Microsoft

Microsoft white paper on the Protection of Personal Information Act 2013 (POPIA)

Table of Contents

Executive Summary

The Protection of Personal Information Act, 2013 (POPIA) came into effect on 1 July 2020. The 12-month grace period for compliance commenced on 1 July 2020. This means that private and public bodies, and anyone else who determines the purpose of, and means for, processing personal information (responsible parties) now have until 30 June 2021 to comply with the Act's comprehensive requirements.

Microsoft commissioned this White Paper with input provided by Webber Wentzel and Cloud Essentials which aims to provide you with an overview of how POPIA will apply to processing activities and the obligations which come with POPIA and how we assist you through our solutions to meet the compliance requirements.

This White Paper sets out key provisions in POPIA but should not be read as an exhaustive summary of its provisions. Likewise, the controls detailed below should not be considered as representative of Microsoft's entire control framework. Furthermore, Microsoft's continuous development of its cloud service capabilities, combined with its focus on supporting and facilitating customers' compliance efforts, means that customers should consult their Microsoft representative for more information on available compliance technologies at the time of reading this White Paper.

What is Personal Information?

Personal information is broadly defined as information relating to an identifiable, living natural or existing juristic person. This means that the personal information of not only individuals but also juristic entities, such as companies, trusts and close corporations are regulated. The individuals and juristic persons to whom the personal information relates are referred to as "data subjects".

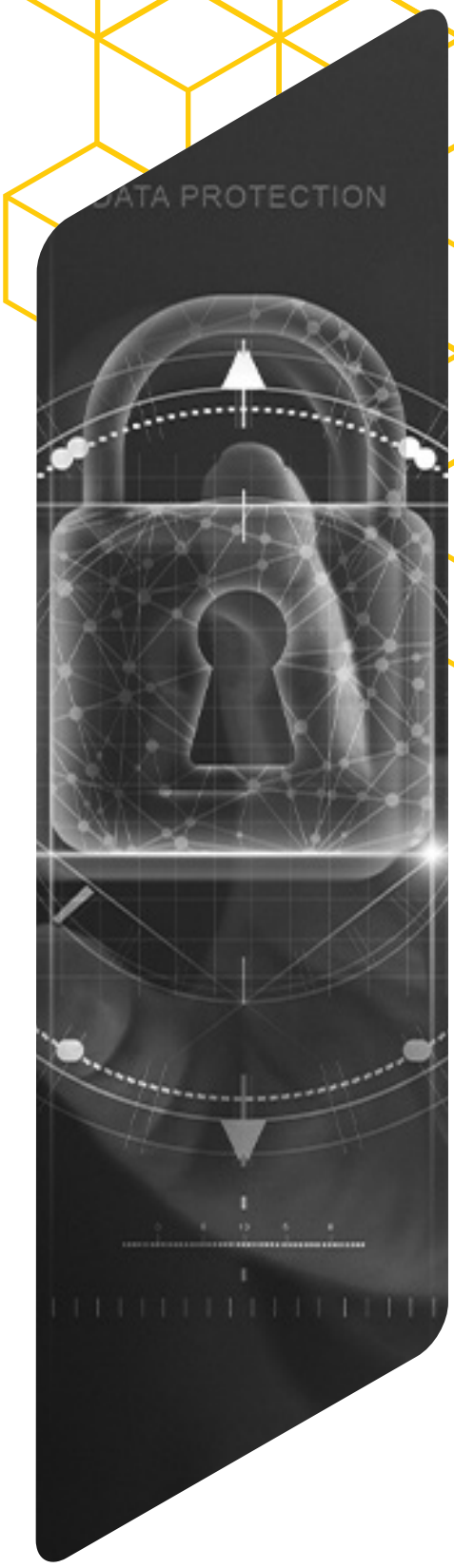
Personal information includes a wide range of information which can be used to identify a data subject and includes, amongst others, information relating to gender, age, financial or education information as well as contact information.

