

Protection of Personal Information Act (POPIA)

Meet Compliance Requirements to Protect Personal Information in South Africa.

The mandate of South Africa's Protection of Personal Information Act (POPIA) is to regulate the processing of personal information. With this Act, data breaches need to be reported by law. Organisations need to develop a clear data protection plan to build trust with customers, drive business growth, and avoid costly penalties. The Act comes in to force on 1st July 2020 with a 1 year grace period thereafter within which to ensure compliance.

The foundation of any data security strategy is to identify sensitive and regulated data so that both users and security technologies can make informed, deliberate decisions on how that information should be protected. Fortra's Data Classification Suite (DCS) helps organisations comply with POPIA by discovering, identifying, and classifying emails and files at the point of creation or in on-premise and cloud-based file shares to ensure compliant policy enforcement.

Make Staff Aware of the Value of Personal Data

A central pillar of POPIA is increased accountability to protect personal data. Data protection must be built into every aspect of the data handling workflow. DCS visual markings and pop-up reminders build a culture of security by forcing employees to consider the value of the personal data with which they are working.

Protect Personal Data

The Act states that organisations must identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control. When people and systems know the sensitivity of an email or file they can accurately enforce the proper data protections. DCS helps to ensure data is shared according to policy across departments, locations, and organisations. In addition, DCS enhances the effectiveness of the entire data security ecosystem.

WHY COMPLY WITH POPIA?



Obey Legal Obligation



Avoid Substantial Penalties Up

to R10 million fines
Up to 12 months in jail



Create A Culture Of Security

Extend security awareness to all
systems and processes



Limit Reputational Damage

Breaches must be disclosed



Prevent Client Loss

A reputation for breaches could drive
away customers and partners

Proactively Delete Old Data After a Reasonable Time

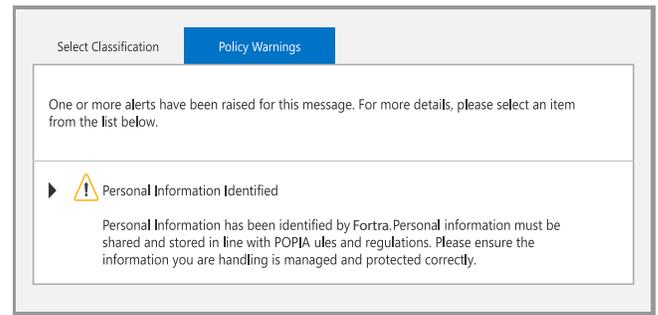
Personal information collected and retained by organisations is also subject to deletion. It can be difficult to guarantee all personal data is deleted if it has been exported to files outside the central database. The metadata DCS applies to files helps enable staff to locate files that should be deleted for compliance purposes, no matter where they are stored.

Supporting the Information Officer

One of the mandates for compliance with POPIA is to have a named Information Officer appointed within your organisation. The Information Officer must ensure that the organisation complies with POPIA. He or she needs the means to monitor how personal information is being shared, discover violations, and enhance data protection policies. As users work with email, documents, and files, DCS logs meaningful activities and policy alerts, permitting detailed reporting and analytics. Classification adds a level of detail to reporting that is not normally available, enabling the Information Officer to identify exactly where sensitive data is being mishandled, or where a user presents a threat to data security.

Supporting Data Subject Access Requests

Under POPIA, any personal data obtained by an organisation can be subject to access requests. Anyone has the right to request if a company holds personally identifiable information (PII) on them, what the data is, the reason for collection, and how long the data will be held for. In many cases, private individuals have the right to request that personal data be deleted from systems in its entirety. DCS machine learning technologies effectively identify and locate hard-to-find PII in data repositories that include on-premise file shares and popular cloud repositories to take the guesswork out of data subject access requests.



Remediate

Remediate

Assists users with privacy awareness



Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.