ManageEngine's guide for **POPIA** compliance

ManageEngine

Table of contents

DISCLAIMER

 This material and its contents ("Material") are intended, among other things, to present a general overview of how you can use ManageEngine's products and services to facilitate compliance with South Africa's POPIA. Fully complying with the POPIA requires a variety of solutions, processes, people, and technologies.

The solutions mentioned in this Material are some of the ways in which IT management tools can help with some of the POPIA requirements. Coupled with other appropriate solutions, processes, and people, ManageEngine's solutions help achieve and sustain POPIA compliance. This Material is provided for informational purpose only and should not be considered as legal advice for POPIA compliance. ManageEngine makes no warranties, express, implied, or statutory, and assumes no responsibility or liability as to the information in this Material.

You may not copy, reproduce, distribute, publish, display, perform, modify, create derivative works, transmit, or in any way exploit the Material without ManageEngine's express written permission.

The ManageEngine logo and all other MangeEngine marks are registered trademarks of Zoho Corporation Pvt. Ltd. Any other names of software products or companies referred to in this Material, and not expressly mentioned herein, are the trademarks of their respective owners. Names and characters used in this Material are either the products of the author's imagination, or used in a fictitious manner. Any resemblance to actual persons, living or dead, is purely coincidental.

What is POPIA?

South Africa now has it's own data protection regulation, namely the Protection of Personal Information Act, or POPIA, which came into effect on July 1, 2020. It concerns both public and private organizations situated within and outside the Republic of South Africa handling the personal information (PI) of South African citizens. Failure to comply with this regulation can lead to either imprisonment of up to 10 years, a fine of up to R10 million, or both.

Objectives of POPIA

Businesses can take a step closer to POPIA compliance by understanding it's three main objectives:

- **Advocating the protection of personal information.**
- **Formulating guidelines and standards for data protection.**
- **Providing personal rights around the data collection and handling process, and direct marketing by means of unsolicited communications and automated decision-making, the process of making decisions without human involvement by profiling the data subjects.**

The POPIA conditions

POPIA sets eight conditions for the lawful processing of PI, and establishes the data subject rights pertaining to information collection, storage, and processing. Organizations are required to meet these conditions to become POPIA compliant. The conditions are:

Condition 1. Accountability

This condition requires the responsible party, usually the Information Officer (IO) or the officials delegated by the IO, to bear the sole responsibility to ensure compliance during the collection, storage, and processing of PI.

Condition 2. Processing limitation

Only adequate information should be collected and processed in a lawful manner. The PI should be directly collected from the data subject unless it is publicly available. Explicit consent is required from the data subject unless it is part of a judicial function.

Condition 3. Purpose specification

The PI collected should be for a specific, explicitly defined, and lawful purpose which the organizations intend to perform. The data subjects must be informed about the purpose of its collection and once its fulfilled, the PI should be discarded in an irretrievable manner.

Condition 4. Further processing limitation

Further processing of the data obtained should be compatible with the purpose stated during the initial data collection. Further processing requires additional consent from data subjects if it wasn't obtained initially unless its for legal or national security requirements.

Condition 5. Information quality

The responsible parties in the organizations should take measures to ensure that the information collected and processed should be complete, accurate, updated, and not misleading in any way.

Condition 6. Openness

This condition requires strict documentation of all the activities accomplished by organizations using the PI in their possession. It should take all possible measures to make the data subject aware of the type, source, and purpose of the PI obtained.

Condition 7. Security safeguards

Organizations must take reasonable technical (e.g. security audits, encryption) and organizational (e.g. compliance policies) measures to maintain the integrity and confidentiality of the PI collected. Officials delegated by the Information Officer (IO) must process data only with their approval. In the event of a breach, the IO should inform the Information Regulator (IR), and the data subject as soon as practically possible.

Condition 8. Data subject participation

This condition focuses on the rights of the data subjects, which are discussed in detail in the subsequent sections. Part B of this condition also prohibits the processing of special information like religious beliefs, ethnic origin, criminal behavior, as well as medical and biometric information without the additional consent of the data subject. But all these rights are subject to certain exemptions.

Data subject rights provided by POPIA

This act highlights certain data subject rights in its conditions, especially in conditions two, three, six, and eight. Knowing these rights will help organizations better comprehend the requirements and purpose of these conditions.The following rights are provided by POPIA to the data subjects:

Information

The right to be informed if their PI is being collected by someone, or is accessed by an unauthorized source.