A sub-category of personal information referred to as "special personal information" is created and is afforded greater protection than information falling within the broader category of personal information. Special personal information includes, amongst others, information relating to religious or philosophical beliefs, race, biometric information and criminal behaviour relating to the alleged commission of an offence.

All "records" that contain personal information and that are processed will be regulated under POPIA. A "record" can refer to any recorded information, irrespective of the form or format in which the information is presented or when that record was first created. Records of personal information may include, written materials, computer generated materials, plans, drawings, photographs or film.

How is Personal Information Processed?

POPIA regulates the "processing" of personal information. Processing has a broad meaning and includes various acts that can be taken in relation to personal information. Collecting, storing, using, disseminating, marking, restricting access to, erasing or destroying personal information are all forms of "processing" personal information. Accordingly, the mere storage of personal data on the organisation's Office 365 or Azure environments will constitute processing for purposes of the Act.



Who can Process Personal Information?

There are two types of persons that process personal information - responsible parties and operators.

A "responsible party" is a person who (alone or with others) determines the purpose of and means of processing personal information. As an example, where a person manages their employees' information on their internal IT systems, that person would likely be acting as a responsible party.

An "operator", on the other hand, is a person who processes personal information for or on behalf of a responsible party in terms of a contract or mandate with that responsible party. As an example, where a person is appointed to provide payroll services to a client, they would be an operator in respect of the personal information of the client's employees.

It is not always easy to determine whether a person is acting as a responsible party or operator. A person could act as both a responsible party and an operator in respect of the same record of personal information, depending on their relationship with the data subject and how they process the personal information.

It is essential to bear in mind that Microsoft does not collect, use, maintain or share customer content on the customer's behalf. As the operator, Microsoft develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving personal information.

Microsoft's Compliance Framework

When it comes to compliance, particularly data privacy compliance, Microsoft adopts a shared responsibility approach. This model involves a division of responsibility for meeting regulatory requirements between Microsoft, as the service and platform provider, and its customers whose data is being processed within these environments.

Historically, organisations managed their own IT infrastructure on premises with data being stored and processed in local servers. Organisations therefore maintained full responsibility for the confidentiality, integrity and availability of the data they processed, and implemented a variety of controls to protect that data such as physical access controls, temperature control mechanisms, fire prevention controls and data backups. Yet, with the migration of data to its cloud environments, Microsoft has assumed a portion of that responsibility.

As the provider of Software-as-a-Service solutions such as Office 365 as well as Platform-as-a-Service and Infrastructure-as-a-Service solutions such as Azure, Microsoft is responsible for both the platforms and services provided. As such, Microsoft aims to ensure that the service and platforms meet the security, privacy, and compliance needs of its customers. Some of the controls implemented by Microsoft to achieve this objective have been detailed throughout this White Paper. By way of illustration, certain of those physical and environmental controls referenced above have been implemented at Microsoft's Azure data centres such as:

- Restricting main access to data centre facilities to a single point of entry that is manned 24x7 by security personnel;
- Ensuring that building exteriors bear no signage indicating that they are Microsoft data centres;
- Requiring physical access authorisations at either a controlled perimeter gate or secured facility door both of which requiring either access badge authorisation or security officer authorisation;
- Restricting access to the facilities' interior to approved personnel only and requiring both access card and biometric authentication;
- Restricting access to transmission media and transmission lines to protect against accidental damage, disruption, and physical tampering;
- Storing equipment in environments engineered to be protected from environmental risks; and
- Protecting data centre equipment and circuits with an uninterruptable emergency power supply system which provides a short-term power supply until generators come online and transition the load.

In addition to the physical controls, Microsoft has implemented within Office 365 systems, at the network level, logical partitions such as appropriately placed firewalls, to provide a layered defence.

