WHITEPAPER

BEYONTRUST AND THE PROTECTION OF PERSONAL INFORMATION ACT

Building a Solid Foundation for POPIA Compliance

BeyondTrust

CONTENTS

Protection of Personal Information Act (POPIA) Overview

The Protection of Personal Information Act requires every public and private body to comply with the 8 principles that prescribe the minimum requirements for the processing of personal information in South Africa. Public and private organizations should be mindful of the rights and duties of persons to protect their personal information from processing that is not in accordance with the Protection of Personal Information Act.

The POPI Act has several objectives:

- To promote the protection of personal information processed by public and private bodies
- To introduce certain conditions to establish minimum requirements for the processing of personal information
- To provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000
- To provide for the issuing of codes of conduct
- To provide for the rights of persons regarding unsolicited electronic communications and automated decision making
- To regulate the flow of personal information across the borders of the Republic
- To provide for matters connected therewith.

Who Is Required To Comply With POPI Act?

The POPIA Act applies to everyone in South Africa who processes the personal information of any South African citizen or organization to protect personal data. This act went into effect on July 1, 2020, and all South African organizations are required to comply before the deadline on June 30th, 2021.

The Act applies to any person or organization who keeps any type of records relating to the personal information of anyone, unless those records are subject to other legislation which protects such information more stringently.

It therefore sets the minimum standards for the protection of personal information. It regulates the “processing” of personal information. “Processing” includes collecting, receiving, recording, organizing, retrieving, or using such information; or disseminating, distributing or making such personal information available.

The Act will also relate to records which are already in the possession of the entity or person doing the processing.

The POPI Act relies on 8 principles, also called conditions:

1. ***Accountability*****:** The responsible party must ensure that they comply with the conditions for lawful processing of personal information defined by the Act and that the measures undertaken to meet the requirements are also compliant.
2. ***Processing limitation*****:** Personal information may only be processed in a transparent and minimal manner, and only with the consent from the data subject.
3. ***Purpose specification*****:** Personal information can be collected and processed only for a specific and defined purpose, and records should not be retained any longer than necessary.
4. ***Further processing limitation*****:** Personal information should only be processed for the primary purpose for which it was initially collected.
5. ***Information quality*****:** The responsible party must take reasonably steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary.
6. ***Openness*****:** All data processing operations should be documented, and the data subject should be aware of which data was collected and which usage and purpose they will have.
7. ***Security safeguards*****:** The integrity and confidentiality of collected personal information must be ensured by taking appropriate technical and organizational measures.
8. ***Data subject participation*****:** Data subjects can require knowing if, where and how their personal information is held, and to require that their personal information is edited or deleted.

What are the penalties for non-compliance?

There are essentially two legal penalties or consequences for the responsible party:

1. A fine or imprisonment of between R1 million and R10 million or one to ten years in jail
2. Paying compensation to data subjects for the damage they have suffered.

In addition to the above, organizations could face:

3. Reputation damage
4. Losing customers (and employees)
5. Failing to attract new customers.

How can you comply with the POPI Act?

Organisations need to understand the requirements of the POPI Act and how these will impact processes, policies, training, technology and security around the data they gather and process. Compliance and IT teams must be proactive to ensure they will be compliant and should consider the following steps:

1. Identify What Data You Hold

Organisations need to obtain a full picture of all relevant data they hold to implement any necessary changes to ensure that they are compliant. However, with the complex hybrid IT environments today and proliferation of data across the organisation (e.g. on personal devices), this task may present a significant challenge. Organisations must be able to answer:

- Where does the data reside? The physical location of all relevant data, whether online or offline – don't forget your filing cabinets! – must be established.
- Who has access to the data? Organisations must limit the access to personal data to only employees who specifically require it for their job role.
- How is data is processed and transmitted? Within an organisation, data could be traveling in and out of network to third-party vendors and stored on a variety of servers.

