comforte

LET’S TALK ABOUT THE POPI ACT

IF YOU’RE BOTHERING TO READ THIS

then you’re trying to understand POPIA’s effect on your business

You may have heard that South Africa’s Protection of Personal Information Act—known either as the POPI Act or just POPIA—became effective on July 1st 2020 (that’s what’s known as its commencement date). The good news is that POPIA includes a grace period of one year, meaning that while the regulation is currently effective, the official enforcement date for POPIA is July 1st 2021. Here are some bite-sized facts you may actually need to know:

- The right to privacy is **constitutionally protected** by the Republic of South Africa, guaranteed in section 14.
- POPIA strikes a **balance** between the individual’s right to privacy and other rights including the access to information to provide goods and services.
- POPIA is part of a **global movement** to codify international standards of the human right to privacy while promoting the **free flow of information.**

WHAT IF YOU COULD?

Consider how these outcomes would change your operations.

- **Protect peoples’ private information** even if it falls into the wrong hands?
- **Implement data security** that greatly exceeds POPIA’s minimum requirements for data privacy?
- **Work with peoples’ sensitive, private data** without having to de-protect or compromise that information?

YOU MIGHT ALREADY KNOW THIS

But if you don't, let's look at a few facts about POPIA.

POPIA regulates data privacy.

It establishes regulatory guidelines for the processing of sensitive personal information within South Africa's national jurisdiction.

POPIA grants citizens many rights.

The Act gives its citizens the rights and remedies to protect their own personal information from processing that is not in compliance with the conditions of the Act.

POPIA has teeth.

As with other data privacy regulations, POPIA establishes an independent regulatory body (the Information Regulator) that grants extensive powers to investigate potential non-compliance and fine violators appropriately. As a matter of fact, this regulatory body has been active since 2016 with the charter to regulate "without fear, favour or prejudice."

Those teeth can bite.

A person who is found guilty of an offense against the terms of POPIA can either be fined, imprisoned, or both.

HERE'S WHY YOU SHOULD CARE ABOUT POPIA

You probably don't need much encouragement to care about a new privacy regulation. But if you do business in or involving the subjects of South Africa and collect any personal information whatsoever, this Act really does concern you.

Purpose of POPIA

POPIA exists to protect the individual's right to personal privacy when that information is being used legally by responsible enterprises and governmental entities. The Act addresses the following:

- The acceptable way for these entities to process and handle that sensitive personal data
- The individual's rights and powers to protect their own personal information in instances that it is not being properly used
- An oversight office—the **Information Regulator**—to ensure compliance with the regulations spelled out by the POPI Act
- Specific applicable penalties for non-compliance

Affected Parties

POPIA protects the privacy rights of individuals within South Africa's national jurisdiction. It applies to:

- Individuals within South Africa's jurisdiction whose private data might be collected and processed by a lawful responsible party
- Responsible parties located within the Republic of South Africa
- Responsible parties located elsewhere that leverage data collection means within South Africa's jurisdiction.

Lawful Processing of Personal Data

POPIA puts the burden on the responsible processing party to handle and use peoples' private information in compliance with the Act. The major conditions of lawful processing include:

- In the **exact manner** as prescribed by the Act so as not to infringe on the individual's privacy
- With the data subject's **awareness** of personal data collection and use
- Only the **minimal amount** of relevant data needed to fulfill the lawful purpose of processing
- With the **consent** of the individual or when another law dictates its legal use
- Collected **directly** from the **individual** with a handful of very specific exceptions
- **Restricted retention** of the personal information collected and processed
- **Securely** to ensure integrity and confidentiality, including acceptable data protection safeguards

POPIA Enforcement

South Africa's Information Regulator has the sole authority to enforce compliance with the Act. Penalties for non-compliance are steep:

- Individuals guilty of offenses against POPIA can find themselves fined, imprisoned, or both, depending on the nature and severity of the offense
- Fines can range up to R10 million, which is over $600,000 USD, depending on a number of factors cited in the Act
- Imprisonment for the most serious offenses can range up to 10 years

