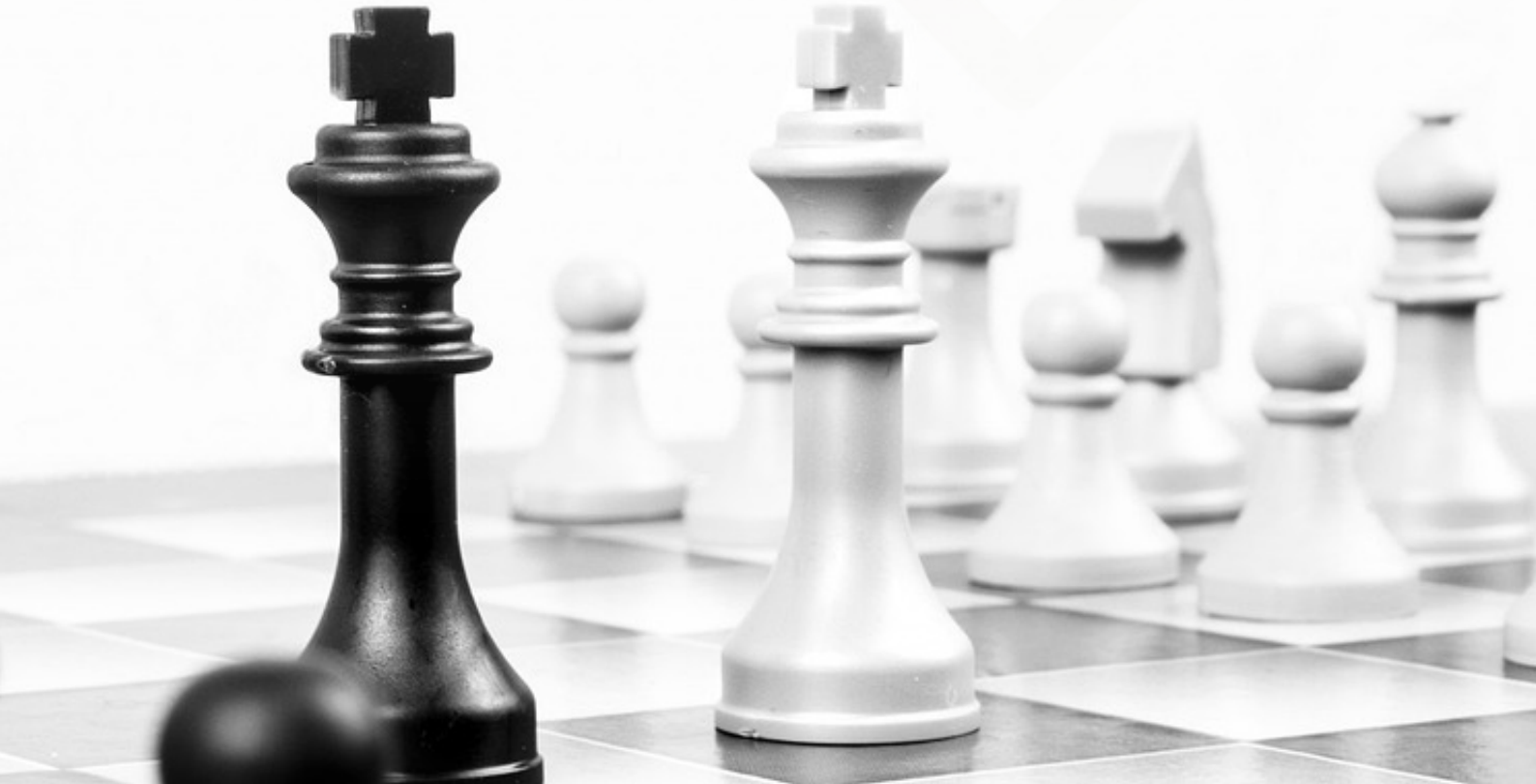
DATA PRIVACY VS. FINANCIAL SECURITY:

"THE BATTLE BETWEEN POPIA AND FICA"

RMG
MORE THAN A DECADE OF SERVICE EXCELLENCE

November 2023
22nd Edition



INTRODUCTION

Financial fraud is a major problem that causes substantial damage each year, wiping away billions. However, there is some hope for individuals as privacy laws such as POPIA have been established to protect personal data from misuse. Additionally, FICA reporting requirements have been put in place to prevent the flow of illicit finance. Amid the conflict between individual rights and public security, it remains to be seen if these two pillars can withstand the ongoing onslaught

This article is a lifeline, revealing how POPIA and FICA work in harmony despite their differing approaches.

