Dial a Nerd
SIMPLIFYING TECHNOLOGY

Accelerating POPIA compliance with Microsoft Cloud

Providing clarity and consistency for the protection of personal data

The Protection of Personal Information Act (POPIA) imposes new rules on organizations that offer goods and services to people in South Africa (SA), or that collect and analyze data tied to SA residents, no matter where they are located.

Enhanced personal privacy rights
Increased duty for protecting data
Mandatory breach reporting
Significant penalties for non-compliance

WHAT CHANGES POPIA?

Personal Privacy
Individuals have the right to:
- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and Notifications
Processors will need to:
- Protect personal data using appropriate security practices
- Notify authorities of breaches
- Receive consent before processing personal data
- Keep records detailing data processing

Transparent Policies
Processors are required to:
- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT and Training
Processors will need:
- Train privacy personnel & employee
- Audit and update data policies
- Employ a Data Protection Officer /Compliance Officer
- Create & manage processor/vendor contracts

HOW DO I GET STARTED?

1. **Discover** Identify what personal data you have and where it resides
2. **Manage** Govern how personal data is used and accessed
3. **Protect** Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches
4. **Report** Keep required documentation, manage data requests and breach notifications

SIMPLIFY YOUR PRIVACY AND PROTECTION JOURNEY

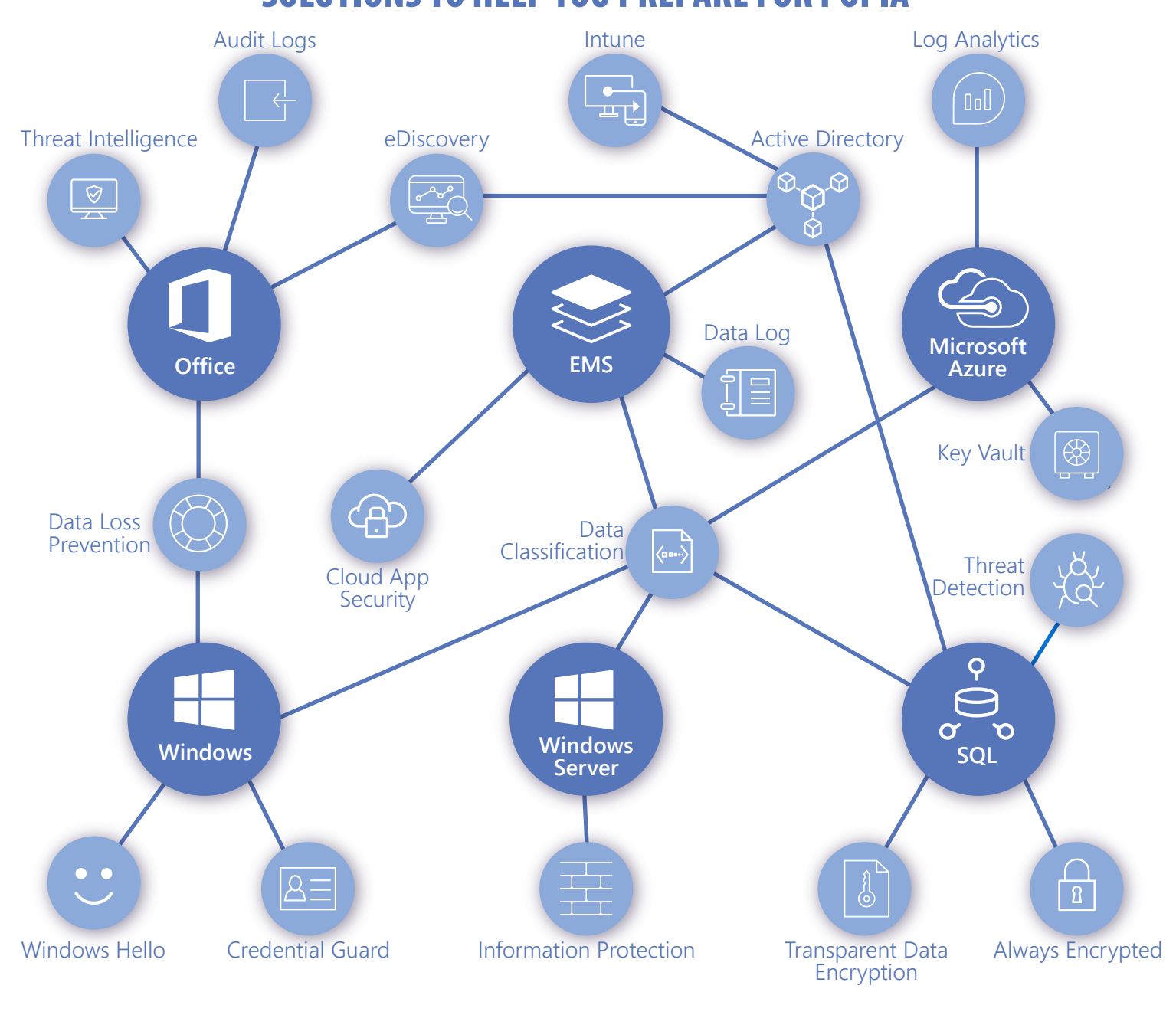
Centralize, Protect, Comply - with Microsoft 365