Access

The right to request access to a copy of the PI held on them by the organization or third parties, if any. Organizations should provide this information within a reasonable time frame in a format which is understandable.

Correction

The right to request correction of any PI which might be outdated, misleading, incomplete, irrelevant, inaccurate, and/or obtained unlawfully.

Deletion

The right to request deletion of irrelevant, excessive, and unlawfully obtained PI.

Objection

The right to object or withdraw consent for the processing of their information if they have legitimate grounds for their objection. Here, processing means doing something with the data like sending marketing communications, storing the email addresses in a database, etc.

Exemptions

The data subject rights concerning the processing of PI is not applicable if:

- It's in line with the public interest, like anti-money laundering, public safety, etc.
- The processing is done by a public body involved in national security, or defense
- It's part of a judicial function
- It's for the economic or financial interest of a public body, like the Cabinet or Executive Council of the Province
- It's for historical, statistical, or research activity

How to prepare for POPIA compliance

Here are some simple measures that organizations can adopt to facilitate POPIA compliance:

1. Understanding the POPIA requirements

Evaluate its:

- Purpose
- Objectives
- Conditions
- Penalties

2. Performing personal information (PI) audits

Classify information into:

- Personally identifiable/non-personally identifiable
- Sensitive/non-sensitive
- Special personal information; Religious or philosophical beliefs, race, ethnic origin, trade union membership or political persuasion, medical or criminal records, biometric information
- Information of children

Assess:

- The location of storage
- Sources of data collection
- Personal information flows within and outside your organization

3. Appointing an Information Officer (IO)

Duties of an IO include:

- Taking measures to comply with POPIA
- Working with the Information Regulator (IR)
- Dealing with data subject rights-based requests

4. Enabling means to enforce data subject rights

Provide:

- Secure web forms for raising such requests
- Contact email address

5. Reviewing the direct marketing methods

- Obtain consent from non-customers
- Additional consent is not needed from existing customers provided clear opt-out options are part of the communications
- Enable simple opt-out options in emails, like unsubscribe links
- Avoid using pre-checked boxes when seeking consent
- Ensure that automated decision-making satisfies the data subject's legitimate interest

6. Having a privacy policy in place

The policy should include:

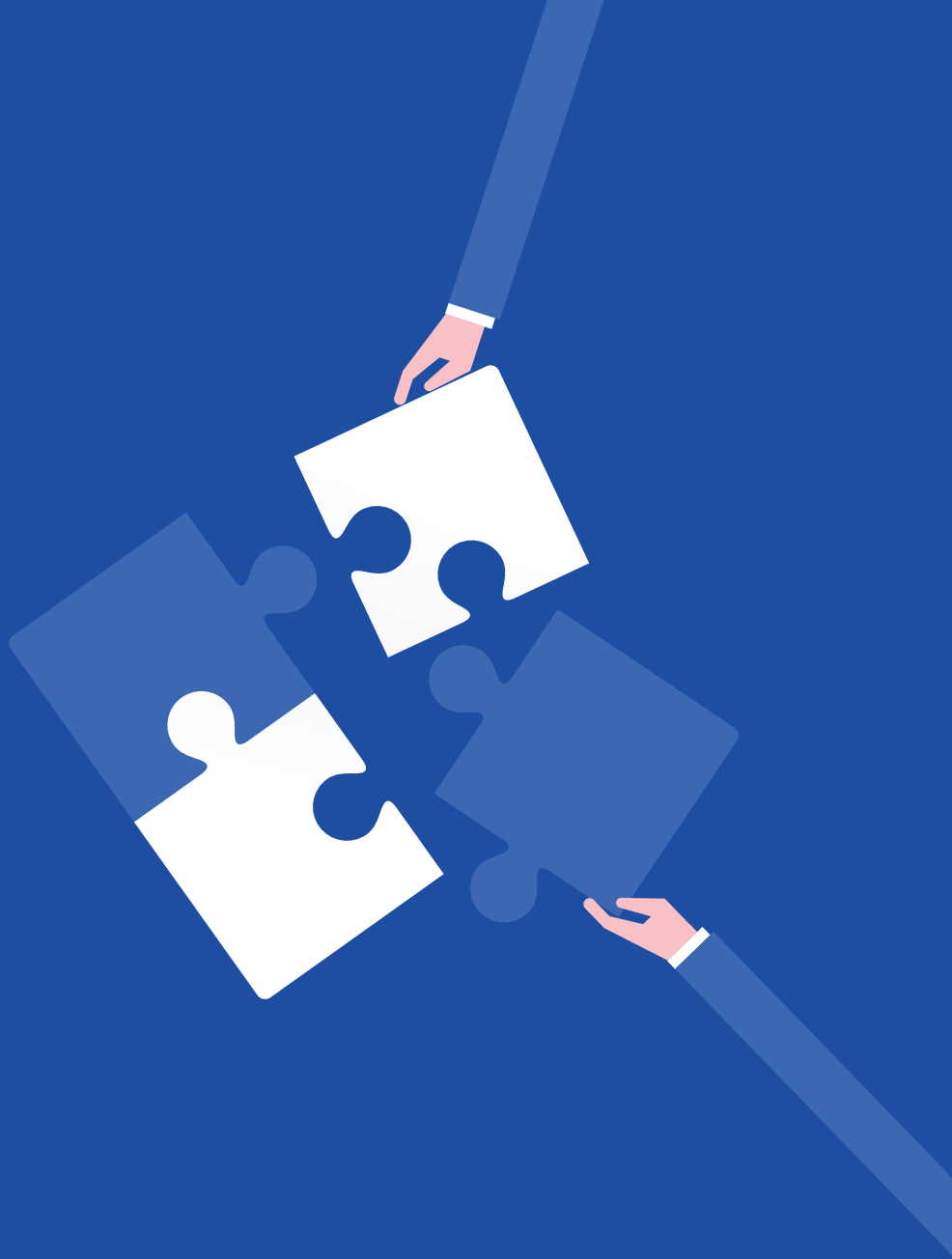
- Company name and contact details
- Nature and purpose of the PI obtained
- Data subject's rights to access and to correct the PI