Microsoft's corporate privacy program is led by its Chief Privacy Officer, supported by a team of privacy subject matter experts and overseen by Microsoft Corporate, External, and Legal Affairs. As the central program, it supports privacy efforts throughout the company, working with privacy program teams throughout the organisation to set the baseline of privacy at Microsoft. Global privacy rules and privacy requirements for the company are reviewed annually and supplemented by legal team's regular review of privacy laws, regulatory guidance, industry best practices, and other sources of interpretation to determine whether internal privacy rules and requirements need to be amended.

The Microsoft Privacy Standard provides the overarching corporate governance structure of privacy at Microsoft, and the rules for managing personal data. The Standard describes the responsibilities and activities that give effect to its privacy program and informs employees, vendors and contingent staff about privacy issues, and the consequences of non-compliance, and educates and trains employees on privacy. The Microsoft Privacy Standard is reviewed annually to ensure that company-wide privacy rules for Microsoft products and services are current and accurate and is subject to final approval by the Board.

Office 365 undergoes various audits such as ISO 27001, ISO 27018, FedRAMP, and SOC 2 Type 2 at planned intervals throughout a given year and Microsoft makes third-party independent audit reports available via the Microsoft Service Trust Portal at servicetrust.microsoft.com. Additional documentation provides detailed insights about the company's technical implementation of security, privacy, and compliance controls. Microsoft also publishes FAQs and whitepapers (like this one) on security, privacy, and compliance topics and guidance on controls that customers can implement to secure their own Office 365 tenant, and on how to use Office 365 features that support security, compliance, and privacy within their own environment.

As part of the shared responsibility model, customers retain ultimate responsibility for the data processed within their cloud environment. To this end, customers must configure their cloud tenant(s) to ensure an appropriate level of protection for their operations and must implement those controls appropriate to the organisation's specific requirements. As an example, it is recommended that customers enable multi-factor authentication for user and administrator access to their Office 365 environments.

Endpoint protection also falls within the customer's responsibility and it is incumbent on organisations to protect those devices used to access Microsoft's cloud services such as mobile phones, tablets and laptops to prevent accidental or inadvertent loss, destruction and unauthorised access.

However, not only does Microsoft implement extensive controls that contribute to its customers' compliance efforts, it has also developed a toolkit of compliance-driven capabilities to support customers' compliance efforts and which make information governance and compliance effective at scale. Furthermore, their ease of use ensures that the organisation's compliance decisions remain firmly in the hands of the information officer and the compliance team. These tools are discussed throughout this White Paper.

How is Personal Information Lawfully Processed

Responsible parties must ensure that any processing of personal information is carried out in compliance with the 8 conditions for lawful processing, summarised below.

Condition 1: Accountability:

Responsible parties must take measures to ensure compliance with the conditions for lawful processing and that these measures are in place at all relevant times.

Condition 2: Processing Limitation:

Personal information may only be processed in limited instances where a responsible party may establish a lawful basis for doing so. In addition, data subjects may freely withdraw any consent that they may have given to process their personal information, or they may object, on reasonable grounds to such processing. Responsible parties must ensure that they only collect and process information that is relevant and necessary. Personal information must be collected directly from data subjects, unless collection from another source is permitted in accordance with a few limited exceptions.

Where Microsoft processes personal information, it determines and documents the legal authority for the collection, use, maintenance, and sharing of personal information, either generally or in support of a specific program or information system need. Details of what personal data is collected, used, maintained and shared by Microsoft are included in the Microsoft Privacy Statement[1].

Condition 3: Purpose Specification:

Personal information must be collected for explicitly defined purposes. Once collected, personal information may not be retained for any longer than is necessary to achieve the purpose for which it was collected and processed, unless certain exceptions apply.

Condition 4: Further Processing Limitation:

There are limited circumstances in which a responsible party may process personal information where it deviates from the original purpose for which the personal information was collected. This may only be done where the further processing is compatible with the original purpose of collection. Typically, further processing will be compatible if (i) consent is obtained; (ii) the information is publicly available; (iii) further processing is required by operation of law; (iv) the further processing is used for historical, statistical or research purposes; or (v) the Information Regulator of South Africa (the "Information Regulator") has granted an exemption.