POPIA establishes a robust framework for managing personal information in South Africa, a unique law in its own right.

The Protection of Personal Information Act, fondly known as POPIA, was crafted to counteract the growing scourge of data theft and misuse.

POPIA delves into the nitty-gritty, distinguishing between personal and special personal information. Personal information encompasses everything from names and contact details to religion and financial data, setting a broad scope for compliance. "Navigating the Complex Landscape: The Ongoing Conflict Between POPIA and FICA"

POPIA cherishes consent and confidentiality, granting individuals control over their information. FICA prizes transparency, pressing institutions to share data that may expose shadows where financial crimes lurk. Yet both laws share common values of integrity, accountability, and trust.

Navigating the turbulent waters of privacy protection and fraud prevention can be treacherous, but not impossible. Achieving a balance between the two can be attained through cooperation, vigilance, and adherence to South Africa's legal safeguards. Those who can navigate this balancing act will stay afloat, while those who ignore it will sink in the swirling tides.

By understanding the symbiotic relationship between POPIA and FICA, individuals and institutions can emerge on the other side with greater safety and security.

POPIA AND FICA: THE IMPORTANCE OF MANAGING COMMERCIAL CRIME

- POPIA helps prevent the misuse of personal data that could facilitate financial fraud or identity theft. Its consent requirements and limits on data use help protect people's information.
- The reporting requirements under FICA provide valuable intelligence that can identify patterns of suspicious transactions. This allows law enforcement to investigate and prosecute complex commercial crimes.
- FICA gives financial institutions and other accountable entities tools to detect and prevent money laundering, terrorist financing, and other financial crimes. This helps safeguard the financial system.
- Striking the right balance between privacy and financial integrity is crucial. Overly strict privacy laws could inhibit financial crime detection, while insufficient data protection could violate rights. POPIA and FICA aim to achieve this balance.
- FICA's "know your customer" rules help businesses avoid doing business with criminals or terrorists by identifying who customers are. This prevents the financial system from being used for illicit purposes.
- Ongoing education, like International Fraud Awareness Week, is important to keep the public informed and vigilant against the evolving techniques of commercial criminals. Preventing crime requires collaboration between government, businesses, and citizens.

POPIA and FICA are core pillars of the legal and compliance framework to combat illicit financial activity that underpins many commercial crimes. When implemented properly, they reinforce each other in upholding both data protection and financial security.

POPIA lays down the law with eight non-negotiable conditions for public and private entities dealing with data, demanding accountability, data processing limitations, purpose specification, and more. It's a comprehensive guide on how to safeguard the data of South African citizens.

The Eight Conditions of POPIA are defined:

Accountability	The responsible party is accountable for the personal information it processes and stays accountable for that personal information even if it passes the information on to a third party. The responsible party is the entity that needs the personal information for a particular purpose (the "why") and determines how that personal information must be processed in order to achieve the purpose (the "how").
Processing Limitation	Personal information must be processed lawfully and in a manner that does not infringe on the data subject's privacy. When processing personal information, those processing activities must be adequate, relevant and not excessive, considering the purpose that the information being collected and processed.
Purpose Specification	Personal information must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity of the responsible party.
Further Processing Limitation	Personal information may only be processed further if it is compatible with the purpose for which it was collected.
Information Quality	Personal information must be complete, accurate, not misleading, and updated where necessary.
Openness	The data subject must be made aware of the personal information being collected and processed, the purpose of collection, and any other relevant details.
Security Safeguards	Appropriate technical and organisational measures must be taken to secure personal information against loss, damage, unauthorised destruction, or unlawful access.
Data Subject Participation	Data subjects have the right to access their personal information held by responsible parties and request correction or deletion of such information.

The provisions of POPIA that allow for the sharing of information without consent in respect of fraud prevention and detection are:

Section 11(2)(b):

Personal information may be processed without consent if it is necessary to prevent or detect a crime or to comply with a legal obligation.