Process all in one place
Centralize processing in a single system, simplifying data management, governance, classification, and oversight.

Maximize your protections
Protect data with industry leading encryption and security technology that's always up-to-date and assessed by experts

Streamline your compliance
Utilize services that already comply with complex, internationally recognized standards to more easily meet new requirements, such as facilitating the requests of data subjects

SOLUTIONS TO HELP YOU PREPARE FOR POPIA



HOW DOES MICROSOFT 365 HELP TODAY?

Discover	Manage	Protect	Report
Identify personal data **Control access**	**Set retention policies** **Classify content**	**Safeguard environment** **Respond to threats**	**Record keeping** **Transparency assurance**
• Utilize eDiscovery templates to identify types of personal data.	• Use Advanced eDiscovery to export and/or delete personal data from Exchange, Sharepoint, etc.	• Protect email from today's sophisticated malware attacks with Advanced Threat Protection	• Conduct risk assessments using built-in tools in the Service Assurance Dashboard
• Easily find, classify, set policies on and manage data with Advanced Data Governance.	• Archive and preserve content across your Office 365 systems	• Prevent sensitive records fom being used by unauthorized users with data loss protectio and file encryption	• Track and repot on user activities with detailed Audit Logs
	• Automatically protect against accidental disclosure by enforcing policy on sensitive data	• Proactively uncover and protect against advanced threats and risks with Threat Intelligence and Cloud App Security	
		• Resrict access to unauthorized users based on varying factors such as risk	

OFFICE AND OFFICE 365

Secure your IT environment and achieve compliance with enterprise-grade user and administrative controls

Discover, Manage, and Protect
- Data Loss Prevention
- Advanced Data Governance
- Office 365 eDiscovery
- Threat Intelligence
- Advanced Security Management
- Office 365 Audit Logs
- Service Assurance
- Customer Lockbox

O365 - POPIA PRODUCT MAPPING

Discover Which type of data , Where data resides	Manage Access Control , Privacy by Design	Protect Data Security at rest and in transit	Report Documentation ,Breach Response
Security & Compliance Center A one-stop portal for protecting your data in Office 365. Grant permissions to people who perform compliance tasks.			
Advanced Data Governance Classify, preserve and/or purge data based on automatic analysis and policy recommendations			
Content search run very large searches across mailboxes, public folders, Office 365 Groups, Microsoft Teams, SharePoint Online sites, One Drive for Business locations, and Skype for Business conversations	**Information rights management** With SharePoint Online, control how long to retain content, to audit what people do with content, and to add barcodes or labels to documents	**Advanced Threat Protection** provides security functions that protect user environments that contain consumer data including Safe Attachments & Safe Links	**Audit Logs** record and search desired user and admin activity across your organization
eDiscovery use cases to manage access, place a hold on content locations relevant to the case, associate multiple Content Searches with the case, and export search results	**Mail Flow Rules** look for specific conditions in messages that pass through your organization and take action on them	**Secure Score** insights into your security position and what features are available to reduce risk while balancing productivity and security	**Service Assurance** deep insights for conducting risk assessments with details on Microsoft Compliance reports and transparent status of audited controls.
Advanced eDiscovery significantly reduce cost and effort to identify relevant documents & data relationships by using machine learning to train the system to intelligently explore large datasets	**Azure Rights Management** prevent sensitive information from being viewed, printed, forwarded, saved, edited, or copied by unauthorized people		**Customer Lockbox** control how a Microsoft support engineer accesses your data during a help session
	Journaling in Exchange Online respond to legal, regulatory, and compliance requirements by recording inbound and outbound email communications.	**Advanced Security Management*** gain enhanced visibility and granular security controls and policies including the ability to suspend user accounts, revoking access to personal data	**Threat Intelligence** analyze and understand the threat environment, including malware detected, targeted users, and links to global security stats
	Customer Lockbox control how a Microsoft support engineer accesses your data during a help session	**Data Loss Prevention** Unified policies covering client end-points, empowering IT pros	
		.Office365 MDM Secure devices accessing O365 resources	