1 https://privacy.microsoft.com/en-US/privacystatement/

Condition 5: Information Quality:

Responsible parties must take steps to ensure that the personal information in their possession is complete, accurate, not misleading and updated when necessary. Except where required to rectify or update personal information, organisations are required to preserve the integrity of the personal information they process. In certain circumstances, this may require that personal information be rendered immutable. Microsoft's Records Management may facilitate organisations' efforts in this regard. Once declared a record, a file cannot be edited. Organisations would still be required to implement a retention policy to prevent deletion but editing would be prevented. When the record is deleted, proof of permanent deletion is provided in the Records Management portal. Where customers' data subjects have exercised their right to erasure of their personal data, this proof of permanent deletion can be provided to the user as evidence of the customer's compliance with their request.

Condition 6: Openness:

Responsible parties must, before personal information is collected or as soon as reasonably possible after it has been collected, ensure that data subjects are aware of the purpose for which the information is collected, the type of information collected and how the information will be processed (among other things). There are limited circumstances where the responsible party is not required to make the data subject aware of this information, including where: (i) the data subject has given their consent, (ii) the data subject will not be prejudiced, (iii) it is permitted by an obligation of law; or (iv) it is not reasonably practicable to make the data subject aware of this information.

Condition 7: Security Safeguards:

Responsible parties must secure the integrity and confidentiality of the personal information under their control by taking appropriate technical and organisational measures to prevent the loss, damage, destruction, unlawful access and unlawful processing of personal information. Responsible parties are required to proactively monitor internal and external risks to personal information in their possession or under their control by identifying possible risks and implementing and maintaining appropriate safeguards to address such risks. Responsible parties are also required to make notifications to data subjects and the Information Regulator where there are reasonable grounds to believe that personal information has been accessed by an unauthorised person. Ensuring the security of its systems is paramount and, to this end, Microsoft has implemented, and continually improves its Information Security Management System ("ISMS") which complies with the requirements of international standards such as ISO-27001:2002. Its ISMS also includes an Office 365 Information Security Policy which governs the security management requirements for Office 365.

- **Privacy Risk Management:**

In compliance with the risk-based approach required by POPIA, Microsoft has documented and implemented a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmission, use, and disposal of personal information and then monitors and mitigates those privacy risks. As part of this risk-based approach, Microsoft ensures that:

- Products meet certain minimum privacy requirements;
- Both customer complaints and privacy incidents are responded in a timely manner;
- All Microsoft suppliers adhere to fundamental privacy practices; and
- The company implements a process to monitor and measure its compliance with all relevant legislative statutory, regulatory, contractual requirements. In this regard, both the regulatory requirement and the organisation's approach to meeting them, are explicitly identified, documented and kept up to date for each information system and for the organisation as a whole.

In addition, Microsoft conducts a Privacy Impact Assessment on all new or changed processes involving personal information, including the design, acquisition, development, implementation, configuration, modification and management of, for example, infrastructure, systems, applications, websites, information repositories, mobile devices and other products and services. Microsoft also ensures that assessments are accepted by a senior privacy manager prior to implementation of that particular change.

Typically, organisations have focussed efforts on identifying and mitigating external threats. Yet internal risks pose as great (if not greater) a risk to the organisation's information assets since an employee's level of access to company resources is usually greater than that of an external player. To this end, Microsoft has developed Insider Risk Management as part of its Compliance Stack. The tool applies machine learning to the more than seven million daily signals received from customers' use of the Office 365 applications to identify patterns of usage that are identified as anomalous or high risk based on defined risk indicators. Insider Risk Management policies can be created using several pre-defined templates and policy conditions that define what trigger events and risk indicators are relevant to the organisation. For example, among the out-of-the-box playbooks included within the tool is that of the "Departing Employee" which enables organisations to monitor how an employee, who has given notice of termination of their employment, interacts with sensitive company data during their notice period. In this example, bulk file downloads during this period would be regarded as anomalous and potentially high risk. Defining policies requires specifying certain conditions which would trigger alerts. Conditions could include how risk indicators are used for alerts, which users are included in the policy, which services should be prioritised, and the period of time during which monitoring is to take place. Insider Risk Management automatically generates alerts where risk indicators match policy conditions and these alerts (including those alerts needing review, open alerts and alert statistics) are visualised in the Alerts dashboard.