7. Enforcing information security measures

- Perform a Data Protection Impact Assessment (DPIA)
- Implement technical measures like encryption, antivirus, firewalls, security audits, deploying IT security solutions
- Implement organizational measures like formulating compliance policies, employee training, privacy by design approach
- Enable breach notifications; timely notification to the information regulator and the concerned individual in the event of a breach

ManageEngine solutions for POPIA compliance

The best practices to achieve compliance has been covered, now let's dive into the specifics of the POPIA conditions and how they can be met. ManageEngine has a comprehensive suite of IT management solutions to help your organization comply with the data security, documentation, and audit requirements of seven out of its eight major conditions.



POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
2. Processing limitation	**10.** Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant, and not excessive.	Collect and store only the sufficient information needed to achieve the specified legal purpose.	Locate and delete junk data, like duplicate and orphaned files, to ensure that only relevant data is stored using DataSecurity Plus. Perform a permission analysis to list users who have access to the data, along with details on what actions each user can perform on it with DataSecurity Plus.
3. Purpose specification	**13.** (1) Personal information must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity of the responsible party.	Collect personal data only for legitimate purposes, and ensure that there aren't any deviations from the stated purposes while processing the data.	Identify anomalous activities, like unauthorized access, data deletion, collection or modification using DataSecurity Plus' access audit reports. Monitor the creation, deletion, access, modification, or renaming of critical files and folders, including failed attempts to perform any of these actions using Log360. Receive notifications in case of anomalous activities in the network with Firewall Analyzer's custom alert profile. OpUtils can be configured to track all the devices in your network automatically and alert you when a rogue or unauthorized device enters your network.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
3. Purpose specification	**14.** (4) A responsible party must destroy or delete a record of personal information, or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2). (5) The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form. 7. Personal information referred to in subsection (6) may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect to a child, or for the protection of the rights of another natural or legal person, or if such processing is in the public interest.	Organizations are required to discard the personal information which they hold in an irretrievable manner as soon as its purpose is achieved. Extended storage or processing requires the data subjects explicit consent.	Discover who has full access to Windows shares, and locate files and folders shared with everyone using DataSecurity Plus. Differentiate and store personal and corporate data in devices using Endpoint Central's containerization feature. You can also delete all forms of PI associated with a user from your servers, and revoke access to the data. Automatically delete all the PI after a certain period of time using OpManager and Network Configuration Manager. Users can also choose to delete it manually as well.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
4. Further processing limitations	**15.** (1) Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13.	Have alert systems in place to get real time notifications on any deviations occurring in the processing of data from the originally stated purposes.	The prepackaged alert profiles in Log360 will warn authorities by sending notifications in case of anomalous activities, like modification or unauthorized access, shares, etc. Track the recent changes made to your files and folders, and trigger instant alerts in case of suspicious activity with the file monitoring feature of Applications Manager.
5. Information quality	**16.** (1) A responsible party must take reasonable practicable steps to ensure that the personal information is complete, accurate, not misleading, and updated where necessary.	Keep the data updated at all times, and take necessary security measures to avoid any modification or destruction to the information.	Know the whereabouts and integrity of the stored data at all times by scheduling scans of all devices in your organization using Endpoint Central. Detect and remove incorrect or outdated PI using the file analysis and storage analysis reports available in DataSecurity Plus. Audit databases using Log360 to determine whether the data storage threshold has been reached so that such personal data can be deleted immediately.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