2. Review Employee Training

Each employee must now be able to identify if their organisation is in violation of the POPI Act and report this to the necessary authority. This could be a data breach from an external attacker for malicious purposes, or an employee that has been granted an improper level of access to personal data.

3. Consider Your Supply Chain

Who else has access to your data in addition to your employees? This can include cloud providers, marketing agencies, and SaaS CRM, HR, and procurement applications. You must ensure that they have the necessary policies and security measures in place so you are compliant if they store or process your data.

4. Control And Monitor All Access To Your Data

Organisations need to ensure that by default personal data is not made accessible to those who do not need it, as well as manage what people who have authorized access can and can't do with the data. Give privileged users just the access they need to enforce "least privilege," and create an audit trail by logging all session activity.

How Beyondtrust Can Help Your Organization Meet POPIA Requirements

With its Universal Privilege Management approach, BeyondTrust's solutions enable businesses to control, monitor and manage access to critical systems and data, while ensuring that people remain productive and are not impeded in their day-to-day job tasks. BeyondTrust solutions allow users to access systems quickly and securely, while defending against threats related to stolen credentials, misused privileges, and unwanted remote access.

- **Enforce policy of least privilege:** Only give access to data to those who need it, when they need it, with granular levels of access controls that eliminate "all or nothing" access

- **Manage privilege 'sprawl':** Identify and secure all your privileged accounts centrally across your organisation including dormant credentials, eliminate insecure practices of employees sharing or writing down passwords, and integrate your security policies

- **Create an audit trail:** Every session and all session activity is fully recorded, creating accountability of which specific people accessed a system and what actions were taken to provide effective attribution

- **Remove all point to point pathways:** BeyondTrust's secure architecture breaks any point to point access paths into your systems with no descending connections, eliminating the need for VPNs

- **Encrypt communication:** BeyondTrust ensures all privileged access session data in transit or at rest are encrypted using TLS 1.2

- **Secure and protect all privileged accounts:** Privileged credentials are stored, rotated, and managed within a secure enterprise password vault, and privileged users are granted access based on their job roles and requirements creating a reliable privilege on-demand workflow

- **Eliminate manual password management and access controls:** Implement secure 'one-click' access to systems for privileged insiders and third parties with automated credential injection

- **Enforce data security policies to comply with POPIA:** Integrate your identity providers and security policies with BeyondTrust solutions

- **Protect personal information stored and / or accessible in Windows, Mac, Unix, Linux**: Remove excessive end user privileges and control applications on without hindering end-user productivity

Mapping POPIA with BeyondTrust solutions

Outlined below are the BeyondTrust capabilities that can help you meet a variety of POPIA standards and significantly reduce security risks related privileged accounts, users, and access.

Article summary	What BeyondTrust does
Condition 2 – Processing limitation **Section 10 and 11** 10. Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant, and not excessive. 11. Personal information may only be processed if— 11.1 the data subject or a competent person where the data subject is a child consents to the processing; 11.2 The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1)(a).	In a remote support scenario, the controller has the ability to customize information fields required to start a session during set up. A customer agreement prompt guarantees explicit consent before a session starts, and at any time the data subject is able to modify or withdraw their consent.
Condition 3 – Purpose for specification **Section 14.1** a. The responsible party must restrict processing of personal information ifits accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information; b. the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof; c. the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or d. the data subject requests to transmit the personal data into another automated processing system.	BeyondTrust enables controllers to ensure consent for processing is obtained. A customer agreement prompt guarantees consent before a session starts, and at any time the data subject is able to change their consent. The action of consent or denial is automatically recorded in BeyondTrust.
Condition 3 – Purpose Specification **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.	BeyondTrust's Endpoint Privilege management solution allows customers to implement File integrity monitoring on critical Unix and Linux assets. 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.