- **Classification:**

Microsoft's Office 365 Asset Classification Standard categorises its information and information systems in accordance with applicable laws, regulations, standards, etc. Each category is designated certain minimum security and privacy requirements. All Microsoft data elements must be classified according to this asset classification system and once classified, must be protected according to the Office 365 Data Handling Standard or Office Trustworthy Computing guidance. Customer data is classified as the most restricted category of data. Microsoft also establishes, maintains, and updates an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing personal information.

Similarly, to enable customers to classify their own data in accordance with sensitivity and risk, Microsoft's Compliance stack includes Sensitivity Labels. Prior to implementing this technology, customers are encouraged to accurately define a classification taxonomy that is appropriate to their organisational and regulatory requirements. Once the taxonomy is defined, can be applied to content allowing the organisation to define the protection settings applicable to the labelled content. As with other compliance features within Microsoft 365, Sensitivity Labels are accessible within Information Protection in the Compliance Center. Sensitivity Labels enable the organisation to specify the locations to which the labels should apply, such as files, emails and/or SharePoint sites, and to stipulate the protection settings to be applied to content tagged with each label in the taxonomy, such as content markings (headers, footers, watermarks) and whether the information should be encrypted. With encryption, organisations can specify the permissions to be associated with the content, whether the file should be available offline and/or whether access rights should expire. Sensitivity labels can be applied manually or automatically or using Trainable Classifiers detailed below.

As part of the classification capabilities, Microsoft has introduced Machine-learning based classification or Trainable Classifiers. Applying labels to vast amounts of data can be extremely challenging and this functionality is key to be able to classify at scale. The organisation must invest some time in training the system to recognise the category of document that is to be labelled with a specific label. Training involves feeding the system hundreds of documents that match the classification and thereafter, providing a mix of matching and non-matching content for the system to predict matches. The trainer will then indicate false positives, false negatives, true positives and true negatives and, in this way, the system learns to recognise matching content. Once the learning process has established a level of accuracy with which the organisation is satisfied (between 95%-100%), the classifier can be published and then used to classify content at scale. Trainable classifiers can also be used for retention as discussed in more detail below.

- **Data Loss Prevention ("DLP"):**

DLP is yet another tool in the Microsoft compliance toolkit which aims to prevent the inadvertent or malicious leakage of sensitive company data, including personal information. DLP helps organisations to identify, monitor, and automatically protect sensitive information through deep content analysis. With DLP, organisations can identify sensitive data across various locations such as Exchange Online, SharePoint Online, OneDrive for Business and Teams. DLP can prevent accidental sharing by identifying a file containing personal information that is shared outside the organisation and can then automatically block access to the document or preventing the email from being sent. DLP provides continuous monitoring when content is shared using desktop applications like Word, Excel and PowerPoint. Organisations can also require that users supply a business justification to override a DLP rule. DLP reporting is available through rich visualisations within the Compliance Center and includes reports on policy matches, false positives and other helpful information. DLP includes several out-of-the-box sensitive information types (alpha-numeric strings that follow the same format such as South African identity numbers and credit card numbers) but organisations can create custom types using regular expressions. Each DLP Policy comprises several components:

- The location of the file to be protected such as SharePoint Online, Exchange Online, etc.;
- Rules to determine when and how to protect specified content;
- Conditions, namely those criteria that the content must match before the action is applied, for example, content with ID numbers shared outside the organisation;
- Actions happen automatically when content matches the conditions, for example, content with ID numbers shared outside the organisation is blocked and a notification is sent to the user and to the compliance officer.

