
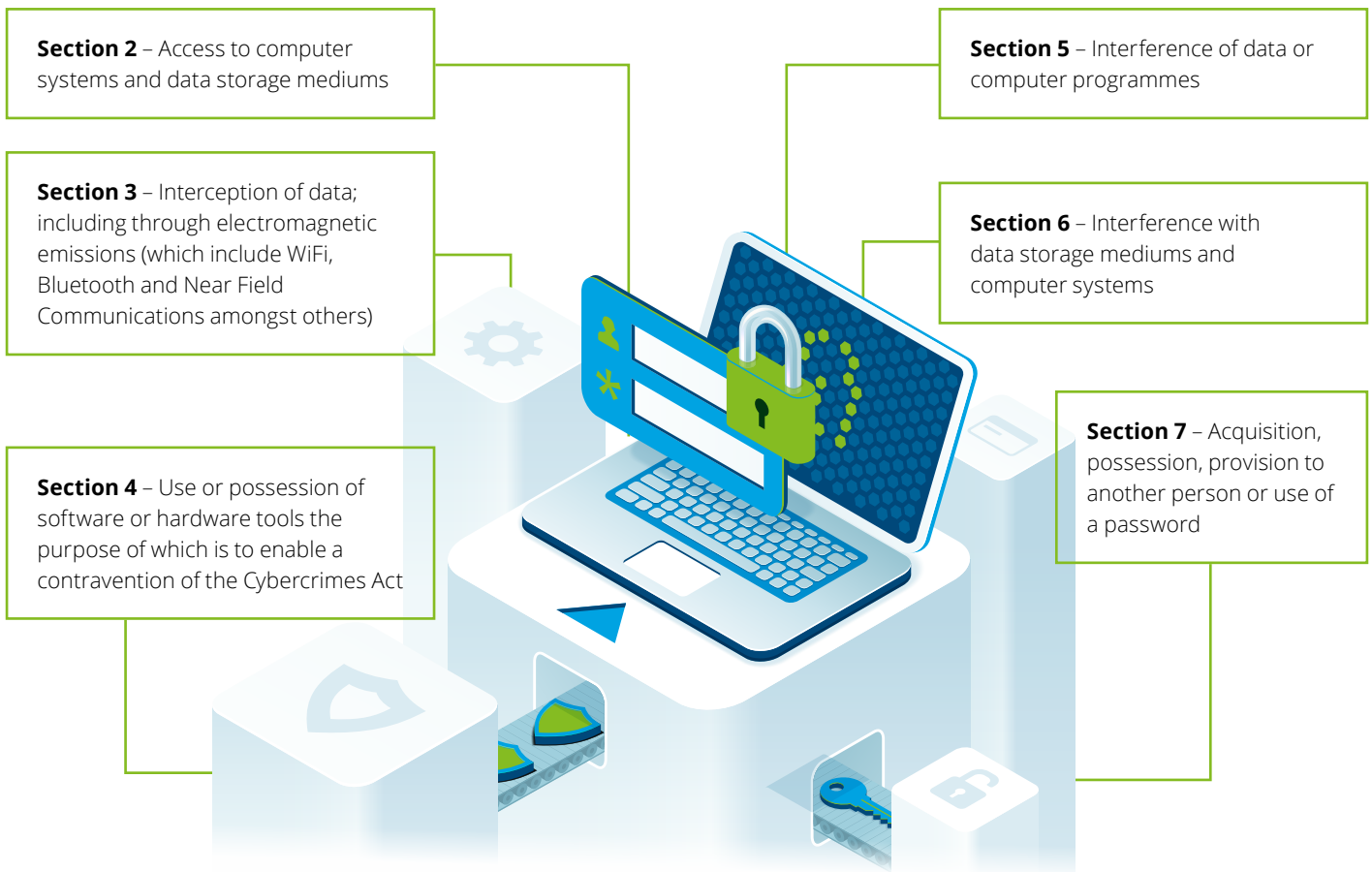


A Privacy Perspective on the Cybercrimes Act, 2020 – Aspects to consider in your Privacy Programme

In keeping with the significant developments over the last 12 months in respect of data privacy legislation, the President signed the Cybercrimes Act, 2020 into law on 2 June 2021.