ENTERPRISE MOBILITY + SECURITY

Protect customer data both in the cloud, and on-premises, with industry-leading security capabilities

Discover, Manage, and Protect
- Microsoft Cloud App Security
- Microsoft Azure Information Protection
- Microsoft Azure Active Directory (Azure AD)
- Microsoft Azure Active Directory Premium
- Microsoft Intune

MICROSOFT ENTERPRISE MOBILITY + SECURITY

	Technology	Benefit	E3	E5
Identity and access management	Azure Active Directory Premium P1	Secure single sign-on to cloud and on-premises app MFA, conditional access, and advanced security reporting	●	●
	Azure Active Directory Premium P2	Identity and access management with advanced protection for users and privileged identities		●
Managed mobile productivity	Microsoft Intune	Mobile device and app management to protect corporate apps and data on any device	●	●
Information protection	Azure Information Protection P1	Encryption for all files and storage locations Cloud-based file tracking	●	●
	Azure Information Protection P2	Intelligent classification and encryption for files shared inside and outside your organization		●
	Microsoft Cloud App Security	Enterprise-grade visibility, control, and protection for your cloud applications		●
Threat protection	Microsoft Advanced Threat Analytics	Protection from advanced targeted attacks leveraging user and entity behavioral analytics	●	●

ENTERPRISE MOBILITY SUITE - POPIA PRODUCT MAPPING

Discover Which type of data , Where data resides	Manage Access Control , Privacy by Design	Protect Data Security at rest and in transit	Report Documentation ,Breach Response
Azure AD Application Catalog Discover and maintain What type of applications users are accessing , cloud or LOB	**Azure AD RBAC & Dynamic groups** Grant access to appropriate content for appropriate personnel. Revoke access instantly	**Azure MFA** Add another layer of authentication to ensure securing identities, works with SaaS, LOB or on-premise apps	**Azure AD Advanced Reports** Sign-in attempts , Sign-in locations , application access logging, account maintenance logging
Cloud Application Security gain enhanced visibility and granular security controls and policies including the ability to block access to unmanaged cloud applications	**AAD Privileged identity management** Grant admin access for selective persons for specific amount of time	**Conditional Access** Restrict access to resources according to location , user , application or risk	**Advanced Threat Analytics** Provides breach notification and remediation for on-premise environment
Azure Information Protection Identify information types using automatic classification capabilities	**Azure Information Protection** enforcing access control policies on mails and documents	**Azure Identity Protection** advanced risk based identity protection with alerts, analysis, & remediation.	**Azure Information Protection** Reporting on documents consumption anywhere around the world
Microsoft Intune Discover mobile device applications that can compromise the device or unsanctioned by the IT	**Cloud Application Security** can use the classification labels set by AIP to enforce automatic governance actions such as quarantining files and revoking the ability to share sensitive files.	**Azure Information Protection** encrypted sensitive data across you environment from unwarranted access or use, at rest and in transit	**Microsoft Intune** Powerful device compliance reporting on wide span of device models, operating systems and vendors
		Microsoft Intune MDM, MAM and PC Management capabilities from the cloud. Intune can provide you with access to corporate applications, data and resources from almost anywhere, on any device while keeping information contained.	
		Cloud Application Security Uses machine learning and advanced DLP scanning to protect against malwares, and prevent the data from leakage outside the organization	

WINDOWS 10

Protect devices with industry-leading encryption, anti-malware technologies, and identity and access solutions

Manage
- Microsoft Data Classification Toolkit

Protect
- Windows Hello
- Windows Defender
- Advanced Threat Protection
- Device Guard
- Credential Guard
- BitLocker Drive Encryption
- Windows Information Protection
- Shielded Virtual Machines

