THE
NATIONAL LAW REVIEW

South Africa's Protection of Personal Information Act, 2013, Goes into Effect July 1

HUNTON
ANDREWS KURTH
Article By
Hunton Andrews Kurth's Privacy and Cybersecurity
Hunton Andrews Kurth
Privacy and Information Security Law Blog-Hunton Andrews Kurth

- Communications, Media & Internet
- Consumer Protection
- Election Law / Legislative News

- South Africa

Monday, June 29, 2020

Zeyn Bhyat of ENSafrica reports that on June 22, 2020, it was announced that South Africa's comprehensive privacy law known as the Protection of Personal Information Act, 2013 (the "POPIA") will become effective on July 1, 2020. POPIA acts as the more detailed framework legislation supporting South Africa's constitutional right to privacy.

POPIA has been a work-in-progress since it was earmarked for implementation by the South African Law Reform Commission in 2005. The delay in its enactment was attributable, in part, to the publication of the draft EU General Data Protection Regulation ("GDPR") in 2013, as the POPIA drafting committee paused to consider some of the proposed innovations in the GDPR and also to take steps to ensure that the South African privacy regulator (i.e., the Information Regulator ("SAIR")) was given an opportunity to develop operational capabilities. In this respect, POPIA came into force over a period of time, with the initial provisions enabling, among other things, the establishment of the SAIR coming into effect on April 11, 2014. To date, the SAIR has taken steps to become fully operational, by, e.g., procuring the publication of regulations, establishing codes of conduct and raising public awareness.

The POPIA provides for a general information protection mechanism applicable to

organizations in both the public and private sectors. Similar to the EU Data Protection Directive 95/46/EC, POPIA establishes eight conditions for lawful processing of data. These conditions are: (1) accountability, (2) processing limitation, (3) purpose specification, (4) further processing limitation, (5) information quality, (6) openness, (7) security safeguards, and (8) data subject participation.

The POPIA applies to the processing of personal information entered in a record by a responsible party who processes the information in South Africa and is domiciled in South Africa, or is domiciled elsewhere but uses automated or non-automated means in South Africa to process the personal information. The POPIA generally applies to "responsible parties" (i.e., the principal processors of personal data, who determine the purpose and means of processing), and limited obligations also extend to "operators" (i.e., data processors).

The POPIA contains an open-ended definition of "personal information," which generally means information relating to an identifiable, living natural person and, where applicable, an identifiable company or other similar legal entity. The definition includes information relating to partnerships and unincorporated persons, and provides a significantly detailed list of examples of personal information. These examples range from private correspondence and information about age, gender, sex and race to identifiers such as identity numbers, telephone numbers, location information, online identifiers, and personal opinions and preferences.

Under the POPIA, a responsible party processing personal information must comply with all eight conditions and the measures necessary to give effect to those conditions. Compliance must be achieved not only when the actual processing of information takes place, but also when determining the purpose and means of processing the personal information.

1. ***Accountability:*** This condition requires that all processing of data occurs in compliance with POPIA. Practically, this requires that a data protection policy is established and that an internal information officer champions the aims of and compliance with the legislation.
2. ***Processing limitation:*** Personal data must be processed lawfully and in a reasonable manner that does not infringe on a data subject's privacy. A responsible party must develop procedures and policies to ensure that personal information is processed in a "reasonable manner."
3. ***Purpose specification:*** Among other things, this entails that personal information may only be collected for a lawful, specific and explicitly defined purpose related to the function or activity of the responsible party collecting the information. Data subjects must be informed of the purpose of the collection, except in exceptional circumstances, such as when the responsible party is required to comply with an obligation imposed by law.
4. ***Further processing limitation:*** Once personal information has been collected and lawful processing has occurred, a responsible party may only further process that data in limited circumstances. These limited circumstances are determined based on whether the purpose of the further processing is "compatible" with the previously defined purpose.
5. ***Information quality:*** A responsible party must ensure that any personal

information in its possession is complete, accurate, not misleading and updated when necessary. In maintaining information quality, the responsible party must consider the purpose for which the personal information is collected or further processed.

6. ***Openness:*** A responsible party must compile a manual that contains stipulated information as required by the South African Promotion of Access to Information Act, 2000, including details on the information that it holds. When personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of: (1) the information being collected and the source of the information; (2) the name and address of the responsible party; (3) the purpose for which the information is being collected; (4) whether the data subject is required to provide the requested information, or may do so voluntarily; (5) the consequences of failing to provide the information; (6) the legal basis for the collection of the information; (7) whether the responsible party intends to transfer the information to a third country and the level of protection afforded to the transferred information; and (8) any further information necessary for the processing to be reasonable under the circumstances.
7. ***Security safeguards:*** A responsible party must secure the integrity and confidentiality of any personal information in its possession or under its control by taking appropriate and reasonable technical and organizational measures to prevent loss, damage, unauthorized destruction of, and unlawful access to the personal information in its possession.
8. ***Data subject participation:***
    1. The data subject has the right to request confirmation of whether a responsible party holds personal information about the data subject. The data subject also has the right to request a record or description of the personal information about the data subject being held by the responsible party, as well as information concerning the identity of all third parties who have had access to the data subject's personal information.
    2. The data subject may request that a responsible party:
        1. correct or delete personal information about the data subject that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained; and
        2. delete or destroy personal information that the responsible party is no longer authorized to retain.

POPIA is not intended to prevent the processing of personal information but to ensure that it is done fairly and without adversely affecting the rights of data subjects. Given the wide-ranging impact of the POPIA, it is expressly provided that all processing of personal information must conform with the POPIA's provisions within one year after its commencement – a 12-month grace period beginning July 1, 2020.

National Law Review, Volume X, Number 181

personal-information-act-2013-goes-effect-july-1