ManageEngine
DataSecurity Plus

Complying with the **POPI Act using** DataSecurity Plus

Complying with the **POPI Act using** DataSecurity Plus

The Protection of Personal Information Act (also called the POPI Act or POPIA) is a data protection law enacted by the South African Parliament. It governs how local and foreign organizations collect, use, store, delete, and otherwise handle personal information in South Africa.

ManageEngine DataSecurity Plus helps address the requirements of the POPI Act by:

- Discovering personal information located in enterprise storage environments.
- Monitoring user activity in files containing sensitive data.
- Protecting files from accidental and malicious data leaks.
- Providing enhanced insights into security permissions and file storage.
- Streamlining POPIA audits with detailed reports.

And much more.

How DataSecurity Plus helps achieve POPIA compliance

This table lists the various sections of the POPIA that are addressed by DataSecurity Plus.

What the POPIA section says	What you should do	How DataSecurity Plus helps
Section 10 Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant, and not excessive.	Ensure that you have not collected personal information that is unneeded for your activities. The personal information you store should be processed only by those employees who require access to it to perform their job.	**Data discovery:** Locates a data subject's personal information that is stored by your organization. It then creates an inventory, allowing enforcers to ensure that only necessary data is stored. **Permission analysis:** Lists users who have access to the data along with details on what actions each user can perform on it. **ROT data analysis:** Identify old, stale, and unmodified files, and ensure that personal information is not stored beyond its intended retention period.
Section 11(4) If a data subject has objected to the processing of personal information, the responsible party may no longer process the personal information.	Find all instances of the data subject's personal information, and take necessary action to stop processing the data.	**Keyword matching:** Identifies data matching a target keyword, enabling accurate, rapid retrieval of the personal information that has to be deleted. **Response automation:** Once the keyword match is found, enforcers can automate its deletion, quarantine, or carry out a customized action to limit its use by executing batch files.
Section 14(1) Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed.	Organizations should not keep personal information for longer than needed, and should perform periodic reviews to identify and address data stored beyond its intended period.	**File analysis:** Helps build a data retention policy by finding redundant, obsolete, and trivial data in your data stores and removing the files that have exceeded their retention period.

Section 14(2) Records of personal information may be retained for periods in excess of those contemplated in subsection (14(1)) for historical, statistical, or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.	When storing sensitive personal information for extended periods of time, organizations must implement controls to ensure the security, integrity, and confidentiality of the data.	**File integrity monitoring:** Audits every successful and failed attempt to create, read, write, delete, permission change, move, rename, copy, or paste a file—in real time. Maintains a detailed audit trail for detailed analysis and proving compliance with regulatory mandates. **Data security:** Triggers instant alerts in the event of a suspiciously high volume of file changes, or if a user modifies a critical file during non-business hours. Blocks attempts to exfiltrate sensitive files via endpoints. **Effective permissions assessment:** Helps ensure the confidentiality of data by analyzing effective permissions. With this, data administrators can verify that users do not have more privileges than required for their role.
Section 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 authorized to retain the record.	Delete sensitive personal information if it reaches its limitation period, if there is no further need to process it, or if the data subject requests its deletion.	**Data discovery:** Identify the data subject's personal information stored by you using keyword matching and regular expressions, and purge them from enterprise storage. **ROT data analysis:** Identifies and automates the deletion of old files.
Section 14(6) The responsible party must restrict the processing of personal information.	Ensure that access to sensitive personal information is limited when it is under dispute, and only provide access when necessary.	**Principle of least privilege (POLP):** Tracks permission changes, lists effective permissions, identifies files that can be accessed by every employee, finds users with Full control privilege, assesses the vulnerability of files, and more, to aid in implementing POLP.

		You can generate these permission reports whenever required, or set up report delivery schedules to review file permissions periodically.
Section 15(1) Further processing of personal information must be in accordance or compatible with the purpose for which it was collected.	Deploy measures to detect and limit anomalous use of the personal information.	**Instant alerts, automated responses:** Triggers alerts when user activities in file servers, failover clusters, workgroup servers, or workstations violate the configured data handling policies. You can also execute scripts to automatically shut down computers, end-user sessions, or more.
Section 16(1) A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading, and updated where necessary.	Identify and verify the correctness of personal information stored by your organization.	**Data discovery:** Uses data discovery to find the data subject's personal information using a unique keyword set, e.g., national identification number, credit card details, email IDs, etc. Provides detailed reports on the personal information's location and the permissions assigned to it. **ROT data analysis:** Locates files older than a user-provided age, which helps in finding data that needs to be updated.
Section 17 A responsible party must maintain the documentation of all processing operations.	Track every action made to the personal information from collection to deletion.	**File change monitoring:** Audits changes made to files and folders in real time with information on who accessed what file, when, and from where. Provides detailed reports for compliance audits. Maintains a detailed audit trail for further analysis and to fulfill compliance needs.