ENTERPRISE MOBILITY SUITE - POPIA PRODUCT MAPPING

Discover Which type of data , Where data resides	Manage Access Control , Privacy by Design	Protect Data Security at rest and in transit	Report Documentation ,Breach Response
Content Search Windows Search or PowerShell to discontinue the processing of files containing personal data that are housed in local or shared storage using file permissions functionality. You can also meet the requests of data subjects to discontinue the processing of their personal data by revoking access to files that contain personal data.	**Data Governance** using Windows permissions administrators can manage and govern access to personal data.	**Strong authentication** Windows Hello replaces passwords with strong two-factor authentication, tied to a device and uses a biometric or PIN.	**Auditing and Logging** provide rich and detailed raw data that can be forwarded into other solutions for deeper analysis or compliance reporting.
	Dynamic Access Control let's you apply and enforce access-control permissions and restrictions based on defined rules that can include the sensitivity of the resources, the job or role of the user, and the configuration devices that access resources.	**Identity Protection** Credential Guard prevents credential theft attacks such as Pass-the-Hash or Pass-The-Ticket attacks by isolate secrets so that only privileged system software can access them	**Windows Defender/ ATP** helps enterprise customers to detect, investigate, and respond to advanced and targeted attacks.
	Microsoft Data Classification Toolkit identify, classify, and protect data in files servers and simplifies applying DAC	**Run trusted software** Device Guard leverages advanced hardware features to only apps authorized by your enterpriseon.	
		Protect data at rest Bitlocker helps ensure that data that is stored on a computer is not revealed if the computer is tampered with when the installed operating system is offline	
		Windows Information Protection(WIP protect data against accidental or intentional disclosure using several security measures, including encryption	
		Windows Defender/ ATP helps enterprise customers to detect, investigate, and respond to advanced and targeted attacks.	
		Threat Resistance Windows Defender Antivirus and SmartScreen help to protect against malicious files, phishing or malware websites.	

POPIA M365 TECHNOLOGY PRODUCT MAPPING

	Business Basic [1,22]	Business Stadard [1,22]	Business Premium [1,22]	F1 [2]	F3 [2]	E3 [2]	E5 [2]	Office 365 [2] F3	Office 365 [2] E1	Office 365 [2] E3	Office 365 [2] E5
USD estimated retail price per user per month (with annual commitment)	$5	$12,50	$20	$4	$10	$32	$57	$4	$8	$20	$35
Mobile Device Management (MDM) for Office 36515	●	●	●	●	●	●	●	●	●	●	●
Microsoft Intune			●	●	●	●	●				
Content Search	●	●	●	●	●	●	●	●	●	●	●
Core eDiscovery (incl. Hold and Export)			●			●	●			●	●
Advanced eDiscovery							●				●
Basic Audit	●	●	●	●	●	●	●	●	●	●	●
Advanced Audit							●				●
Apply sensitivity labels or retention labels manually17			●		● [18]	●	●	● [18]	● [18]	●	●
Apply sensitivity labels, retention labels or retention policies automatically17							●				● [19]
Apply basic org-wide or location-wide retention policies17						●	●			●	●
Apply retention policies automatically17							●				● [19]
Azure Information Protection			Premium Plan 1	Premium Plan 1	Premium Plan 1	Premium Plan 1	Premium Plan 2			AIP for 0365	AIP for 0365
Office 365 Data Loss Prevention (DLP) for emails and files			●			●	●			●	●
Communication DLP (Teams)							●				●
Basic Office Message Encryption			●		●	●	●			●	●
Advanced Office Message Encryption							●				●
Insider Risk Management							●				●
Customer Lockbox							●				●
Privileged Access Management							●				●
Office 365 Cloud App Security							●				●
Microsoft Cloud App Security							●				
Office 365 Advanced Threat Protection (ATP) Plan 1			●				●				●
Office 365 ATP Plan 2 (Office 365 ATP Plan 1 + Threat Protection)							●				●
Windows Defender Antivirus, Device Guard, Windows Information Protection, BitLocker and BitLocker To Go			●		●	●	●				
Windows Autopilot, Windows Hello for Business			●		●	●	●				
Microsoft Defender ATP							●				
Azure Advanced Threat Protection							●				
Azure Advanced Threat Analytics				●	●	●	●				