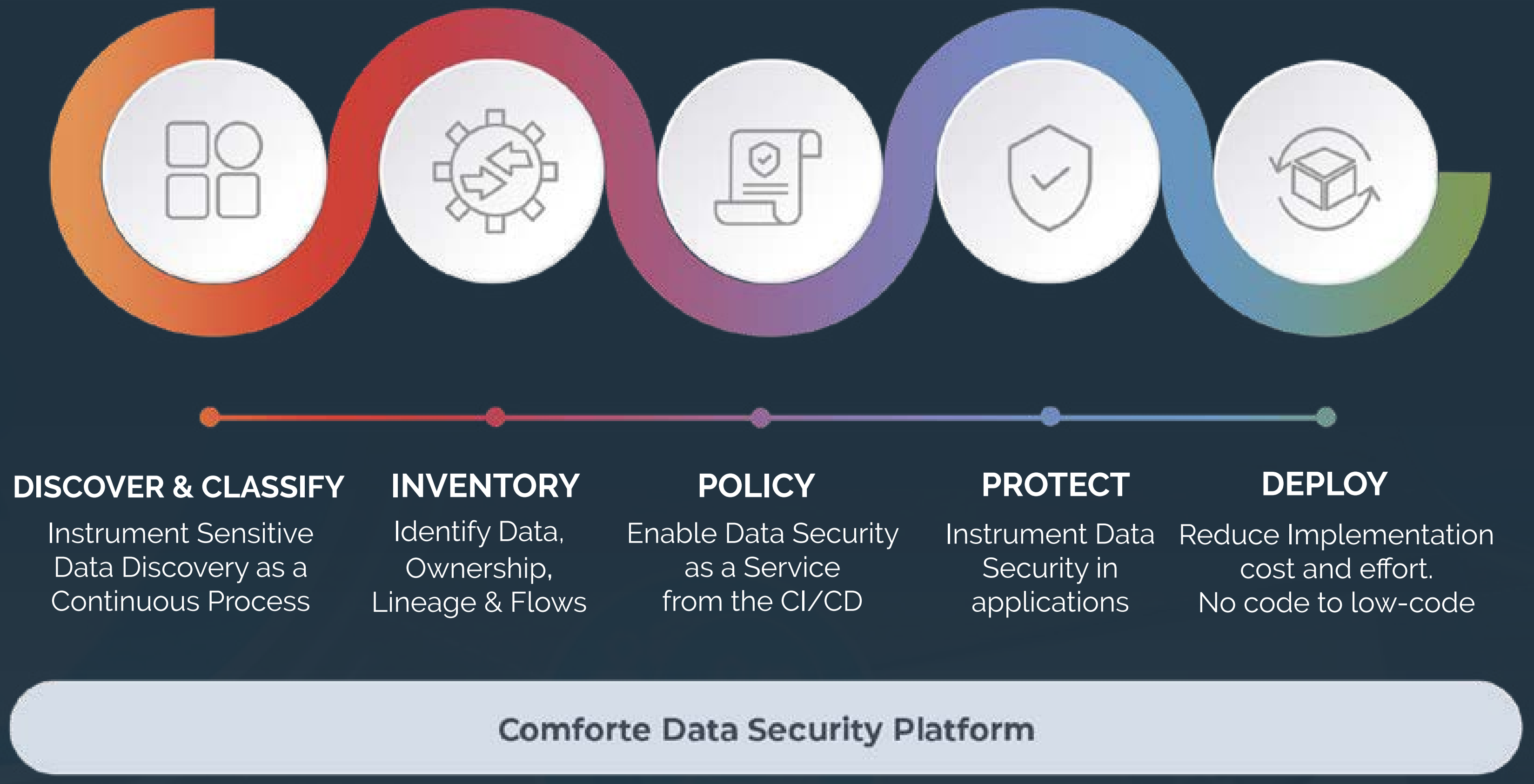
DATA-CENTRIC SECURITY TO THE RESCUE!

No doubt you realize that POPIA demands a sensible solution. But how? The best way to comply with data privacy regulations such as POPIA, GDPR, and others is to implement data-centric protection for all sensitive information in your data ecosystem. Data-centric security focuses on the protection of data itself (rather than perimeters, boundaries, or storage mechanisms around that data) and is based on two overarching principles that correspond to proper safe data processing:

1. **Protect sensitive data as early as possible in its life-cycle**
2. **De-protect sensitive data only when absolutely necessary**

To execute these two rules effectively, you need a specific set of technical capabilities going beyond just protection (like encrypting the data or tokenizing it). Organizations first need to be able to discover and classify sensitive data across various systems, repositories, and platforms. Gaining that knowledge allows organizations to get a clear picture of their data landscape and the associated levels of risk. With a focus on protecting all of their sensitive information, organizations can now create policies and deliver the right data protection methods that actually fit their business use cases and data types.

With appropriate protection mechanisms such as tokenization, the security mechanism travels with the data – independent of applications, databases and platforms – at rest, in motion, or in use. This allows organizations to take complete control of their sensitive data (control user access in real time and on granular levels leveraging behavior analytics, reports of data usage and security events), lowering compliance costs and significantly reducing the risk of data breaches..



DISCOVER & CLASSIFY
Instrument Sensitive Data Discovery as a Continuous Process

INVENTORY
Identify Data, Ownership, Lineage & Flows

POLICY
Enable Data Security as a Service from the CI/CD

PROTECT
Instrument Data Security in applications

DEPLOY
Reduce Implementation cost and effort. No code to low-code

Comforte Data Security Platform

Figure 1. Our data security platform provides end-to-end data discovery, classification, and protection, with ease of integration and cloud-native support.

SECURDPS IS A GAME-CHANGER

To comply with POPIA, the enforcement date of which is fast approaching, you need to be able to implement a data-centric security rapidly and in a cost-effective manner. You also need to ensure that it scales with your organization's data ecosystem and processing needs. Our SecurDPS Data Security Platform meets all of these requirements across the entire lifecycle of data in your enterprise.

We designed our platform from the ground up specifically for the modern, agile enterprise. This approach enables resilient data-intensive organizations to deliver privacy and security for their customers by design. We ensure that data protection can snap-in to applications, data processes, and workflows. Enterprises using comforte's SecurDPS Data Security Platform can truly balance data use, privacy, customer data value, and security under a single integrated and intelligent platform. Our customers can make privacy a business advantage to compete and grow successfully while building customer trust and loyalty.

Today, comforte's Data Security Platform is protecting hundreds of millions of payment transactions, healthcare records, insurance records, and more, reliably running in business-critical environments. Comforte experts have implemented the platform in large enterprises and bring decades of experience to client projects for success on a global basis. We take our leadership in the industry seriously and contribute to standards for data protection.

Our Data Security Platform has been helping organizations comply with governmental data privacy regulations for years now.

Check out our capabilities and some success stories by going to

www.comforte.com/solutions/compliance.