6. Openness	**17.** A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.	Maintain strict records of all activities undertaken in association with the collection, processing, and deletion of the collected data, including the security measures taken to safeguard the data.	Get a complete audit trail of all the activities related to the sensitive data stored in your organization using ADAudit Plus. Maintain a record of all processing operations as mandated by POPIA with Endpoint Central's Audit LogViewer. Obtain simplified reports on the personal data stored, including the type, location, and the amount stored in each file by using DataSecurity Plus. It also helps to detect and audit the user activities occurring in individual files containing confidential information. Receive context-based audit logs and session recordings of all activities performed on personal data repositories using Access Manager Plus. Maintain and view a record of all processing operations related to sensitive data using Action Log Viewer feature in Patch Manager Plus.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
			Prove compliance with various standards by providing forensic investigators with readily available video recordings, out-of-the-box compliance, custom reports, and audit logs on every privileged activity by using PAM360. Applications Manager lets you view the Audit Log information to keep track of all the events occurring in your account. It helps identify changes made to your profile within a specific period. OpManager lets you view Audit log reports from Reports → Audit, where you can keep track of all the events/activities performed in the product.
7. Security safeguards	**7.19.** (1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical, and organisational measures to prevent— (a) loss of, damage to or unauthorised destruction of personal information; and	Take utmost care to secure the personal data from unauthorized means of processing and cyber-attacks by taking the appropriate technical and organizational measures.	Identify users and devices trying to gain access into confidential data and business systems using Endpoint Central's Conditional Exchange Access feature. Instantly notify authorities when unauthorized accesses and critical file changes are attempted to thwart such attempts using predefined alert profiles in Log360.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
	(b) unlawful access to, or processing of, personal information.		Audit file and folder actions, audit file accesses, trigger instant email alerts in case of suspicious activity, detect and contain ransomware attacks using DataSecurity Plus. Monitor browsers to detect and fix misconfigurations based on their compliance to security standards using Browser Security Plus. You can also perform periodic scans of all browsers used in multiple devices to detect any threats with the help of Browser Security Plus. Use Patch Manager Plus to mask/remove/retain PI while scheduling or exporting user reports. Get detailed reports on the users who have access to folders and servers containing sensitive data, manage the access permissions to critical file servers, clean up stale user accounts and empty security groups, thereby avoiding unauthorized access using AD360. Monitor configuration drifts and misconfiguration in endpoints using a predefined set of baselines, and correct them to achieve compliance using Vulnerability Manager Plus.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
			Allow only authorized applications to execute by blacklisting and whitelisting applications using Application Control Plus, thereby preventing malware intrusions, threats, and zero day attacks. View Audit Log informati on to keep track of all the activities of firewall users with Firewall Analyzer. The file monitoring feature in Applications Manager helps track recent changes made to your files and folders, and generates alerts if the files and folders undergoes any changes. Trigger instant alerts in case of any authentication failures using the event log and SNMP trap monitoring features in OpManager. Also, it's file and folder monitoring feature will raise an alert in case of any modification. Notify administrators immediately when there is a change in the state of an IP address using OpUtils' IP address management feature