SQL SERVER

Protect the data inside your databases with controls for managing access and authorization at several levels

Discover
- SQL Query Language

Protect
- Azure SQL Database firewall
- SQL Server authentication
- Dynamic Data Masking (DDM)
- Row-Level Security (RLS)
- Transparent Data Encryption
- Always Encrypted
- Auditing for SQL Database and SQL Server audit
- SQL Database Threat Detection

SQL - POPIA PRODUCT MAPPING

Discover Which type of data , Where data resides	Manage Access Control , Privacy by Design	Protect Data Security at rest and in transit	Report Documentation ,Breach Response
Dynamic data masking (DDM) can automatically discover potentially sensitive data and suggest the appropriate masks to be applied.	**SQL Server authentication** helps you ensure that only authorized users with valid credentials can access your database server. It supports Azure Active Directory authentication.	**Azure SQL Database firewall** limits access to individual databases within your Azure SQL Database server by restricting access exclusively to authorized connections.	**Auditing for SQL Database and SQL Server audit** track database events and write them to an audit log. Auditing enables you to understand ongoing database activities, as well as analyze and investigate historical activity to identify potential threats or suspected abuse and security violations
	SQL Server authorization enables you to manage permissions according to the principle of least privilege. SQL Server and SQL Database use role-based security,	**Transparent data encryption** protects data at rest by encrypting the database, associated backups, and transaction log files at the physical storage layer Transport Layer Security (TLS) provides protection of data in transit on SQL Database connections	**SQL Database Threat Detection** detects anomalous database activities indicating potential security threats to the database. Threat Detection uses an advanced set of algorithms to continuously learn and profile application behavior, and notifies immediately upon detection of an unusual or suspicious activity
	Dynamic data masking (DDM) is a built-in capability that can be used to limit sensitive data exposure by masking the data when accessed by non-privileged users or applications.	**Always Encrypted** allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the database engine	
	Row-level security (RLS) is an additional built-in capability that enables SQL Server and SQL Database customers to implement restrictions on data row access. RLS can be used to enable fine-grained access over rows in a database table, for greater control over which users can access which data		

SQL - POPIA PRODUCT MAPPING

Discover Which type of data , Where data resides	Manage Access Control , Privacy by Design	Protect Data Security at rest and in transit	Report Documentation ,Breach Response
Azure Security Center provides you with visibility and control over the security of your Azure resources. It continuously monitors your resources, provides helpful security recommendations, and helps you prevent, detect, and respond to threats. Azure Security Center's embedded advanced analytics help you identify attacks that might otherwise go undetected.			
Azure Data Catalog Discover, understand, and consume data from different sources and databases.	**Azure AD RBAC & Dynamic groups** Grant access to appropriate content for appropriate personnel. Revoke access instantly	**Azure Key Vault** analyze and understand their local threat environment, including malware detected, targeted users, and links to global security stats	**Log Analytics** Azure provides configurable security auditing and logging options that can help you identify and repair gaps in your security policies to prevent breaches
Log Analytics Log Analytics helps you collect and analyze data generated by resources in either your cloud or on-premises environments. It provides real-time insights using integrated search and custom dashboards to readily analyze millions of records across all workloads and servers regardless of their physical location	**AAD Privileged identity management** Grant admin access for selective persons for specific amount of time	**Data Encryption in Azure Storage** automatically encrypt your data when it is written to Azure Storage using Storage Service Encryption. Additionally, you can use Azure Disk Encryption to encrypt operating systems and data disks used by virtual machines, also in transit	**Azure AD Advanced Reports** Sign-in attempts , Sign-in locations , application access logging, account maintenance logging
Azure AD Application Catalog Discover and maintain What type of applications users are accessing , cloud or LOB	**Azure Information Protection** enforcing access control policies on mails and documents	**Azure MFA** Add another layer of authentication to ensure securing identities, works with SaaS, LOB or on-premise apps	**Azure Information Protection** Reporting on documents consumption anywhere around the world
Azure Information Protection Identify information types using automatic classification capabilities		**Azure Identity Protection** advanced risk-based identity protection with alerts, analysis, & remediation.	
		Azure Information Protection encrypted sensitive data across your environment from unwarranted access or use, at rest and in transit	

Microsoft