Document fingerprinting is a DLP feature that converts a standard, commonly used form into a sensitive information type which can then be used in a DLP policy. For example, the organisation can create a blank form template which serves as the "fingerprint" and all subsequent documents based on that template will be detected and protected. A good example would be an employee onboarding form. Document Fingerprinting works with any text-based forms that are not password protected and contain all the text. Organisations can create a document fingerprint using PowerShell in the Security and Compliance Center.

- **Encryption:**

Microsoft employs a variety of encryption technology to protect customer data in transit (between the user and the data centre and between data centres) and at rest. Disk encryption and file encryption is used to protect SharePoint and OneDrive data at rest. At the disk level, Microsoft has implemented BitLocker Drive Encryption on all servers that host customer data. At the file level, each file is encrypted in conformance with AES with its own 256-bit key. For endpoint protection customers can use BitLocker, which integrates with the Windows operating system, for their own devices to protect data stored on those devices. For data in transit, for example, data transmitted via Exchange Online, Microsoft uses Transport Layer Security to encrypt the connections between Microsoft Exchange servers and the connections between the Microsoft Exchange servers and other servers such as the recipients' mail servers. Therefore, data sent through that connection is sent through an encrypted channel. However, the encryption of the channel does not mean that the actual message is encrypted. In this regard, it is recommended that customers use Microsoft Office Message Encryption when transmitting sensitive information via email for that added level of protection.

Condition 8: Data Subject Participation:

Responsible parties must ensure that data subjects are able to exercise certain rights in relation to their personal information. Data subjects must be afforded the right to access their personal information as well as the right to know who has access to or who has accessed their personal information. Furthermore, data subjects may, in certain circumstances, request that responsible parties correct or delete their personal information. Data subjects may at any time, and on reasonable grounds relating to their particular situation, object to the processing of their personal information. Once a valid objection has been received, the responsible party is no longer permitted to process the personal information of the data subject or it may be required to restrict the manner in which it processes the personal information (depending on the nature of the objection).
As documented in the Microsoft Online Services Data Protection Addendum, the features and functionality of Microsoft Online Services mean that customers remain in control of their content stored within Office 365[2]. Microsoft provides Office 365 customers with the means to enable them to fulfil their obligation to facilitate the exercise of a person's rights to access, correct and/or erase their personal information.

The Data Subject Access Request tool within Compliance Center enables customers to search across their Office 365 environment for all data containing a particular data subject's name. Alternatively, Microsoft's eDiscovery and Advanced eDiscovery capabilities can be used to detect data subject information stored within Office 365. These tools provide the organisation with search capabilities supporting much more granularity in queries, enabling specific and targeted searches. With eDiscovery, organisations can place holds on information within specified locations to prevent inadvertent or malicious destruction of key information. Using Advanced eDiscovery, organisations can analyse discovered data by applying the text analytics, machine learning, and the relevance/predictive coding capabilities to identify content that is relevant to that particular request.
The descriptions of the eight conditions above are merely illustrative and are not intended to be a comprehensive discussion on each of the requirements and obligations under POPIA. There are numerous exceptions and requirements applicable to each of the eight conditions for lawful processing.

OPERATOR CONTRACTS

Responsible parties must enter into written contracts with operators who process personal information on their behalf (which may, for example, include a cloud storage provider, IT vendor or payroll provider), in order to ensure that the operators implement appropriate technical and organisational measures to secure the integrity and confidentiality of the personal information in their possession and to prevent the loss of, damage to, unauthorised destruction of, unlawful access to or unlawful processing of personal information.

The written contract must require operators to take a proactive approach with regard to the protection of personal information. Operators must identify possible risks to the personal information in their possession, implement appropriate safeguards against those risks and constantly test these safeguards to ensure that they adequately address potential risks. Operators must immediately notify responsible parties where they suspect that the personal information of a data subject has been unlawfully accessed or acquired by a third party and the contract should regulate the manner in which such a notification is to be made.