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
	7.19. (2) In order to give effect to subsection (1), the responsible party must take reasonable measures to— (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; (b) establish and maintain appropriate safeguards against the risks identified; (c) regularly verify that the safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated in response to new risks, or deficiencies in previously implemented safeguards.	Be prepared for both internal and external risks which might arise from data alteration, deletion, or leakage by periodically assessing and updating appropriate preventive mechanisms.	Calculate the risk score of files containing sensitive personal data by analyzing their permissions, volume, and type of rules violated, audit details, and more using . Classify business-critical files based on their sensitivity, and prevent their leakage via email, USBs, printers, etc with DataSecurity Plus. Shut down infected DataSecurity Plus systems and disconnect rogue user sessions to help limit the damage using DataSecurity Plus' automated threat response mechanisms. Secure data in transit and learn easy ways to monitor and manage your public key infrastructure using Key Manager Plus. Encrypt personal data stored on mobile devices and set alerts in case a device does not check in with the server over a predefined period using Endpoint Central. Centralize and correlate security data from multiple sources to identify potential threats instantly and avoid data loss with Log360.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
			Audit changes to personal data like modification, renaming, deletion, or permission changes using Log360. The website content monitoring module of Applications Manager identifies and alerts user of security infringements or website defacement through which potentially hazardous content can be detected. Its Real Browser monitoring module also helps detect anomalous workflows in case the site is being hacked.
	7.20. (1) An operator or anyone processing personal information on behalf of a responsible party or an operator, must— (a) process such information only with the knowledge or authorisation of the responsible party; and (b) treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.	Ensure that only authorized personnel gain access to the PI and take measures to maintain the confidentiality and integrity of the data.	Manage, monitor, and audit administrative access to systems and applications that handle personally identifiable information using Password Manager Pro. Detect unauthorized access to personal data without proper permissions using Log360 and AD360. Provide users with granular, time-bound access to sensitive systems and applications via a request-approve-release workflow with Access Manager Plus.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
			Encrypt entire disk volumes to prevent unauthorized access and data extrusion using Vulnerability Manager Plus. Grant permissions of your choice, based on multiple predefined and/or tailor-made roles using it's Role-Based Access Control (RBAC) approach with Device Control Plus. Establish role-based access control for Microsoft 365 administration so that only authorised users can access privileged data by using the delegation feature in M365 Manager Plus. Enforce a Password Policy set for SQL servers for each user and set expiration dates for the password created, further reducing the risk of unauthorized access by using old passwords using Applications Manager. Grant access to servers and shares containing sensitive data, and also modify or revoke the permissions granted, through AD360's : - Group membership management and file server permissions management capabilities - User provisioning and re-provisioning templates

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
			- Approval based workflow, temporary access settings - Role-based delegation Enable two-factor authentication and access control workflows in PAM360, and leverage its just-in-time privileged access to ensure that only authorised users can remotely access sensitive data for a specific time period.
	7.22. (1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, the responsible party must notify— (a) the Regulator; and (b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.	Implement security systems which will help to detect the source and impact of any potential vulnerabilities or cyberattacks. This would enable the timely notification to the concerned authorities and data subjects.	Mitigate external threats by detecting known attack patterns like DoS, DDoS, SQL injections, ransomware attacks. etc., with the twenty-five predefined rules in its real-time correlation engine using Log360. Gain access to in-depth analytical reports that help investigate any data breach attempts or incidents with Log360. Perform log forensics using Log360's intuitive log search engine which helps to conduct root cause analysis on data breaches. It sheds light on the time and source of the breach, its impact on the data and systems, and parties responsible. You can also construct incident reports using the forensic information which needs to be submitted to the IR.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
			Analyze the root cause and the scope of a data breach using extensive records on all file and folder related activities in Windows file servers, failover clusters, and workgroup environments along with details on who accessed what, when, and where using DataSecurity Plus. Provide tamper-proof privileged session recordings and audit trails of every session as security-relevant evidence to support compliance investigations using Access Manager Plus. Configure breach notifications and get notified if a data breach is detected using Vulnerability Manager Plus. The impact of the breach along with the relevant fix will also be conveyed within the stipulated time. Monitor traffic patterns to, and detect a broad array of, external and internal security threats that may have surpassed your network firewall, and identify context-sensitive anomalies, DDoS attacks, port scans, and zero-day intrusions using NetFlow Analyzer's Advanced Security Analytics Module.

POPIA conditions	POPIA sections	What should be done?	How can ManageEngine help?
8. Data subject participation	**24.** (1) A data subject may, in the prescribed manner, request a responsible party to— (a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or (b) destroy or delete a record of personal information about the data subject that the responsible party is no longer authorized to retain in terms of section 14.	Provide data subjects the option to request for the correction or deletion of their information at anytime.	Scan entire Windows file systems at regular intervals using the DataSecurity Plus' automated file discovery feature. Find the data subject's personal data and execute batch files to delete or move them to a secure location for further processing using the data discovery feature in DataSecurity Plus. You can also locate all files pertaining to a data subject's PI using its keyword matching feature.

