WERKSMANS
ATTORNEYS

REGULATORY

Not Today, April fool Protection of Personal Information – South Africa falling further and further behind

1 April 2020 *5 min read*

by Ahmore Burger-Smidt, Director and Head of Data Privacy Practice Group, Werksmans Attorneys and Dale Adams, Candidate Attorney

With everyone getting to grips with the lock-down and uncertainty as to the true impact of COVID-19 in South Africa, it is understandable that Government is considering all possible options to assist it in flattening the curve. Undoubtedly, a huge amount of personal information is informing this process.

Since time immemorial, South Africa has been playing catch up in respect implementing the data privacy laws it has developed. So much so that the United Nations special rapporteur on data and privacy protection Professor Joseph Cannataci has stated on 11 March 2020 at a roundtable discussion at the Human Sciences Research Council in Pretoria that –

"*Privacy laws started decades ago. By 2001 there were more than 20 countries that brought legislation up to certain levels. South Africa is about 30 years behind. The first data privacy laws were written in Sweden in 1973. Other European countries then followed shortly. South Africa, in 2020, is only now playing catch up.*"[1]

In an attempt to combat the novel COVID-19 pandemic, on 25 March 2020, the Minister of Communications, Telecommunications and Postal Services, Stella Ndabeni-Abrahams ("**the Minister**"), announced that cell phone data will be utilised to curb the spread of COVID-19. The Minister announced that cell phone companies have agreed to give the Government the location data of its subscribers to help fight against COVID-19. The location data, it seems, will be used to determine an approximate number of people an infected individual has been in contact with. The Minister did not provide further details nor Regulations on how this will be implemented.[2]

Last week it was also announced that various Governments across the world are planning to make use of location data to monitor the spread of COVID-19. Some Governments have indicated that they will work with mobile network providers and make use of anonymous (in POPIA terms de-identified) location data to create movement maps. In fact Governments such as China, South Korea, Hong Kong and Israel have gone much further and implemented active surveillance measures, including the use of personal data. In some instances certain Governments ensure that COVID-19 positive individuals reveal both their movements as well as contacts through an application.

But we need to ask ourselves why these intrusive actions are required. It is clear from statements by our own Government that it is imperative to understand at minimum –

- how the virus is spreading and identify risks to particularly vulnerable groups of people;
- identify emerging hot spots; and
- direct resources to those areas in greatest need.

Now imagine a world where personal information is protected in terms of data protection legislation and a world where the Protection of Personal Information Act, 2013 ("**POPIA**") has been fully enacted. What would have been the legal position in South Africa?

POPIA provides for the de-identification of personal information. In terms of POPIA, certain exclusions are provided for and the legislation clearly states that POPIA does not apply to personal information that has been de-identified. More importantly, POPIA provides that the legislation does not apply to the processing of personal information by or on behalf of a public body i.e. Government, if it involves, amongst others, processing for a purpose that involves national security or public safety.

Section 15(3)(d) of POPIA provides that personal information, for instance location data, held by mobile network operators, can be further processed where and if it is necessary to prevent or mitigate an imminent threat to the public health or public safety. Alternatively, in order to mitigate an imminent threat to the life or health of the data subject or other individual.

What then could be the concerns in relation to Government and mobile network operators processing location data for purposes of COVID-19?

There are certain fundamental principles that should be adhered to when processing personal information, even if processing of personal information is taking place amidst the COVID-19 pandemic.

It goes without saying that, without a single database to gather and analyse collected data, decision-makers will not be able to move as quickly as the required response demands; information gathered will be duplicated and outdated as real-time updates will not take place seamlessly, leading to inaccurate information and situational analysis.

But who will be and remain in control of the information and records? Also, once the COVID-19 crisis has dissipated, will the personal information be destroyed, aggregated or de-identified?

Generalised location data trend analysis will definitely help to understand and plan around the COVID-19 crisis. Where this data is properly de-identified and aggregated, it does not fall under data protection law because no individual is identified. But still the necessary safeguards should be in place which provide for strict controls that meet the requirements of data protection legislation and ensure that the personal data of individuals cannot be re-identified.

POPIA principles, if followed, would mean that personal information collected will only be used for COVID-19 and not for any other purpose and only relevant information will be collected all this while taking all reasonable steps to ensure that personal information is kept secure.

What will happen without POPIA during and after COVID-19?

We awaited the full enactment of POPIA on 1 April 2020. It did not happen.

The question then is, when?

Can the person with an answer please lift his hand?

---

[1] L Kiewit "South Africa must implement privacy laws to protect citizens, says UN expert" available at https://mg.co.za/article/2020-03-12-south-africa-must-implement-privacy-laws-to-protect-citizens-says-un-expert/, accessed on 1 April 2020.

[2] P de Wet "South Africa will be tracking cell phones to fight the COVID-19 virus" available at "https://www.businessinsider.co.za/south-africa-will-be-tracking-cellphones-to-fight-covid-19-2020-3, accessed on 1 April 2020.



Ahmore Burger-Smidt

Head of Regulatory

View Profile