ManageEngine
Log360

An IT Admin's Guide to POPIA

www.manageengine.com/log360

TABLE OF CONTENTS

What is POPIA?

The Protection of Personal Information Act (POPIA) is a regulatory mandate to be imposed on organizations in South Africa for ensuring personal data security.

The POPIA is all about lawfully collecting and processing confidential data from individuals and keeping that data always secured. It is similar to the recent General Data Protection and Regulation (GDPR) mandate.

What's considered as personal information according to POPIA?

According to the POPIA, personal information is any detail that relates to an identifiable living, natural person. This includes (but not limited to) information related to a person's:

- **Identity - race, gender, age, ethnic or social origin, and the like.**
- **Educational, financial, medical, or employment information.**
- **Contact information such as email address, physical address, telephone number, and more.**
- **Online identifier such as IP address, cookies, etc.,**
- **Biometric information.**
- **Opinion or preference.**

The POPIA also defines confidential correspondence (such as email) sent by individuals as personal information. Businesses that collect, store, and/or process such information are liable to comply with POPIA.

How POPIA affects your enterprise IT?

POPIA outlines eight conditions to ensure lawful processing of personal data. However, not all these eight conditions are of your concern. POPIA's conditions talk about:

Data Subject Participation: Adopting processes to meet the request of data subjects to delete their information on account of consent withdrawal or data inaccuracy.

Accountability: Appointing an individual who will be responsible for taking necessary action to ensure your company's compliance with POPIA.

Stating Specific Purpose: Obtaining personal information from individuals by clearly and explicitly stating the purpose for which it is being collected.

Processing Limitation: Ensuring that personal data is being processed lawfully and only with the consent of the data subject.

Information Quality: Ensuring that the collected personal information is always complete, accurate, and not misleading.

Security Safeguards: Securing the personal data against the risk of loss, unlawful access, modification, unauthorized destruction, and disclosure.

Out of these conditions, what concerns the IT department the most is the '**Security Safeguards**' condition.

How Log360 can help you meet POPIA's security safeguard condition?

Log360, the comprehensive Security Information and Event Management (SIEM) solution from ManageEngine, helps enterprise IT to safeguard the confidential information they store against data breaches.

Now, let's see how Log360's features and audit-ready report templates can meet the 'Security Safeguard' condition of POPIA.

Log360's feature	What POPIA condition does it meet?
Real-time event correlation: Log360 comes with around twenty-five correlation rules to instantly detect known attack patterns such as brute force attacks, malware attacks, SQL injection attempts, and much more. The correlation engine also tightly integrates with the threat intelligence platform of Log360. It detects and alerts security professionals when any malicious traffic tries to enter the network.	Procedure to establish and maintain appropriate safeguards against identified risks.
Real-time correlation engine: The predefined rules in the real-time correlation engine of Log360 detect and mitigate potential external threats including but not limited to: • **Suspicious malware installation** • **Suspicious SQL database access/copy** • **Malicious URL requests** • **Possible SQL injection attempts** • **Potential ransomware activities**	Procedure to identify foreseeable internal and external risks to potential information.

User entity behavior analytics (UEBA) and AD change monitoring: When it comes to internal threats, you need to closely monitor the behavior of your users and critical changes to your Active Directory (AD), that govern user accesses and authorizations. Log360's UEBA engine detects suspicious user behaviors with its unsupervised machine learning algorithms and statistical analysis. It can identify anomalous activities such as: • **Unusual volume of logon failures** • **Unusual logon activity time** • **Critical resource accessed by unusual users** • **Unusual bulk user management activities** Further, the solution also detects changes made to GPOs, ACLs, admin groups, and more, which could possibly be the start of an internal attack. Log360 not only detects these events and sends real-time email/SMS notifications when they occur, but also provides in-depth analytical reports that help investigate such incidents.	
To prevent unauthorized access or modification of personal data it is essential to continuously monitor user accesses of systems/servers where personal information is stored and detect any suspicious behavior at the initial stage.	Procedure to prevent personal data falling into unauthorized hands

File server monitoring: For personal data stored in file servers, Log360 provides information on: • **Logon failures with the reason for failure** • **Changes to file permissions** • **Changes to ACLs** • **Changes to security groups that have permission to access/modify folders that hold personal data.** **Database monitoring:** If your enterprise stores personal data in Microsoft SQL and Oracle databases, Log360 can help you detect unauthorized access of personal data by providing information on: • **Privilege abuse attempts.** • **Account lockouts** • **SQL injection attempts** By analyzing the above mentioned incidents, you can stop personal data from moving beyond your network perimeter or falling into the wrong hands.	Procedure to prevent personal data falling into unauthorized hands
Log360 sends you real-time email/SMS notifications when a file that contains personal information is copied, modified, or accessed. This solution also sends out alerts for	Process of alerting when personal information is accessed or modified without authorization

- **Selected tables**
- **Updated tables**
- **Inserted tables**

The predefined reports provide in-depth information on who performed these actions, from where, and when.

Process of alerting when personal information is accessed or modified without authorization

Log forensics: Log360 comes with an intuitive log search engine which helps you conduct a root cause analysis on data breaches and provides data including:

- **The source of the data breach**
- **When the breach occurred**
- **What hosts were affected because of the breach.**

Process to identify the source of data breach and procedure to neutralize such breach