Solution Brief

mimecast™

Simplify POPIA Compliance for Cybersecurity

The Protection of Personal Information Act (POPIA) is South Africa's data protection law. It aims to monitor, protect and regulate the processing and flow of personal information within and outside organisations to ensure the legitimate use of personal data. POPIA follows the implementation of similar regulations elsewhere in the world, most notably the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA).

POPIA empowers South African citizens with enforceable rights regarding their personal information, including the right to access, the right to correction, and the right to erasure, also known as the right to be forgotten.

POPIA was signed into law on 26 November 2013 and was made effective in July 2020. Organisations have been given a grace period until 1 July 2021 to put appropriate measures in place to comply with the regulations contained within POPIA.

POPIA's Implications for Cybersecurity

Under POPIA, "personal data" is defined as any information about an identifiable natural living person, or a juristic person, or a legal entity such as an organisation.

Types of personal information include:

- Contact details such as an email address, telephone number, physical address
- Demographic information such as age, gender, birth date, ethnicity
- Historic information such as past employment, financial information, education, criminal records, medical history
- Biometric information such as blood type
- Opinions of and about a person
- Private correspondence

POPIA establishes eight minimum requirements for the lawful processing of personal data, namely Accountability, Process Limitation, Purpose Specification, Further Processing Limitation, Information Quality, Openness, Security Safeguards and Data Subject Participation.

Of the eight requirements, security safeguarding holds the greatest potential risk for organisations. The growing volume and sophistication of cyberattacks means organisations are perpetually besieged by an array of attack types designed to breach organisational defences and steal sensitive personal and company data.

Under POPIA, responsible parties can still be considered compliant with the Act if they suffer a data breach, as long as they have taken 'all reasonable steps' to secure and protect the personal data of any data subject. Failure to do so could expose organisations to loss of trust with customers, damage to their reputation and, from a legislative point of view, fines or even imprisonment imposed by the Information Regulator, who has been appointed to oversee POPIA compliance in line with the stipulations of the Act.

To protect against modern attack types and maintain compliance with POPIA, organisations need to develop layered security strategies that protect users and data across three zones, namely:

1. At their email perimeter, which most cyberattacks leverage in some form through phishing, ransomware, malware and impersonation attacks;
2. Inside their network and organisation, where threats can easily and quickly spread from one infected user to another, either by accident or purposely through malicious insiders; and
3. Beyond their perimeter, where even unsophisticated attackers can impersonate organisations' websites or send fake emails using legitimate domains.

In addition, the volume of unstructured business data – such as data in emails, collaboration tools such as Microsoft Teams, archives and shared drives – is growing. More than 80% of the world's data is unstructured. POPIA requires that organisations protect personal information in all its forms, including unstructured data. This means organisations need additional tools and controls for collecting, processing and storing structured and unstructured data, to ensure they are able to efficiently search for, find, extract and potentially delete data on request.

How Mimecast Supports POPIA Compliance

While no single solution can make an organisation fully compliant with POPIA, Mimecast offers a range of solutions that can support and ease compliance efforts for organisations of every size.

Mimecast Email Security with Targeted Threat Protection helps organisations defend against a number of email-borne threats, including impersonation attacks, ransomware and phishing. It also helps defend against internal threats, such as employees intentionally or unintentionally sending emails containing malware to internal or external recipients.

Mimecast Information Protection gives organisations the ability to integrate Data Leak Prevention and other email content control tools into their environment seamlessly. Organisations can also safely transmit and control how users share or access confidential information through email with Secure Messaging, and safely send and receive large files through Large File Send.

Mimecast Cloud Archive provides a unified platform for information governance, with fully integrated capabilities for retention management, email encryption, discovery and data recovery to ensure complete litigation readiness and compliance control.

Mimecast SAFE Cloud enables organisations to protect, discover, investigate and recover data from internal and external threats within supported applications. As part of Mimecast's holistic approach to helping organisations achieve cyber resilience, Mimecast SAFE Cloud is currently available for Microsoft Teams; delivering protection against malicious files and URLs, archiving that captures messages and content in native format (including text, images and more), case review for litigation and investigation support, and legal hold for data preservation.

Mimecast DMARC Analyzer empowers organisations to detect and prevent spoofing of their own domains, keeping customers and partners safe from phishing attacks and maintaining high levels of trust between the organisation and its stakeholders.

Mimecast Brand Exploit Protect helps organisations protect their brand by preventing cybercriminals from registering lookalike domains to launch targeted attacks aimed at stealing their customers' and partners' personal information, credentials and money.

Mimecast Awareness Training helps to equip employees with practical tools and knowledge to empower them to spot and avoid risky online behaviour, including clicking on unsafe links, sharing potentially harmful emails or attachments, and spotting attempts at phishing and impersonation fraud.

Mimecast's API integrators also provide valuable add-on tools that bolster an organisation's security posture and helps keep sensitive data safe from criminals.

Zone 1	Zone 2	Zone 3
At the Email Perimeter	**Within the Network and Organisation**	**Beyond the Perimeter**
Protection against business email compromise, phishing, spear-phishing, ransomware, malware, malicious URLs, data loss.	Protection against malicious insiders, employee error, spread of email threats from one infected user to another.	Protection against brand impersonation, domain hijacking, extended phishing attacks targeting customers and suppliers.

Conclusion

POPIA will transform how personal data of South African data subjects is collected, stored, managed, and secured. While it promises a new era of control and transparency for data subjects, POPIA significantly raises the stakes for any organisation that collects, processes or stores personal data, with potentially ruinous penalties for those that don't comply with its requirements.

Organisations already besieged by cyberattacks – made even worse since the start of the pandemic which caused major uncertainty and disruption – now need to take all steps possible to maintain the highest standards of data security and protection.

Old tactics and techniques won't suffice in an environment where the volume and sophistication of cyberthreats continue to grow exponentially. Implementing simple controls and safety measures won't provide the security needed to protect data. Organisations require a layered security approach that provides protection within the organisation, at its perimeter, and beyond, where threat actors are finding increasing benefits from brand impersonation and exploitation.

Mimecast is a committed partner to organisations and their efforts in becoming POPIA compliant, offering a portfolio of cloud-based cyber resilience solutions that can keep customers – and data – safe from cyber threats.