Article written by Ayanda Motlou, Candidate Attorney, checked and released by Chantelle Gladwin-Wood, Senior Partner at Schindlers Attorneys.

Introduction

We live in a digital age where almost all of our everyday activities are exercised through our devices. Technology has moved the needle forward in how we interact and go about our lives by widening the scope of our reach, and our influence, making the whole world accessible at the click of a button, or a “hey Siri” voice command. Making purchases, or payments, educating yourself, and communicating, amongst other things, have never been this easy.

However, having access to the worldwide web, unfortunately, results in the world wide web having access to us, and our personal and private information such as addresses, account numbers, and contact information. This makes us vulnerable to hackers and cybercriminals who are experts at manipulating our data to our personal and/or financial detriment. This threat ought to cause us to be hyper-vigilant about online security, and we ought to be taking precautionary measures to avoid falling victim to the above.

Be that as it may, circumstances exist where we cannot avoid handing over our personal data to secondary parties, whether it be to a service provider, or government entities such as the City of Johannesburg Municipality, for various personal/business transactional reasons. In such cases, the obligation rests on the entities to whom we entrust our personal information, to protect that personal information, and not to use it in a way that could be harmful or prejudicial to us. These secondary parties are a major source of cyber risk. Cybercriminals often target secondary-party providers to target their clients’ data and networks.

South Africa has the third-highest number of cybercrime victims from secondary source targeted attacks worldwide, losing approximately R2.2 billion a year to cyber-attacks.

The POPI Act protects your personal information in those unavoidable circumstances where same is handed over to secondary parties, setting the standard of cyber security for secondary parties, ensuring that your cyber personality is not compromised, ensuring accountability, and providing the necessary sanction in the event that it Is.

What is the POPI Act?

The Protection of Personal Information Act (“POPIA”) is legislation applicable nationwide, that safeguards consumers’ and employees’ personal information by making sure that companies responsibly manage the capture and storage of personal data to protect the sensitivity and integrity of that personal information. It also provides for accountability mechanisms, should the storage/safety/usage restrictions as set out in the Act be breached.
In terms of the Act, there are 8 conditions under which personal information may be lawfully collected and processed. These include:

• **Accountability**
The institution or entity referred to in the Act as the “responsible party” is legislatively required to ensure compliance with all the measures and conditions concerning the purpose and processing of information set out in the Act.
• **Processing Limitation**
The consent of the data subject is required for the processing of personal information, and personal information may not be processed unfairly.
• **Purpose Specific**
Personal information may only be processed for specified and legitimate reasons.
• **Further Processing Limitation**
Personal information may not be processed for a secondary purpose unless that processing is compatible with the original purpose.
• **Information Quality**
Reasonable steps must be taken by the responsible party to ensure that information the information collected is complete, accurate and is up to date.
• **Openness**
Data subjects must be made aware of the collection of their personal information, and the purposes thereof.
• **Security Safeguards**
The responsible party must safeguard personal information against risk of loss, unlawful access, interference, alteration, unauthorized destruction, and publication.
• **Data Participation**
Data subjects may request that their personal information be deleted or corrected.

Requirements of Section 19 of the POPI Act

Section 19 of POPIA introduces a comprehensive set of cybersecurity and data protection duties for entities that control person data. In terms of said section, entities are required to regularly review, verify, and update responses to identified risks by the taking of appropriate, reasonably technical and organisational measures. These institutions are required to always maintain sufficient security measures to ensure that the integrity and confidentiality of personal information held and/or processed by them is protected, and they must take reasonable steps to prevent the loss of damage to, or unauthorised access to, such personal information.

In giving effect to these requirements, POPI, at section 19, requires the responsible party to ensure the presence of suitable measures to:

1. Identify all reasonably foreseeable internal and external risks to personal information held by the entity;
2. Establish and maintain appropriate safeguards against the risks identified above;
3. Regularly review these measures to ensure that they are implemented effectively; and
4. Ensure that these safeguards are consistently reviewed and updated where necessary to keep up to date with the ever-evolving risks associated with the storage and processing of personal information.

The COJ's Cyber Data and/or Personal Information Breaches

The City of Johannesburg and/or its subsidiaries (City Power, Joburg Water, and Pikitup) have a history of data breaches occurring, all of which put the personal information of the City's consumers and service providers at risk. On or about 24 October 2019, the COJ shut down its systems due to a cyber attack, with hackers holding millions of South African's persona data and billing information at ransom. An almost identical cyber-attack against the COJ occurred a few months prior (*Jeff, O. 2019. City Of Johannesburg Announces Second Ransomware Attack In Recent Months*. https://www.cshub.com/attacks/articles/city-of-johannesburg-announces-second-ransomware-attack-in-recent-months).

