



# SOPHOS & POPI

## Key Points

The POPI Act sets forth 8 conditions for the lawful processing of personal information. These conditions address how organisations demonstrate accountability of ensuring they respect the privacy of individuals in South Africa.

### 8 POPI CONDITIONS:

<p><b>1</b> <b>ACCOUNTABILITY</b></p> <p>Organisation/person responsible for data compliancy.</p>	<p><b>2</b> <b>PROCESSING LIMITATION</b></p> <p>Collecting and using minimal information, with consent from data subject.</p>	<p><b>3</b> <b>PURPOSE SPECIFICATION</b></p> <p>Data collected for a specific purpose and data subject advised of purpose.</p>	<p><b>4</b> <b>FURTHER PROCESSING LIMITATION</b></p> <p>Regulates further processing of personal information collected in point 3.</p>
<p><b>5</b> <b>INFORMATION QUALITY</b></p> <p>Responsible party to ensure that collected data is complete, accurate, not misleading and up to date.</p>	<p><b>6</b> <b>OPENNESS</b></p> <p>Be open about the collection of data and purpose for data usage.</p>	<p><b>7</b> <b>SECURITY SAFEGUARDS</b></p> <p>Technical and organisational measures to ensure integrity of data.</p>	<p><b>8</b> <b>DATA SUBJECT PARTICIPATION</b></p> <p>Data subject can request confirmation of their data being stored and a description.</p>

Below is where Sophos fits in from a compliance perspective in the Security Safeguards condition:



**BOUNDARY DEFENCES**



**MALWARE PROTECTION**



**DATA ACCESS CONTROL**



**AUDIT AND LOGS**



**DATA LOSS PREVENTION**



Below is where Sophos fits in from compliance in the Security Safeguards condition:



## BOUNDARY DEFENCES

### Sophos Central

Sophos XG Firewall includes IPS, APT, antivirus, sandboxing with deep learning, and web protection to monitor and block malicious traffic from inbound or outbound access. Stops data-stealing attacks at your network perimeter.



## MALWARE PROTECTION

### Sophos Central

Sophos Intercept X, Intercept X Advanced with EDR, and Intercept X for Server modules on Sophos Central, integrate innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease.

### Sophos for Virtual Environments

Protects virtual servers and desktops from malware.



## DATA ACCESS CONTROL

### Sophos Central

- Sophos Central protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).

- Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile, store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location. Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.

- User awareness across all areas of our Sophos XG Firewall governs all firewall policies and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. XG Firewall facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.



## DATA LOSS PREVENTION

### Sophos Central

- Data Leakage Prevention (DLP) capabilities can detect credit or debit card numbers and can prevent leaks of credit and debit card details via email, uploads, and local copying.

- Sophos Intercept X keeps your endpoints secure from the latest data-stealing malware and ransomware. Sophos Central Device Encryption provides full disk encryption. Sophos XG Firewall allows for policy-based encryption for VPN tunnels, protecting data in transit.

- Sophos Mobile can enforce and monitor the encryption state of mobile devices. Our Secure Workspace app (part of Sophos Mobile) encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications.



## AUDIT AND LOGS

### All Sophos Products

Generate security event logs that can be integrated into a centralised monitoring program for incident detection and response.

### Sophos Central

- Sophos XG Firewall controls remote access authentication and user monitoring for remote access and logs all access attempts.
- Sophos Intercept X and Intercept X for Server create detailed log events for all malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process sensitive data.