POPIA Explained – Part 7

By Lize de la Harpe, legal adviser

In the last edition we recapped on the eight conditions for the lawful processing of personal information and discussed Information Quality and Openness in detail.

In this edition we will move on to the next condition, namely Security safeguards.

Let's recap

As explained previously, POPIA requires the responsible party to process personal information lawfully and in a manner that does not infringe on the privacy of data subjects.

In order for such processing to be "lawful" it must comply with the conditions as set out in the act. Section 4 of POPI lists eight conditions for the lawful processing of personal information, namely:

1. Accountability (as referred to in section 8);
2. Processing Limitation (as referred to in sections 9 to 12);
3. Purpose specification (as referred to in sections 13 and 14)
4. Further processing limitation (as referred to in section 15);
5. Information quality (as referred to in section 16);
6. Openness (as referred to in sections 17 and 18);
7. Security safeguards (as referred to in sections 19 to 22); and
8. Data subject participation (as referred to in sections 23 to 25).

Let's look at Condition 7, namely Security safeguards, in more detail.

Security safeguards – sections 19 to 22

Security measures on integrity and confidentiality of personal information – section 19

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent:

a. Loss, damage or unauthorized destruction of personal information; and

b. Unlawful access to or processing of personal information.

In order to do this, section 19(2) states that a responsible party must take reasonable measures to:

a. identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control (**for example, conducting an audit to determine whether current measures leave personal information susceptible to being lost, damaged or destroyed and/or easily accessed by a third party*);
b. establish and maintain appropriate safeguards against these identified risks (**i.e.: once you know where your data protection weaknesses are, you must implement the necessary steps*);
c. regularly verify that safeguards are effectively implemented (**for example, by monitoring systems and processes to determine if the security measures put in place are effective*); and
d. ensure safeguards are continually updated in response to new risks or deficiencies.

Responsible parties must also have due regard to generally accepted information security practices and procedures which may apply to them generally or be required in terms of a specific industry or professional rules and regulation (**such as, for example, industry specific codes).*

What would be *appropriate and reasonable* measures?

As stated above, section 19 states that responsible parties must take appropriate, reasonable, technical and organisational measures to secure the integrity and confidentiality of personal information.

Exactly *what* technical and organisational measures would be "appropriate" and "reasonable" will depend on the circumstances of the specific responsible party. In the end, it will amount to a risk-based approach: responsible parties will need to consider the *risks* involved in processing and the *nature* of the information to be protected as well as the cost of implementing such measures.

Ultimately, the security measures put in place will need to be appropriate for the nature of the personal information held versus the harm which may result from a security breach *(*the more sensitive the information, the higher the applied security must be*).

To use an example: an insurer (when issuing a disability policy) processing special personal information (such as information regarding policyholder's medical records) will need to have stricter security measures in place than a small call centre only processing cell phone numbers.

Suggested measures to safeguard personal information include:

- physical measures (**for example, securing filing cabinets and access control at offices)*;
- organisational measures (**for example, ensuring staff sign appropriate confidentiality undertakings and training staff on the importance of protecting personal information*);
- technological measures (**for example, implementing firewalls and anti-virus programmes, using passwords and encrypting removable devices used for taking personal information out of the office*);

and,

- the development of an information security policy for privacy which addresses all of the above.

Remember: responsible parties should be in a position to provide *evidence* of the reasonable steps taken to safeguard personal information.

Processing by operator – sections 20 and 21

You will recall we discussed operators in Part 1 (copy attached). If a responsible party outsources certain services which involve the processing of personal information to a third-party (i.e.: an " operator"), the responsible party remains liable for the protection of that personal information.

As such, section 21 sets specific requirements for the processing of personal information by operators. It requires the responsible party to enter into a written contract with the operator which ensures:

a. that the operator establishes and maintains the required confidentiality and security measures which apply to the responsible party (*as set out in section 19, which we discussed above*); and

- places a contractual obligation on the operator to inform the responsible party if there was unauthorised access or disclosure of personal information.

To use an example: where a retirement fund outsources its fund administration to an administrator it must (contractually) obligate the administrator to ensure a method of safeguarding that is consistent with the security measures implemented by the fund and that is compliant with the Act (as summarised above).

Section 20 then goes on to state that the operator must process personal information only with the knowledge or authorisation of the responsible party and treat personal information as confidential.

Notification of security compromises – section 22

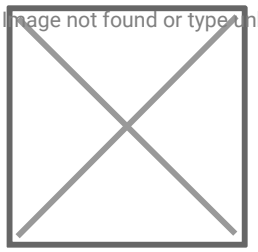
Where there are reasonable grounds to believe that personal information has been accessed by an unauthorised person, the responsible party must notify the Regulator and the data subject as soon as reasonably possible after the compromise (**PS: the responsible party may only delay notification of the data subject if it will impede a criminal investigation*).

Such notification must be in the time and manner prescribed in sections 22(4) and 22(5). (**PS: in terms of section 22(6) the Information Regulator may direct the responsible party to publicise the compromise.*)

Conclusion

We have now covered Condition 7, namely Security safeguards – in the next edition we will discuss the last condition, being Data subject participation (as referred to in sections 23 to 25).

Glacier Financial Solutions (Pty) Ltd and Sanlam Life Insurance Ltd are licensed financial services providers



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.