

Time to focus: POPIA following on the heels of the coronavirus

20 March 2020 5 min read

by Ahmore Burger-Smidt, Director and head of Data Privacy

Without a process to monitor, understand and prevent the spread of COVID-19 by all stakeholders, the global challenge we are confronted with will not be manageable.

At the same time, on 1 April 2020, POPIA will be fully enacted and we are reminded that POPIA and privacy laws, internationally, will inform actions undertaken by Governments and all stakeholders, including companies, alike.

Many of the actions undertaken to understand and prevent the spread of COVID-19 will involve the processing, as well as further processing, of personal information (such as name, address, workplace, travel details) of individuals, including in many cases sensitive, 'special personal information' (such as data relating to health).

POPIA provides that the processing of special personal information is prohibited, but also provides that the processing of special personal information without consent is lawful where it is necessary for compliance with a legal obligation or an obligation in terms of international public law. Furthermore, if it is for amongst others, statistical or research purposes, to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned, consent from an individual is not required.

Many questions by companies during this uncertain time, relate to what can and cannot be done, taking into consideration privacy laws –

- We are already seeing that more staff are working from home. POPIA does not prescribe or restrict working environments. Working from home does however require that personal information should still be protected. Therefore, companies will have to consider what security measures are required for home working and whether these measures are sufficiently robust to protect, not only confidential information, but mitigate against a possible data breach.
- As the number of infections is on the rise, unfortunately that might mean that a staff member could be diagnosed with COVID-19. Companies have an obligation to ensure the health and safety of employees and a duty of care towards employees. POPIA does not prevent an organisation from disclosing that an employee has been diagnosed with COVID-19. What is a far more complicated issue to consider is whether companies can disclose the identity of the individual. This means that companies will have to consider whether there is a need to name a specific individual and if so, should not provide more information than is absolutely necessary.
- Companies should also act in a prudent manner in that if they need to collect specific health data, they do not collect more than necessary and ensure that any information collected is treated with the appropriate safeguards in place to keep the information confidential. Safeguards relate to limitation on access to the personal information, strict time limits for erasure, and other measures such as adequate staff training to protect the privacy rights of individuals.
- Insofar as companies collect health information, for example body temperature at the entrance to buildings in order to prevent contamination, the processing of this information must be, in terms of content and duration, limited to the bare necessity to achieve this purpose.
- Most importantly, companies might have to share information with authorities about specific individuals in relation to COVID-19. Where this is required by Government, it would be deemed to be in the public interest for statistical purposes as well as to prevent the spread of the virus. POPIA does not provide for the wide exclusions on the level provided for in terms of the General Data Protection Regulation to disclose personal information in the current circumstances. However, it is suggested that privacy legislation should not prevent a company from co-operating with Government to mitigate the risk of the virus spreading in the country.

In short –

- Personal information relating to health must be considered as sensitive and cannot in principle be obtained and dealt with, without consent.
- The processing of health-related personal information must be necessary and appropriate in order to prevent new infections and must not go beyond what is absolutely necessary to achieve this objective.

It is inevitable that the processing of special categories of personal information without consent may be necessary for public health reasons. However, such processing should not result in the personal information being processed for other purposes by third parties, such as employers or insurance companies.

The same applies to personal data processed by companies as part of operational and organisational measures aimed at preventing contamination. At the least when the threat of the current coronavirus pandemic has ceased to exist, the personal health information must be completely deleted.

It is clear that companies might need to share information quickly or adapt the way they work. Privacy legislation and POPIA in particular will not stop companies from doing that. It is all about being proportionate – if something feels excessive, then it probably is. If the process feels as if it could result in a data breach, then it probably can. If it feels that personal health information is being processed for any other purpose than to prevent and manage the coronavirus from spreading, it probably is.

We live in uncertain times. At least be certain when processing personal health information in terms of POPIA post 1 April 2020.

Written by

Ahmore Burger-Smidt

Director, Head of the Data Privacy Practice Group

[Download PDF](#)