On the 11th of March 2021, Joburg Water published a media statement to service providers, cautioning service providers against procurement scams via email and/or other forms of correspondence. The City was therefore aware of a potential data breach by scamsters in relation to the data that the City held of service providers, however, no such letter or media brief was published to warn the public of the potential phishing attacks or bogus emails that appear to be from the COJ in relation to its service providers. By not putting out a public warning, the City was arguably not alerting future service providers to the problem.

The Legal Responsibility of the COJ for Data Protection

Section 19 of POPIA binds information-based organisations such as banks, financial institutions, insurance companies, and municipalities to take reasonable cyber-security measures to protect their customers and service providers' personal information. In light of the City's obligations in terms of POPIA, it may then be found that, as a result of the most recent data breach incidents, the City has failed to comply with its responsibilities in law in terms of POPIA to protect the personal information of its customers and service providers. If this is indeed the case, it may be that any persons who have suffered a loss as a result of the City's failure to protect their personal information may be able to claim damages from the City for their losses.

Section 22 of POPI requires that a responsible party must notify certain parties as soon as reasonably possible, chiefly the Information Regulator, which is a body created by POPI to be specifically responsible for monitoring and enforcing compliance with the Act, and the affected individuals, once it suspects that personal information has been accessed or acquired by an unauthorised entity. It is not clear whether the City did this in relation to the 2021 attacks. Seeing that the City has been the subject of at least three reported cyber-attacks, affecting personal information, in the last three years, it is submitted that the Information Regulator should take an active interest in monitoring the City's compliance with its obligations in terms of POPIA when it comes to the protection of personal information of its customers and service providers.

The City might arguably be said to have failed in its obligations to take reasonable measures to protect the personal information of its customers and service providers, by virtue of the fact that it appears, from its website, to not have updated its privacy policy since 2014. This conduct might be found to be inconsistent with section 19(2)b of POPI, which requires that institutions take reasonable measures to ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Sanction for Criminal Offences with the POPI Act

Sections 100 to 106 of the POPI Act sets out the instances of conduct/failure to act that would be considered as noncompliance that would be criminal in nature and constitute an offence. These include the following:

• hindering or unlawfully influencing the Regulator;
• failing to comply with an enforcement notice;
• offences by witnesses, for example, lying under oath or failing to attend hearings;
• unlawful Acts by responsible party in connection with account numbers, and;
• unlawful Acts by third parties in connection with account number.

Sanctions applicable to the respective offences are set out in section 107 of the Act. For the more serious offences the maximum penalties are a R10 million fine or imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment.

For the less serious offences, for example, hindering an official in the execution of a search and seizure warrant the maximum penalty would be a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment. Failure to comply with the requirements of the POPI Act could have dire consequences.

Conclusion

The right to privacy set out in section 14 of the Constitution includes the right to protection of your personal data. The POPI Act gives effect to this right through legislatively binding procedures for the gathering and processing of information. It is therefore mandatory for entities, including state institutions such as municipalities, including the City of Johannesburg, to comply with the POPIA requirements, failing which, to face the necessary sanctions.

Any person who suffers loss/damage as a result of the City’s failure to protect their personal information may be able to claim damages from the City as a result of said failure. However, as always, each case is to be decided on its unique facts. Should you have experienced a loss/damage as a result of a municipality’s failure to protect your personal information, contact a reputable attorney or expert in the field for assistance.

References

https://www.cshub.com/attacks/articles/city-of-johannesburg-announces-second-ransomware-attack

Schindlers Attorneys

-in-recent-months#:~:text=On%20October%2024%2C%20the%20municipality,offline%20as%20a%20precautionary%20measure.&text=The%20city%20also%20launched%20a%2024%2Dhour%20investigation%20into%20the%20attack.

https://www.immuniweb.com/compliance/popia-compliance-privacy-cybersecurity/

https://johannesburgwater.co.za/service-providers-warned-of-procurement-scam/

https://www.joburg.org.za/Pages/Privacy-Policy.aspx

https://www.iol.co.za/technology/a-new-breeding-ground-for-hackers-1052791

https://www.timeslive.co.za/news/south-africa/2019-10-25-joburg-cyber-attack-cities-among-fastest-growing-targets-of-hackers/

https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia

Value

POPIA places a duty on Municipalities to protect the privacy and integrity of your personal information. Data breaches can cause a myriad of damages and losses for the victim. As such, should there be a leak of your personal data by the COJ, or any other municipality, you will be able to pursue reasonable compensation for the loss.