Global Data and Cyber Handbook - South Africa

Key Data & Cybersecurity Laws

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# How are data and cybersecurity laws/regulations implemented?

Last review date: 31 December 2024

☒ omnibus – all personal data

☒ sector-specific — e.g., financial institutions, governmental bodies

Electronic Communications and Transactions Act, 1998

Consumer Protection Act, 2008

Labour Relations Act, 1995

Employment Equity Act, 1998

Basic Conditions of Employment Act, 1997

National Health Act, 2003

☒ constitutional

# What are the key data privacy laws and regulations?

*Last review date: 31 December 2024*

The Protection of [Personal Information Act, 2013](http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf) ("**POPIA"**) was signed into law in 2013 and only came into force on  1 July 2021.

POPIA promotes the protection of personal information processed by public and private bodies, introduces minimum requirements for the processing of personal information, outlines the rights of data subjects, regulates the cross-border flow of personal information, introduces mandatory obligations to report and notify data breach incidents, and imposes statutory penalties for violations of the law.

POPIA sets out the essential parameters for the lawful processing of personal information, including:

eight "core-information-protection principles";

a number of substantive issues concerning, inter alia, the processing, collection and transfer of personal information, including that:

personal information may only be processed in a fair and lawful manner;

personal information be processed for specific, explicitly defined and legitimate reasons;

the steps required to make affected data subjects aware of the processing and the purposes of the processing of personal information;

personal information may only be kept for as long as it is required to fulfil the purpose for which it was collected; and

personal information may only be transferred cross-border subject to certain requirements

responsible parties (i.e. data controllers) being required to:

appoint an Information Officer and Deputy Information Officer to ensure compliance with the lawful processing conditions set out in POPIA and deal with data subject rights requests in terms of POPIA and the Promotion of Access to Information Act. 2000 ("**PAIA**") as well as complaints from data subjects who seek to enforce POPIA;

develop, implement, monitor and maintain a data protection and privacy compliance framework;

undertake a personal information impact assessment;

assist with and respond to data subject requests made in terms of POPIA and access to information requests made by requesters in terms of PAIA;

maintain documentation of all processing;

encourage and ensure compliance with PAIA:

develop, monitor and maintain a manual in terms of sections 14 (public bodies) and 51 (private bodies) in terms of PAIA;

evaluate and approve requests for access to information received regarding the grounds set out in PAIA within the time constraint or any extended period;

respond to data subject requests and requests made by the Information Regulator pursuant to POPIA;

conduct internal training sessions on the requirements of POPIA;

work with the Information Regulator in relation to any investigations undertaken by the Information Regulator in respect of the responsible party; and

secure the integrity and confidentiality of personal information in its possession or under its control and ensure that it is appropriately safeguarded against loss, destruction or unlawful access;

exemptions from the information protection principles;

the rights of data subjects regarding unsolicited electronic communications and automated decision making;

the establishment of the Information Regulator to exercise certain powers and to perform certain duties and functions in terms of POPIA and PAIA; and

enforcement mechanisms.

# What are the key cybersecurity laws and regulations?

*Last review date: 31 December 2024*

The Cybercrimes Act 19 of 2020 ("**Cybercrimes Act**") was signed into law in June 2021 and came into force on 1 December 2021. It brings the country's cybersecurity legislation in line with global standards. The Cybercrimes Act compels electronic communications service providers and financial institutions to act when they become aware that their computer systems have been involved in a cybersecurity breach and which constitutes an offence under the Cybercrimes Act and to report such breaches to the South African Police Service within 72 hours of becoming aware of the breach, and preserve any information, which may be of assistance in the investigation. Non-compliance with this provision is a criminal offence and monetary fines can be imposed. The Cybercrimes Act further criminalizes harmful data messages, such as those that invite or threaten violence or damage to property, as well as those that contain intimate images. Data is broadly defined in the Cybercrimes Act as "electronic representations of information in any form." The Cybercrimes Act also criminalizes cyber fraud, extortion, forgery and the theft of incorporeal property. Also listed as an offence is the unlawful accessing of a computer system, data storage medium or personal data. Those found guilty of a cybersecurity offence face hefty fines and lengthy prison sentences of up to 15 years.

# What are the key laws and regulations relating to non-personal data?

Final National Data and Cloud Policy dated 31 May 2024 (**Policy**) issued by the Minister of Communications and Digital Technologies (**Minister**).

The Policy prioritises an acceleration of the rollout of digital infrastructure (to ensure fast, secure, and reliable broadband connectivity), data privacy and security, open data and data interoperability, and the adoption of a cloud-first approach (requiring collaboration, funding, stakeholder engagement, and the capacitation of the State Information Technology Agency (**SITA**)). The Policy outlines several initiatives aimed at addressing specific issues related to data and cloud computing technologies, namely:

**Digital infrastructure and access to data and cloud services:** The Policy prioritises the capturing of all government data in digital format and the migration of all government IT services to the cloud, while also ensuring interoperability between various government departments and enhancing digital services for citizens. In attaining this objective, the Policy advocates for a decentralised approach and the State’s co-operation with the private sector. The Minimum Information Security Standards, 1996 are to be updated and used as the guiding framework for access to Government data in unified Government data centres, while open data and data for development frameworks aimed at enabling access to timely, accurate, complete, consistent, and valid Government data are to be developed.

**Data sovereignty, data localisation and cross-border transfers:** Whereas previous iterations of the Policy had recommended that: (i) all data identified as critical information infrastructure must be processed and stored only within South Africa; (ii) any cross-border transfers must be subject to localisation requirements (including requiring that copies of any data transferred outside of South Africa must also be stored in South Africa for law enforcement purposes); and (iii) all data generated in South Africa was to be considered to be the property of South Africa, irrespective of the location of the technology company, the Policy has been amended to provide that only Government data that incorporates ‘content pertaining to the protection and preservation of national security and sovereignty’ of South Africa must be stored in digital infrastructure within South Africa’s borders.

**Creating a digital trust environment:** To address growing cybersecurity concerns, the Minister is required to ensure the capacitation of South Africa’s cybersecurity hub and to prioritise the signing and ratification of regional, continental, and global treaties dealing with the prosecution of cybercrimes. To deal with cybersecurity threats, all digital technologies used by Government must incorporate cybersecurity-by-design principles.

**Data Centres:** The Policy imposes several obligations on data centres, including compliance with environmental obligations.

**Competition Concerns:** The Policy details certain required policy interventions relating to competition in the data and cloud market. One such intervention being the need for the Competition Commission to conduct studies into the data and cloud services markets to identify anti-competitive trends and behaviours.

# Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date:  31 December 2024*

In September 2021, the Information Regulator requested that public comments be submitted on the Amendment of the Regulations Relating to the Protection of Personal Information, 2018 ("**Draft Regulations**"). The Draft Regulations outline the procedure to be followed in certain circumstances contemplated in POPIA, including:

Guidance for data subjects on how to object to the processing of their personal information.

Guidance on how data subjects can request the correction, destruction or deletion of their personal information.

Guidance on how responsible parties can request a person's consent to process their personal information for unsolicited electronic direct marketing.

How data subjects can go about submitting a complaint to the Information Regulator.

**Cyberattack obligations:** There are obligations provided for in the Cybercrimes Act on electronic communications service providers and financial institutions relating to cybercrimes, however these obligations are not yet in force.

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.