Condition 3 – Purpose for specification **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 authorised to retain the record in terms of subsection (1) or (2).	Anyone using BeyondTrust, whether from the technician or support rep perspective, or as a customer has the right to be forgotten. The controller can search for a specific user using the indexed search field and either remove or anonymize the user. Customizable retention policies allow an organization to choose how long and what data they need to retain in order to meet compliance.
Condition 3 – Purpose Specification **Section 14.6** The responsible party must restrict the processing of personal information.	BeyondTrust's Endpoint Privilege Management solution ensures you can implement the principle of least privilege (POLP) in a quick and easy way. We allow you to remove excessive end user privileges and control applications on without hindering end-user productivity.
Condition 5 – Information Quality **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. 2. In taking the steps referred to in subsection (1), the responsible party must have regard to the purpose for which personal information is collected or further processed.	BeyondTrust enables secure two factor authentication via RADIUS, Smart Cards, or natively, which allows users to authenticate using a device of their choice such as their mobile phone or laptop. BeyondTrust can be integrated with identity management solutions such as LDAP(s), Active Directory, or SailPoint to enable granular control over group policies. BeyondTrust offers highly granular control over user access and privileges, and all traffic runs through standard ports. Admins have the ability to set granular session permissions and configure parameters such as access time constraints and areas of access. Access can be approved as necessary. Sessions automatically terminate after the specified time is up. BeyondTrust's data at rest encryption allows organizations to use their existing key management solution to encrypt their BeyondTrust configuration, text-based session audit history, and session recordings, further ensuring that personal data is only being used when necessary.
Condition 6 – Openness **Section 18.1** Notification of data subject when collecting personal information: 18. If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of— iii) existence of the right of access to and the right to rectify the information collected.	Recorded BeyondTrust data can be retrieved as needed. Controllers can populate and retrieve information for a request based on a specific data subject.

Condition 7 – Security Safeguards **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 organisational measures to prevent— a. loss of, damage to or unauthorised destruction of personal information; and b. unlawful access to or processing of personal information. 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. The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.	BeyondTrust PAM solutions enable organizations to securely access remote devices, systems, and users. With features such as secure two factor authentication, granular permissions settings and approval processes, automatic recordings, encryption, and a choice of deployment options, BeyondTrust helps organizations to meet security standards. BeyondTrust offers highly granular control over user access and privileges, and all traffic runs through standard ports. Controllers have the ability to set granular session permissions and configure parameters such as access time constraints and network areas of access. Access can be approved on an ad hoc basis. Sessions automatically terminate after the specified time is up. Controllers have the ability to set up Jump Clients (BeyondTrust proxy) for frequently accessed systems and use existing protocols, including RDP, Vpro, SSH Telnet, SUDO, and others. All access can be automatically recorded for auditing, enabling the organization to demonstrate compliance.
Condition 7 – Security Safeguards **Section 22** 1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised 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. 2. The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.	Session activity is automatically recorded and logged and there are built in capabilities allowing users to generate comprehensive reports for analysis. BeyondTrust can also integrate with SIEM tools for advanced analysis of audit logs. Alerts can be set for misuse or suspicious activity. Preventative measures can mitigate breach risk. Sessions can be authorized on an ad hoc basis, and workflows can be configured via integrated change management tools. Access can be restricted on a granular basis. Immediate credential rotation upon session completion ensures a minimal availability of useful credentials.