Office 365 does not process personal information under a data processing contract for any purpose independent of the instructions of the customer. Microsoft describes the purpose(s) for which personal information is collected, used, maintained, and shared in its privacy notices and the Microsoft Online Services Privacy Statement[3]. Microsoft also notifies users of rights in their data and documents terms regarding how customers can use the service in the Online Services Terms document and program agreement. The OST is updated monthly and is available for download.

[2] https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31

3 https://www.microsoft.com/en-us/privacystatement/OnlineServices/

In compliance with this requirement for its own operators, Microsoft establishes privacy roles, responsibilities, and access requirements for all contractors and service providers. In addition, Microsoft evaluates any proposed new sharing of personal information with third parties to assess whether authorised, and whether additional or new public notice is required. By default, no one at Microsoft has access to customer data without authorisation. Subcontractors handle personal information only when required to provide or maintain a service but Microsoft does inform customers which subcontractors are used and for what purpose. Customers may download the current Office 365 Subcontractor list from Microsoft's website[4].

Security strength requirements are included, explicitly or by reference in all Microsoft's contracts for the acquisition of information systems, system components, or information system services in accordance with applicable regulatory requirements and organisational mission or business needs. Yet no dedicated information security services are outsourced to external third parties.

PERSONNEL CONTROLS

Microsoft requires all information system users (including managers, senior executives, and contractors) to take Security and Privacy Foundations training as part of their initial training and annually thereafter. In addition, Microsoft provides role-based security and privacy related training prior to authorising access to systems, when required by system changes and at least annually. The Office 365 Rules of Behavior describes Microsoft user responsibilities and establishes expected behavior when using Office 365 and other Microsoft systems. All Microsoft Users, including employees, vendors, and contractors are required to follow the Rules of Behaviour. The organisation establishes and institutionalises contact for its privacy professionals with selected groups and associations within the privacy community to facilitate ongoing privacy education and training, to maintain currency with recommended privacy practices, techniques, and technologies and to share current privacy-related information including threats, vulnerabilities, and incidents.

In addition, agreements are put in place to protect trade secrets, sensitive, or business confidential information and assets. The Non-Disclosure Agreement and Employee Handbook include statements regarding information and asset protection responsibilities. They also describe the penalties for the violation of these responsibilities.

DATA SECURITY AND BREACH NOTIFICATION

Responsible parties must notify the Information Regulator and the affected data subjects where there are reasonable grounds to believe that the personal information of data subjects have been compromised, for example where personal information is accessed or acquired by an unauthorised person. There are limited circumstances where the notification to data subjects may be delayed, including where such a notification would impede a criminal investigation.

Notifications must be made in writing and must provide enough information to allow the data subject to take proactive measures against potential consequences of the compromise.

[4] RE2JOJ1 (microsoft.com)

Microsoft's breach notification obligations are outlined in the Microsoft Online Services Data Protection Addendum[5]. This document provides that where Microsoft becomes aware of a security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data or Personal Data while processed by Microsoft, Microsoft will promptly and without undue delay notify customer, investigate the incident and provide the customer with detailed information about the incident. Furthermore, Microsoft will take all reasonable steps to mitigate the effects of the incident and to mitigate any damage that results. Microsoft also undertakes to make reasonable efforts to assist the customer in fulfilling their obligations in terms of applicable privacy law including notifying the appropriate regulator and any data subjects affected. However, customers remain ultimately responsible for addressing data breaches in accordance with POPIA and are urged to notify Microsoft as soon as possible regarding any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

At Microsoft, all personnel are required to report suspected security incidents to the organisational incident response capability. Office 365 service team personnel are required to report suspected security incidents to the Office 365 Security Incident & Response team in near real time upon discovering a suspected security incident. Microsoft then provides an organised and effective response to privacy incidents in accordance with a documented and implemented organisational Privacy Incident Response Plan.

