mimecast™ | FAQ

Mimecast and POPIA — Frequently Asked Questions

What is POPIA?

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 makes provision for individuals to request any data that organisations are storing that relates to them personally, withdraw consent to use such data, and effectively request its destruction.

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.

What constitutes "personal data" under POPIA?

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

Where should organisations focus their efforts to ensure they can adequately protect and manage personal data?

While most compliance efforts are centred on the collection and processing of structured data - such as data organised in systems linked to relational databases including marketing lists, financial systems or enterprise resource planning systems - more than 80% of the world's data is unstructured. POPIA requires that organisations protect personal information in all its forms, including the unstructured and semi-structured data found in email systems, collaboration tools such as Microsoft Teams, archives and shared drives.

Organisations need to implement tools and controls that can help manage the collection, processing and storage of all structured and unstructured data, and ensure they are able to efficiently search for, find, extract, and potentially delete data on request.

How does the Mimecast Cloud Archive help organisations achieve POPIA compliance?

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

Through the Mimecast Cloud Archive, organisations gain access to comprehensive search, e-discovery and compliance support capabilities that provide retrieval of important corporate data, underpinned by tamper-resistant chains of custody to support data governance and resilience.

Immutable audit logs keep a record of all access to the archive, including searches performed and archive messages viewed in accordance with any company or regulatory policies such as POPIA. Real-time notifications and additional security options are enforced for each search by entering a "search reason", which is logged for audit purposes.

Granular role-based controls determine the level of access IT administrators have and which tasks they can perform, such as viewing specific personal information or exporting a restricted set of data within the archive.

What assurances can Mimecast provide that personal information held in the Mimecast Cloud Archive is complete, accurate and up-to-date?

The Mimecast Cloud Archive offers secure storage for email and file information with all its metadata intact. Comprehensive regulatory, e-discovery and litigation support is available with compliance-driven chains of custody maintained throughout the entire information lifecycle.

Mimecast's ISO27001 certification provides validation of the security mechanisms and controls employed to protect the authenticity and integrity of a customer's information stored within the Mimecast archive. ISO 27018 certification provides further validation related specifically to the protection of personally identifiable information.

What can Mimecast do to limit the amount of personal data that is retained in accordance with POPIA?

Retention of messages containing personal data is automatically managed based on predefined settings. Retention schedules can be adjusted or customised using various attributes such as content, people, location or department.

In cases where POPIA data retention requirements apply, IT Administrators may need to remove messages containing personal data from the corporate archive permanently (known as a purge) or reduce the time these messages are held in the archive.

Adjustments can be set to either expire emails immediately or to expire emails after a certain number of days. Retention adjustments cannot be used to extend the retention period of emails beyond maximum retention settings.

Mimecast uses a single instance storage service, meaning any email that is subject to a retention adjustment is updated or expired in its entirety for all recipients of the message. Once a message is expired it is not recoverable.

How does Mimecast help organisations notify data subjects when their personal information is being archived?

IT administrators can use Mimecast's stationery service to add legal disclaimers to emails or send notifications directly to data subjects when personal information is detected within an email or its attachments.

Mimecast Document Services further allow watermarks to be embedded into Microsoft 365 documents before converting them to PDF. Such watermarks can be used to notify the sender or recipient that the document contains personal information and could be archived for further processing in the future.

Why is email an important component of POPIA compliance?

Email is the number one business application and the primary form of business communication. It contains a wealth of personal information that, under POPIA, organisations must take 'all reasonable steps' to protect.

Studies have found that 90% of successful phishing cyberattacks start with email as the main attack vector. Any breach of personal information due to insufficient email security and data protection could result in a loss of trust, reputational damage, and even fines or jailtime, making it essential that organisations take all reasonable steps to secure their email systems.

What tools does Mimecast offer that help with securing email?

With the ongoing rise in the volume and sophistication of cyberattacks, organisations face a daunting task to ensure the email data they manage remains secure.

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 email containing malware to internal or external recipients.

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.

Is it enough to just protect my email to ensure POPIA compliance?

No single solution can make an organisation fully POPIA compliant. When it comes to preparing to manage and adhere to data regulations, like POPIA, organisations need to think beyond traditional, defence-only security. With organisations bearing a greater level of responsibility for data protection, compliance and continuity, an evolution from cybersecurity to cyber resilience is required.

Organisations need to ensure they protect their customers and themselves across all 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.

Mimecast can help organisations develop a layered security strategy that protects data and customers and helps them recover from and continue with business as usual in the event of an attack:

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. The Mimecast Cloud Archive gives customers of all sizes the confidence, control and accessibility they need to manage their data. This means going beyond the boundaries of traditional archiving by creating a central repository of corporate data which is stored for 99 years in the Mimecast Cloud Archive, a fully encrypted, immutable and redundant system. This dramatically decreases the risk of data loss or corruption after a cyberattack, human error or technical failure.

Mimecast Business Continuity enables employees to access everyday tools, like Microsoft Outlook or G-Suite by Google Cloud, without disruption. If PCs or the broader network are affected, Mimecast provides alternative email access points through the web and our robust mobile continuity apps.

Organisations need to be prepared to quickly and seamlessly switch to an available service, should downtime, due to breach, human error or technical failure, occur. With no company email, employees could use personal email, which likely doesn't meet compliance requirements. Such personal email usage by employees could pose a significant risk.

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

Mimecast Brand Exploit Protect helps organisations protect against cybercriminals registering lookalike domains to launch targeted attacks aimed at stealing personal information, credentials and money.

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.

How does Mimecast support data subject access requests as described in POPIA?

The Mimecast Case Review App supports data subject access requests by allowing IT administrators or legal staff to locate personal data through the application of granular filters during content, attachment and metadata searches.

The process of responding to data subject access requests is simplified by enabling multiple search streams to be grouped into a single case for query, comment or culling, which can be extended to external parties such as outside counsel or third-party e-discovery service providers.

Will the personal data of South African citizens be transferred out of the country?

All Mimecast customers' data is stored in defined, appropriate jurisdictions perpetually within a secure, resilient, scalable and immutable archive. Organisations can classify personal information through content policies, to secure information entering and leaving the organisation or the country.

As a company, is Mimecast POPIA compliant?

Mimecast's products and services are aligned with POPIA compliance requirements.

At Mimecast, we hold ourselves to the highest security and privacy standards. We have implemented security and data protection measures that span the technology, operations, and legal aspects of protecting customer data, including POPIA. We constantly undertake and maintain numerous certifications and audit reports to provide transparency and communicate internal controls to our customers and partners.

The list of certifications, attestations, and assessments achieved by Mimecast include the following:

- **ISO 22301 Certification:** Business Continuity Management System (BCMS)
- **ISO 27001 Certification:** Information Security Management System (ISMS)
- **ISO 27018 Certification:** Protection Controls for Personally Identifiable Information (PII)
- **SOC 2 Attestation Report:** Internal Controls for Security, Availability, Processing Integrity, Confidentiality, and Privacy

For more information, please visit www.mimecast.com