Other data privacy regulations which ManageEngine solutions help you comply with:

ManageEngine solutions helps comply with the following regulations, and has also provided numerous organizations with the technological support to achieve GDPR and CCPA compliance.

GDPR

A pan-European regulation that requires businesses to protect the personal data and privacy of EU citizens for the processing of their personal data. Our cloud offerings have privacy features that comply with the GDPR, and our processing of customer data adheres to the GDPR's data protection principles. ManageEngine's GDPR compliance page will help you gain a comprehensive understanding about the requirements of this mandate.

CCPA

The CCPA is a state-wide data privacy regulation which aims to protect the personal information of California residents. This regulation stresses several actions that organizations need to take to prevent personally identifiable information (PII) from falling into the wrong hands.

ManageEngine's CCPA compliance page provides an extensive look into the CCPA requisites and how organizations can comply with them.

LGPD

The LGPD is a Brazilian data protection law that will require businesses to handle the personal data of Brazilian citizens with care, or risk heavy fines. ManageEngine's AD360 and Log360 solutions will help you meet the IT security requirements of this mandate.

ManageEngine's LGPD compliance page will help you compare and contrast LGPD and GDPR mandates.

Certifications that ManageEngine products comply with:

ManageEngine solutions comply with a number of standards and certifications including:

ISO/IEC 27018

We follow guidelines for implementing measures to safeguard the personally identifiable information (PII) that is processed in a public cloud.

ISO/IEC 27001

ManageEngine has earned the most widely recognized independent international security standards, the ISO/IEC 27001:2013, for Applications, Systems, People, Technology, and Processes.

ISO/IEC 27017

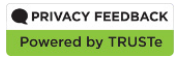
ManageEngine is certified with ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27701

ManageEngine and its solutions are fully compliant with the requirements of ISO/IEC 27701. This certification enhances the existing Information Security Management System (ISMS) and helps continually improve the Privacy Information Management System (PIMS), thereby enables us to demonstrate compliance with various privacy regulations.

SOC 2 Type II

The design and operating effectiveness of our controls meet the AICPA's Trust Services Principles criteria.



TRUSTe Review

Our processes and policies have been reviewed by TRUSTe for compliance with their program requirements for all the controls, including that of privacy.

Take control of your IT

Monitor, manage, and secure your IT infrastructure with enterprise-grade solutions built from the ground up

Unified service management

- Full-stack ITSM suite
- IT asset management with CMDB
- Knowledge base with user self-service
- Built-in and custom workflows
- Orchestration of all IT management functions
- Service management for all departments
- Reporting and analytics

Identity and access management

- Identity governance and administration
- Privileged identity and access management
- AD and Azure AD management and auditing
- SSO for on-premises and cloud apps with MFA
- Password self-service and sync
- Microsoft 365 & Exchange management and auditing
- AD & Exchange -backup and recovery
- SSH and SSL certificate management

Security information and event management

- Unified SIEM for cloud and on-premises
- AI driven user and entity behavior analytics
- Firewall log analytics
- Data leakage prevention and risk assessment
- Regulatory and privacy compliance

Unified endpoint management and security

- Desktop and mobile device management
- Patch management Endpoint device security
- OS and software deployment
- Remote monitoring and management
- Web browser security
- Monitoring and control of peripheral devices
- Endpoint data loss prevention

IT operations management and observability

- Network, server, and application performance monitoring
- Bandwidth monitoring with traffic analysis
- Network change and configuration management
- Application discovery and dependency mapping
- Cloud cost and infrastructure monitoring
- End-user experience monitoring
- AIOps

Advanced IT analytics

- Self-service IT analytics
- Data visualization and business intelligence for IT
- Hundreds of built-in reports and dashboards
- Instant, flexible report creation
- Out-of-the-box support for multiple data sources

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—over 60 products—to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers.

And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.

Trusted by


IBM


IKEA


NEC


HCL


Hallmark


ERICSSON


intel


GE


SIEMENS


Lufthansa


HONDA
The Power of Dreams


ABN·AMRO

ManageEngine

www.manageengine.com/za

ManageEngine ManageEngine ManageEngine/