



NCPT

NORTHERN CAPE PROVINCIAL TREASURY

LEGAL SERVICES AND LABOUR RELATIONS

2022/2023

LEGAL NOTE 1

THE RELATIONSHIP BETWEEN POPIA ACT AND CYBERCRIMES ACT



We serve with passion. We deliver on time.



NCPT

NORTHERN CAPE PROVINCIAL TREASURY

INTRODUCTION

The use of technology, internet, computers and mobile programmes is fast growing in many parts of the world, and this has in turn come with risks and challenges associated with criminal activity on the cyberspace. In an attempt to prevent cyberbullying and the unauthorized sharing or retrieving of personal information of an individual, South Africa introduced the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013(POPIA).

The Cybercrimes Act seeks to provide for actions that will be considered as offences in the cyberspace, and the Protection of Personal Information Act on the other hand deals with data privacy. POPIA places obligations on institutions that collect, process and store personal information of data subjects to comply and adhere to 8 conditions for lawful data processing being accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.

DIFFERENCES OF PROTECTION OF PERSONAL INFORMATION ACT AND CYBERCRIMES ACT AND PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

The purpose of this Act is to give effect to section 14 of the constitutional right to privacy, by safeguarding personal information when processed by a responsible party. The regulation of the collection, use, and processing of personal information through legislation is an internationally accepted practice.

The Act applies to everyone who keeps any type of record relating to someone's personal information. It governs how personal information is "processed" through collecting, receiving, recording, organizing, retrieving, or using personal information; or disseminating, distributing, or making such personal information available (processed).

It also applies to each record already in possession of the responsible party, excluding information processing of personal or household activities, of which the processing authority is a public institution concerned with national security, defence, public safety, anti-money laundering, or the Cabinet or Executive Council of a province or even a judicial function. Information can only be processed with the consent granted by the data subject, for conclusion or performance purposes of a contract to which the data subject is a party, where it safeguards the legitimate interests of the party, or when required by law.



NCPT

NORTHERN CAPE PROVINCIAL TREASURY

The responsible party is required to ensure the integrity and confidentiality of personal information by implementing appropriate, reasonable technological and organizational systems to prevent loss of personal information, damage, or unauthorized destruction, as well as unlawful access to or processing of personal data.

POPIA places obligations on institutions that collect, process and store personal information of data subjects to comply and adhere to 8 conditions for lawful data processing being accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.

CYBERCRIMES ACT

Cybercrime is defined as *an unlawful interception of data, unlawful acquisition, possession, provision, reception or use of password, access of codes or similar data or devices, cyber fraud and cyber extortion.*

The Act aims to create an integrated cybersecurity legislative framework to effectively combat cybercrime and address cybersecurity issues by bringing a reprimand to some cyber actions which, *inter alia*, are recognized and considered as cybercrimes, viz, Cyber fraud, Forgery, Extortion, Ransomware, Hacking, Unlawful interception of data, Unlawful acquisition, possession or receipt of passwords and access code.

This Act intends to create offences, which have a bearing on cybercrime; to criminalise the disclosure of data messages that are harmful including messages that contains intimate images and provide for interim protection orders.

The Act further regulates the powers to investigate cybercrimes by providing an overarching legal authority on how these offences must be investigated; the process that amongst others include searching and acquiring access to, or seizing information pertinent to cybercrimes.

Section 3 of this Act makes provision for offences relating to personal information as defined in the [POPIA Act](#) including the abuse, misuse and the possession of personal information of another person or entity where there is a reasonable suspicion that it was used, or may be used, to commit a cybercrime.

Section 54 of the Cybercrime Act, imposes an obligation on Electronic Communications Service Providers ("ECSPs") and Financial Institutions, such as banks, to report cyber offences within 72 hours of becoming aware of them to the South African Police Services (SAPS). They must preserve any information that may be of assistance in the investigation and they are required to work with law enforcement, where applicable, in the investigation of



NCPT

NORTHERN CAPE PROVINCIAL TREASURY

cybercrimes. In certain instances, this may involve the handing over of data and hardware. ECSPs and Financial Institutions must report cyber offences without undue delay and within 72 hours of becoming aware of them, failing which, they may be liable to a fine of up to R50 000.

THE CONNECTION

The POPIA Act and the Cybercrimes Act are two pieces of legislation aimed at protecting data subjects from data breaches. Both pieces of legislation confer power to the South African Police Services to investigate, search and access or seize any article used in the commission of an offence, and create mechanisms for mutual assistance between foreign states in cross border investigations.

In collaboration, the Cybercrime Act and POPIA broaden the South African legislative framework relating to data protection and privacy, to bring South Africa in line with international guidelines. They establish minimum requirements for the processing and protection of personal information thereby promoting the right to privacy enshrined in section 14 of the Constitution.

Although these two Acts (POPIA and Cybercrimes Act) are closely related, challenges may be found when these need to be implemented in a situation of urgency side by side, so as not to impede privacy, while pursuing security or vice versa. Rights to privacy, dignity and freedom of the person may clash against the Cybercrimes Act investigative procedures.

However, as per the Cybercrimes Act, failure by responsible parties to adhere to the 8 conditions in POPIA will be dealt with enforcement procedures of POPIA. In this way, the Cybercrimes Act and the POPIA work in tandem to achieve security within the perspectives of privacy.

The objectives of POPIA and the Cybercrimes Act are intertwined and mutually beneficial, because privacy is only possible if cyberspace is secure.