The actual commencement date is yet to be proclaimed by the President, and will appear in the Government Gazette sometime in the future. As many South African organisations are in the process of maturing their privacy programmes in anticipation of the Protection of Personal Information Act's (POPIA) imminent commencement date on 1 July 2021, it is important to identify key principles from the Cybercrimes Act to consider in your privacy programme, as in certain instances, POPIA has been incorporated into the Cybercrimes Act. 

From a Cybercrimes perspective, organisations should consider adopting policies, processes, procedures and technical controls to prevent the unlawful and intentional activities:



From a POPIA perspective, for the purposes of section 2, 3 and 7 above, the Cybercrimes Act provides that failures by organisations to comply with Chapter 3 of POPIA (8 principles), section 72 (Transfer of Personal Information outside the Republic) and any applicable codes of conduct, will be dealt with in terms of the Enforcement provisions of POPIA, that is, Chapter 10. Thus, the substantive provisions detailing the requirements to bring about compliance therewith, have been prescribed in POPIA.

From a cyber security perspective, section 19(1) (principle 7) of POPIA requires that an organisation secure the integrity and confidentiality of personal information in its possession or under its control by deploying appropriate, reasonable technical and organisational measure to prevent –

- Loss of, damage to or unauthorised destruction of personal information; and
- Unlawful access to or processing of personal information.

Section 19(3) requires organisations to have due regard to generally accepted security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules.

Importantly then, the Cybercrimes Act requires an organisation to adopt POPIA as its baseline cyber security standard, and as a result, such standards must be implemented, monitored and maintained in a manner that can withstand legal and compliance scrutiny required in terms of POPIA.

As a result, certain aspects of the Cybercrimes Act being enforceable in terms of POPIA, the ability to demonstrate and evidence a compliant cyber security posture that is adequate and effective on a continuous basis is essential; especially in the context of the Information Regulator's ability to conduct an Assessment of its own accord, or at the behest of a responsible party or data subject in terms of section 89 of Chapter 10 of POPIA.





Thus, an evaluation of an organisation's cyber security posture in this specific regard would amongst others, include the assessment, configuration or implementation of the following policies, processes, procedures and technical controls to address the requirements of the Cybercrimes Act in the context of POPIA:

- Identity and access management
- Data access governance
- Secure data management
- Data encryption and certificate management
- Master data management
- Database security and governance
- Logging and monitoring
- Wireless access management
- Password policy management and end user training and awareness
- Privilege access management

It is important to consider the Cybercrimes Act's requirements as part of the larger privacy programme as soon as possible, as post compliance considerations will have a significant impact on cost, resourcing, technical solutions and information security architectures; all of which will have a time-to-compliance impact.

Lastly, section 54 of the Cybercrimes Act requires that electronic communications service providers or financial institutions that become aware that any electronic service or communications network involved in the commission of any category or class of offence in section 2 – 7 must:

- without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and
- preserve any information which may be of assistance to the South African Police Service in investigating the offence.

An electronic communications service provider or financial institution that fails to comply with the reporting requirements is guilty of an offence, and is liable on conviction to a fine not exceeding R50 000.

The requirements of section 54 should be embedded into privacy and cyber incidence responses moving forward in terms of section 21 and 22 of POPIA, notwithstanding that the Cybercrimes Act has not become effective, to ensure:

- that organisations adopt the correct behavioural response to offences;

- the preservation of critical evidence to assist law enforcement capture perpetrators; and
- to prevent future offences.

Should you require any further information on any of these aspects, please do not hesitate to contact us.

Contact:

Leishen Pillay
Director

Cyber Risk | Risk Advisory Africa

Tel: +27 (0)11 209 6418

Email: lpillay@deloitte.co.za