Section 11(2)(c):

Personal information may be processed without consent if it is necessary to protect the legitimate interests of the data subject or of another person.

FICA: DEFENDERS OF FINANCIAL INTEGRITY

The Financial Intelligence Centre Act, or FICA, was born from the necessity to combat financial crimes ranging from money laundering to identity theft. Over the years, FICA has evolved to align South African legislation with international standards set by the Financial Task Force.

The majority of criminal activities are perpetrated to achieve one thing - Financial Gain

If money is generated by crime, it is useless unless the original tainted source or intended usage of funds can be disguised as it could connect the criminals to the illegal activity and law enforcement officials would seize it.

Accountable Institutions in South Africa must walk the FICA tightrope before engaging in business relationships or transactions. They are mandated to collect, assess, and report specific personal information pertaining to their clients. The processing of this data may include analysis and escalation through reporting mechanisms to the Financial Intelligence Centre, aiding in the identification of suspicious transactions.

The 2017 FICA amendment marked a historic milestone by recognizing Crypto Asset Service Providers (CASPS) and including them in the Schedule 1 Accountable institutions. FICA's reach extends to entities like:

- Financial Services Providers
- Legal Practitioners
- Property Agents
- Motor Vehicle Dealers
- Mutual Banks

FICA Demands the following:

- Comprehensive Risk Management and Compliance Program
- A risk-based approach to information security and compliance
- Robust record-keeping procedures
- Know-Your-Customer Due Diligence
- Sanction Screenings

The responsibility for FICA compliance rests on the shoulders of directors and senior management within these institutions. Chapter 3 of FICA obligates Accountable Institutions to verify identities, report suspicious transactions, and act as gatekeepers against terror financing and money laundering.

CONCLUSION: THE BRIDGE BETWEEN DATA PRIVACY AND FINANCIAL SECURITY

POPIA and FICA are two important pieces of legislation that govern the collection, processing, and sharing of personal information in South Africa. While these laws may seem to be at odds at times, they ultimately work together to protect both data privacy and financial security.

POPIA ensures that individuals have control over their personal information and that it is not misused. FICA helps to prevent financial crimes by requiring Accountable Institutions to collect and report certain information about their clients.

When POPIA and FICA are implemented correctly, they can help to create a more secure and trustworthy environment for businesses and consumers alike.

In the case of Director of Public Prosecutions v Gerber (2007), the Constitutional Court of South Africa held that the common law right to privacy is not absolute and can be limited in certain circumstances, such as when it is necessary to protect the public interest. The Court found that FICA's collection and reporting requirements were justified in the public interest of preventing financial crime.

This case law example shows that the common law right to privacy can be superseded by statutory law in certain instances.

Legal jargon often leaves us bewildered, and those in the legal profession dedicate years to master the art of deduction. The Financial Intelligence Centre offers guidance to new Accountable Institutions, while consumers must respect the laws governing these institutions. In this environment of mutual respect and full legal compliance, business relationships

INTERNATIONAL FRAUD AWARENESS WEEK 2023

November 12th - November 18th

In 2023, the International Fraud Awareness Week, celebrated from November 12th to November 18th, takes centre stage. Fraud is an art of deception for unlawful gain and extends beyond just financial crimes. It encompasses identity theft, voter fraud, and healthcare fraud. The Association of Certified Fraud Examiners (ACFE) spearheads this annual global event, promoting anti-fraud awareness, education, and training to minimize the impact of fraud.

November 12 -18, 2023

5% OF GLOBAL ANNUAL REVENUE LOST TO FRAUD

The South African government reports a staggering 5% of global annual revenue lost to fraud each year according to the Association of Certified Fraud Examiners (ACFE) 2022 Global Study on Fraud and Abuse. To counter this, the government initiated the National Anti-Corruption Hotline (0800701701), centralizing the reporting of corruption and fraud cases. In addition to training and education, senior management is encouraged to conduct fraud checks within their organizations to identify vulnerabilities in their controls and processes, ensuring compliance with legislation.

- **POPIA ensures that individuals have control over their personal information**
- **FICA helps to prevent financial crimes by requiring Accountable Institutions to collect and report certain information.**

BIBLIOGRAPHY

Westerncape.gov

serr

popia.co.za

safetica

masthead

blog.docfox

debrarrichardson

gov.za

nationaltoday

RMG

fic.gov