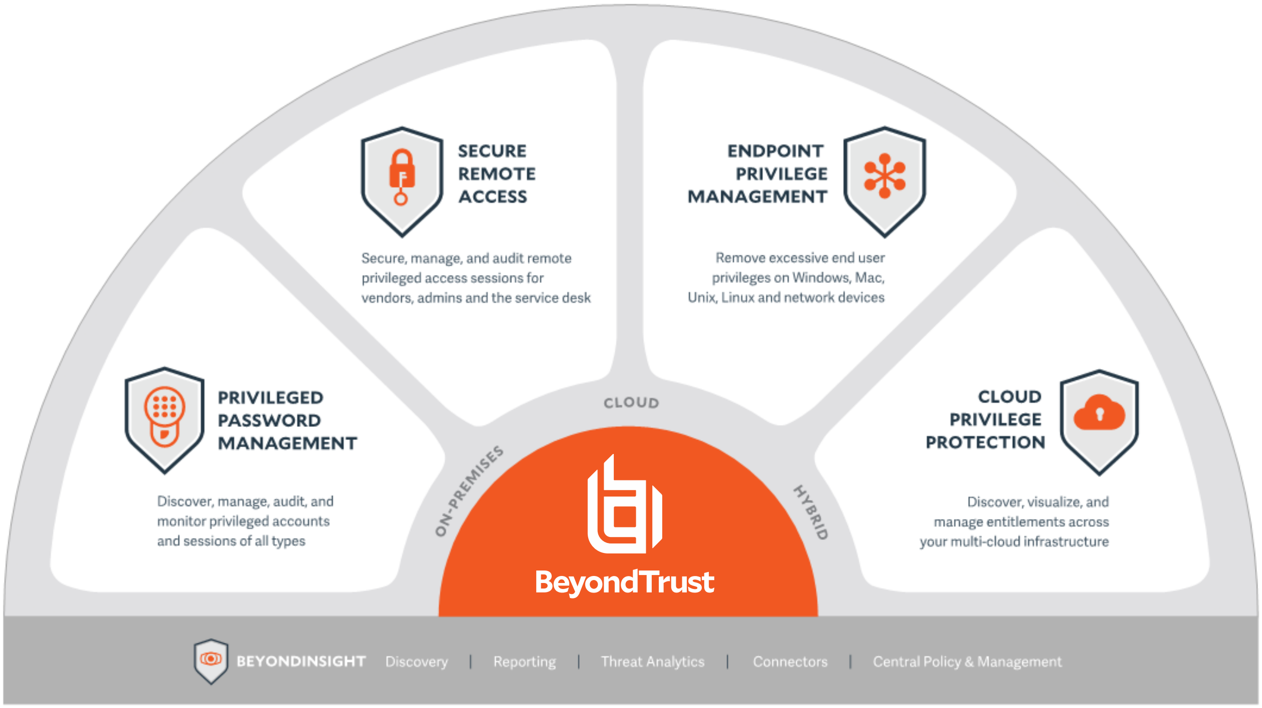
Note: *This framework is generated based on BeyondTrust software released in 2021 or later. Older versions of the software may not meet all of the compliance requirements as stated.*

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.


SECURE REMOTE ACCESS
Secure, manage, and audit remote privileged access sessions for vendors, admins and the service desk
ENDPOINT PRIVILEGE MANAGEMENT
Remove excessive end user privileges on Windows, Mac, Unix, Linux and network devices
PRIVILEGED PASSWORD MANAGEMENT
Discover, manage, audit, and monitor privileged accounts and sessions of all types
CLOUD PRIVILEGE PROTECTION
Discover, visualize, and manage entitlements across your multi-cloud infrastructure
CLOUD
ON-PREMISES
HYBRID
BeyondTrust
BEYONDINSIGHT
Discovery
Reporting
Threat Analytics
Connectors
Central Policy & Management

BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

Conclusion

The Protection Of Personal Information Act (POPIA) is one of the most important movements in the area of data protection in recent years. POPIA is a complex and wide-ranging law that has far reaching consequences and complying with this regulation will require a significant amount of work for most organisations. Building a solid cyber security foundation - that is both powerful and simple - provides a vital base on which to assemble the processes, procedures and products necessary for full POPIA compliance. The BeyondTrust PAM Platform can be quickly deployed to help your organization achieve POPIA compliance with a fast time to value and lower total cost of ownership.

Notes

- This document does not constitute a full guide to the POPI Act compliance, BeyondTrust recommends that you consult with a legal specialist in order to manage your compliance with the new regulation.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.