existence).

Personal information of employees would include details of an employee's salary and bank account, e-mails, personnel file, leave records, performance reviews, etc. It may also include personal information that qualifies as Special Personal Information as set out in section 26 of the act. Special personal information includes information about a data subject's:

- religious or philosophical beliefs;
- race or ethnic origin;
- trade union membership;
- political persuasions;
- health or sex life;
- biometric info; or
- criminal behaviour.

As discussed in Part 2 ("*Types of Personal Information*"), the processing of Special Personal Information is prohibited UNLESS one of the exemptions as set out in section 27 applies (**see copy of part 2 attached*).

Processing by employers

As you well know, the processing (and further processing) of personal information is only lawful if it complies with the eight Conditions as set out in Chapter 3 of the act. Accordingly, the processing of personal information of employees must at all times comply with the eight Conditions as set out in the act.

Processing by an employer covers a wide range of activities, including *but is not limited to* the following:

- Recruitment of staff, including retention of application forms and supporting documentation (**e.g.: such as cv's, copies of degrees, IDs, etc*)
- Paying salaries;
- Processing and storing leave requests;
- Performance assessments;
- Administration of retirement fund benefits;
- Internal documentation relating to disciplinary action; and
- Processing personal information for purposes of termination of an employment contract.

****PS:** *Special care should be taken when processing personal information regarding an employee's trade union membership, which falls within the category of Special Personal Information - see section 30.*

Vicarious liability of employers

Common law

Before we look at the liability of the employer (*as a responsible party*) for acts performed by employees in the context of the act, let's take a step back and look at the common law principle of vicarious liability of employers.

Even before the introduction of POPIA, the legal principle of vicarious responsibility of employers was well established in SA law. In terms of the common law principle of vicarious liability an employer will be held liable for the delicts committed by its employees where the employees are acting in the course and scope of their employment.

Civil remedies – section 99 of the act

As mentioned in the last edition – copy attached - section 99(1) (*Civil Remedies*) provides that a data subject or the Information Regulator (at the request of the data subject) may institute a civil action for damages in a court against a responsible party for breach of any provision of the act as referred to in section 73 (*i.e.: arising from an interference with the protection of personal information*), whether or not there is intent or negligence on the part of the responsible party.

Section 99(1) therefore entrenches the common law principle of vicarious liability into POPIA. As such, an employer may be held vicariously liable for the conduct of its employees, whether or not there is intent or negligence on the part of the employer.

Mitigating the risks

Employees may, as per of their role, process the personal information of clients (as well as the processing of personal information of other staff members by HR staff).

Notwithstanding the measures put in place by employers to limit the risks of breach by employees when processing information, it is critical to remember that section 99(2) as also discussed in the last edition limits the defences which may be raised by the employer against a civil action for damages, being:

- a. *vis major* (**being “an act of God”*); or
 - consent of the plaintiff; or
 - fault on the part of the plaintiff; or
 - compliance was not reasonably practicable in the circumstances; or
 - the Information Regulator has granted an exemption in terms of section 37 (**as discussed previously in Part 14 when we discussed the powers and functions of the Information Regulator*)

).

It is therefore not enough for only the employer to be aware of the obligations imposed by the act – they will need to ensure that their employees comply with these obligations as well when processing personal information on their behalf.

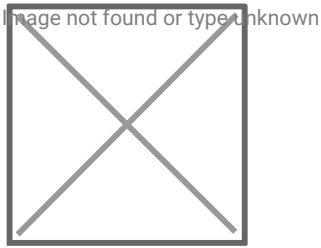
Similarly, in the HR context, employers will have to evaluate the types of personal information they collect, the purpose therefore as well as its retention policies in that regard (also having regard to legislative time periods applicable to staff information such as the Basic Conditions of Employment Act, etc), revise contracts of employment to provide for the necessary consents to process (and further process) personal information, revise HR policies, ensure it has adequate policies and procedures in place to comply with the eight Conditions and adequately train staff to ensure compliance with the act.

However, having regard to the wording of section 9(1), the implemented measures may not necessarily be enough to limit the risks faced by the employer in respect of breach by an employee. It may however serve as mitigation of such risks, especially considering that section 99(3) empowers the court to award an amount of damages that is just and equitable which will depend on the particular circumstances (**put differently: the court will take these measures into account when determining an appropriate amount of damages*).

Conclusion

The provisions of section 99(1) has a serious impact on employers. It is therefore vital that responsible parties ensure that staff are adequately trained on the requirements for lawful processing of personal information and that they have the appropriate security measures in place to safeguard this information.

Equally important: employers need to ensure that they *do not ask more information of their employees than what is absolutely required* for the purpose for which it is collected. Put differently, carefully check what *types of* personal information you request as part of your recruitment process and in terms of your employment contracts and remove fields requesting special personal information *that it's not absolutely necessary for the intended purpose* In the next edition we will discuss POPIA in the context of retirement funds in more detail.



Lize de la Harpe

Lize de la Harpe obtained an LLB degree in 2005 from the University of Stellenbosch, whereafter she completed her articles and was admitted as an attorney in the Cape High Court. During 2008 she completed a Postgraduate Diploma in Financial Planning (CFP) from the University of the Free State. Lize joined Glacier in June 2012 as the legal adviser and principal officer. Prior to joining Glacier, she worked as legal counsel in the investment cluster at Momentum for four years.

This document is intended for use by clients, alongside their financial intermediaries. The information in this document is provided for information purposes only and should not be construed as the rendering of advice to clients. Although we have taken reasonable steps to ensure the accuracy of the information, neither Sanlam nor any of its subsidiaries accept any liability whatsoever for any direct, indirect or consequential loss arising from the use of, or reliance in any manner on the information provided in this document. For professional advice, please speak to your financial intermediary.

Glacier Financial Solutions (Pty) Ltd.

A member of the Sanlam Group

Private Bag X5 | Tyger Valley 7536 | Email client.services@glacier.co.za | Tel +27 21 917 9002 / 0860 452 364 | Fax +27 21 947 9210 | Web www.glacier.co.za | Reg No 1999/025360/07

Licensed Financial Services Provider | Glacier Financial Solutions (Pty) Ltd. is also a Licensed Discretionary Financial Services Provider FSP 770, trading as Glacier Invest | Sanlam Multi-Manager International (Pty) Ltd. | A member of the Sanlam Group

Private Bag X8 | Tyger Valley 7536 | Tel +27 21 950 2600 | Fax +27 21 950 2126 | Web www.smmi.com |*Reg No 2002/030939/07

Licensed Discretionary Financial Services Provider, acting as Juristic Representative under the Glacier Financial Solutions FSP 770

Glacier International is a division of Sanlam Life Insurance Limited

Sanlam Life Insurance Ltd. | Email life@sanlam.co.za | Tel + 27 21 916 5000 / 0860 726 526 | Fax +27 21 947 9440

Reg No 1998/021121/06 | Licensed Financial Services Provider