Section 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 organizational measures to prevent— A) loss of, damage to or unauthorized destruction of personal information; and B) unlawful access to or processing of personal information.	Implement a data loss prevention (DLP) solution to prevent accidental or malicious leakage of sensitive personal information.	**Permission analysis:** Lists every user who can access a file containing personal information to verify whether they require the privilege. **Endpoint data loss prevention:** Monitors the use of removable storage devices in endpoints. Blocks the movement of sensitive files to USB devices, or via email as attachments. Prevents accidental data leaks by triggering system prompts about the risk of moving critical data. Reduces incident response times with instant alerts and an automated threat response mechanism. **Ransomware detection and response:** Identifies potential ransomware attacks and automatically shuts down infected servers, quarantines corrupted files, and limits the spread of the ransomware.
Section 19(2) 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.	Identify and assess risks to the personal information stored by you. Implement measures to mitigate the risk.	**Data risk assessment:** Calculates the risk score of files containing personal information by analyzing their permissions, volume, and type of rules violated along with audit details and more. **Endpoint data loss prevention:** Classifies business-critical files based on their sensitivity and prevents their leakage via email, USBs, printers, etc.
Section 22(2) A breach notification must take into account any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.	Forensically investigate the potential causes and extent of a data breach.	**Detailed audit trail:** Maintains a complete audit trail of every action leading up to the data breach, which aids in effectively analyzing the root cause of the breach, and the data that has been compromised.

Section 23(1) A data subject has the right to— A) request a responsible party to confirm whether the responsible party holds personal information about the data subject; and B) request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all parties who have, or have had, access to the information.	Locate and share all information about the data subject stored by your organization along with information on individuals who have accessed it.	**Data discovery:** Locates instances of personal information stored across Windows file servers and failover clusters. Scans for national identification numbers, credit card details, email IDs, and over fifty other types of sensitive personal data using preconfigured data discovery rules and policies. **Security permission analysis:** Finds who has what permission over files containing the personal information. **File access auditing:** Audits user activity in files and provides details on who accessed what file, when, and from where.
Section 24(1) A data subject may request a responsible party to correct or delete personal information about the data subject in its possession.	Locate and revise all instances of inaccurate information about the data subject. Delete the data that the data subject objects to.	**Data discovery:** Uses data discovery to find the data subject's personal information and can execute batch files to delete or move them to a secure location for further processing.
Section 26 A responsible party may not process personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behavior of a data subject, unless authorized under sections 27-31 of POPIA.	Organizations cannot collect or store the described personal information without necessary authorization.	**Data discovery:** Scans data stores for content that matches a regular expression or a keyword set. This helps organizations without the necessary authorization to detect and rectify instances of the pertinent personal information, and avoid non-compliance penalties. **Data risk assessment:** Reports on the files that contain the personal information along with details on its location, who has access to it, its risk score, and more.

DataSecurity Plus

ManageEngine DataSecurity Plus is a data visibility and security solution. It tracks and alerts on critical file modifications and movement across file servers, failover clusters, workstations, and USBs. Users can locate and analyze files containing PII, PCI, and ePHI stored in enterprise storage environments using built-in data discovery rules. Its data leak prevention (DLP) capability helps detect and respond to the exfiltration of sensitive data via USBs, email, printers, and more. It also provides detailed audit reports that help organizations streamline compliance with multiple IT regulations.

To explore these features and see DataSecurity Plus in action, launch the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore
DataSecurity Plus' solutions

File server auditing

Audit, monitor, report on, and alert on all file accesses and modifications made in your file server environment in real-time.

Learn more

Data leak prevention

Detect, disrupt, and respond to sensitive data leaks via USB deivces, emails, printers, and more through real time security monitoring.

Learn more

Data risk assessment

Perform content inspection and contextual analysis to discover sensitive data in files, and classify it based on vulnerability.

Learn more