

Solutions thick and fast but as of 1 July 2020, innovation must incorporate POPIA conditions

1 July 2020 5 min read

By Ahmore Burger-Smidt, Director, Head of the [Data Privacy Practice Group](#)

"The recently reported cyber attack on a healthcare institution in South Africa highlights yet again the harsh reality that cyber criminals across the globe are continually on the lookout for ways to exploit the COVID-19 pandemic for their own gain."^[1] Eugene Kaspersky, CEO of Kaspersky

It is time to focus on the what, where, how and why. POPIA will inform how every entity deals with personal information going forward. A clear understanding of the impact of POPIA on both the private and public sectors is non-negotiable.

Recently, the World Economic Forum has warned that as the COVID-19 crisis accelerates, so do cyber risks. It stated that the constant flow of information in relation to COVID-19 has multiplied opportunities for cyber criminals to deliver malware, ransomware and phishing scams. This already links to the security of data and POPIA obligations in relation to security safeguards.

In the healthcare sector, globally, there has been a spike in cyber-attacks targeting medical organisations at the forefront of the response to COVID-19.

Human Rights Watch has urged governments to respect privacy and human rights when using digital technologies to contain COVID-19. At a minimum, it has been recommended that technology-assisted measures should^[2]:

- *Be lawful, necessary, proportionate, transparent, and justified by legitimate public health objectives.*
- *Be time-bound and only continue for as long as necessary to address the pandemic*
- *Be limited in scope and purpose, used only for the purposes of responding to the pandemic*
- *Ensure sufficient security of any personal data that is collected*
- *Mitigate any risk of enabling discrimination or other rights abuses against marginalized populations*
- *Be transparent about any data-sharing agreements with other public or private sector entities*
- *Incorporate protections and safeguards against abusive surveillance and give people access to effective remedies*
- *Provide for free active, and meaningful participation of relevant stakeholders in data collection efforts*

A COVID-19 Tracing Database was introduced on 02 April 2020 in South Africa. The Tracing Database provides that information in the database is confidential and may only be used for the contact tracing purpose, and there are penalties for disclosure. It also provides that if information obtained from mobile network operators is not relevant to the database purpose, the National Department of Health may not retain that information for longer than a period of 6 weeks. Also, the information must be de-identified within 6 weeks of the termination of the national State of Disaster and retained thereafter only for research teaching and study purposes^[3] Furthermore, a number of innovative solutions are being put forward by business.

Mobile location tracking undoubtedly introduces privacy risks. Location tracking information can contain sensitive and revealing insights about a person's identity, location, behaviour, associations, and activities. The use of mobile phone network data creates granular, real-time targeting opportunities. This in itself involves an invasion of every citizen's right to privacy.

Minister of Higher Education and Training, Blade Nzimande, announced on 09 June 2020 that his department will use HealthCheck, a purpose-built coronavirus daily screening and monitoring tool, to allow students to return to campus safely.

"HealthCheck is secured to use by students and staff entering our campuses daily to self-check their body temperature and will link such data to the tracking system of the Department of Health.

"All students and staff – approximately two million people – will be required to register for HealthCheck and use it every day to assess their own level of risk Nzimande said that if the risk is low, the individual will receive clearance valid for 24 hours."^[4]

Minister of Higher Education and Training,

Blade Nzimande

Minister Nzimande indicated that the tool will allow for early detection, mapping and management of Covid-19 cases within the country's Higher Education institutions and feeds into the Department of Health's tracking and tracing system.

But what does all of this actually mean from a POPIA perspective? At minimum Government and those entities putting forward innovative solutions should –

- keep collected information to the minimum;
- consider that some information only needs to be held momentarily and there is no need to create a record for a prolonged period of time;
- tell individuals how and why their personal information will be used, including implications for them;
- ensure information security; and
- establish avenues for individuals to be able to exercise their information rights.

At minimum it is time to understand what lawful processing of personal information means in terms of POPIA. Equally important, it is time to focus on data security and obligations set out in POPIA.

[1] "Security gurus weigh in on SA's latest cyber attacks" (Samuel Mungadze, ITWeb 12 June 2020) <<https://www.itweb.co.za/content/WnpNgM2KPz5qVrGd>>

[2] "Mobile Location Data and Covid-19: Q&A" (Human Rights Watch (hrw.org/news 03 May 2020) <<https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>>

[3] Department of Co-operative Governance and Traditional Affairs Disaster Management Act, 2002: Amendment of regulations issued in terms of section 27(2) Government Gazette No. 43199, 2 April 2020, (Published under Government Notice No. R. 446) https://www.gov.za/sites/default/files/gcis_document/202004/43199rg11078-gon446.pdf (accessed 29 May 2020)

[4] "All South African students and university staff will have to register to be screened and cleared for Covid-19 every day" (Businesstech 09 June 2020 Businesstech) <https://businesstech.co.za/news/technology/406255/all-south-african-students-and-university-staff-will-have-to-register-to-be-screened-and-cleared-for-covid-19-every-day/>



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)