For customers' own breach investigations, Microsoft's Advanced Audit is going to play a key role. Organisations can have visibility into many types of audited activities across a variety of different services in Microsoft 365 such as user and admin activity in SharePoint Online and Teams and Admin activity in Azure Active Directory. This is essential to determine the scope of a data breach as it provides vital information such as when emails were accessed, sent, replied to or forwarded. Advanced Audit applies a default audit log retention policy of one year to audit records but extending this for longer periods is key for compliance investigations and to demonstrate the organisations compliance with the provisions of POPIA.

INFORMATION OFFICERS

An information officer is the person who is responsible for overseeing a responsible party's compliance with the provisions of POPIA. Information officers will often be the point of contact for all matters related to POPIA.

It should be noted that all companies that process personal information must appoint an information officer, irrespective of the size of the company or the amount of information it processes. In private companies, the information officer will automatically be the head of the private organization (i.e. the CEO of the company) or equivalent officer of the juristic person or any person duly authorised by that officer; or the person who is acting as such or any person duly authorised by such acting person. A responsible party may also appoint deputy information officers to assist the information officers with the discharging of their obligations.

Microsoft appoints a Senior Agency Official for Privacy/Chief Privacy Officer to be accountable for development, implementation and maintenance of the organisation-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information by programs and information systems. Microsoft's legal team identifies and reviews privacy-relevant laws, regulations and other standards and identifies areas where Microsoft policies and procedures must be updated. Microsoft ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy and its Chief Privacy Officer.

[5] Licensing Terms | Microsoft Volume Licensing

PROCESSING JUSTIFICATIONS

Responsible parties may only process personal information where they have a lawful basis to do so. Specifically, a responsible party may only process personal information where;

- the data subject (or a competent person, where the data subject is a child) consents to the processing;
- processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
- processing complies with an obligation imposed by law;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary for pursuing the legitimate interests of the responsible party or a third party to whom the information is supplied.

PRIVACY NOTICES

Responsible parties are required, before the collection of personal information or as soon as reasonably practicable after the information is collected, to ensure that data subjects are aware of:

- the fact that their personal information is being collected;
- the source from which it was collected;
- the purpose for which it was collected;
- whether the personal information will be transferred to a third country or international organisation and the level of protection afforded by such third country or international organisation; and
- the data subject's rights to access or rectify personal information and the right to object to the processing of personal information.

Responsible parties may bring the above to the attention of data subjects in a number of ways, including by way of publishing a privacy notice on their website (if applicable) at the point of collection.

Where a responsible party intends to collect the same information once again or information of the same kind for the same purpose as the original purpose of collection, the responsible party will not need to once again take steps to ensure the data subject is made aware of the above.

Microsoft incorporates in the Microsoft Online Services Privacy Statement, referred to above, details of what personal data it collects, uses, maintains and shares6. The Statement also outlines how personal data is used and for what reason. Users are provided guidance on how to access and control their own data and gain insights into privacy information relating to specific Microsoft products and services. Finally, the Privacy Statement includes a link to contact Microsoft with privacy queries, concerns or complaints[7].

[6] https://privacy.microsoft.com/en-US/privacystatement/

[7] https://go.microsoft.com/fwlink/p/?linkid=2126612

TRANSBORDER INFORMATION FLOWS

Personal Information may only be transferred outside of South Africa in limited instances. Responsible parties may not transfer the personal information of a data subject to a third party in a foreign country unless:

- the third party receiving the personal information is subject to a law, binding corporate rules or a binding agreement which provides an adequate level of protection that:
  - effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information; and
  - includes provisions that are substantially similar to the provisions of POPIA relating to the trans-border transfer of personal information;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- the transfer is for the benefit of the data subject, and
  - it is not reasonably practicable to obtain the consent of the data subject for the transfer; and
  - if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

Responsible parties will be required to obtain the prior authorisation of the Information Regulator where the responsible party intends to transfer the special personal information of data subjects or the personal information of minors to a third party in a foreign country that does not provide an adequate level of protection. Most customer data is stored and processed by Microsoft in data centres within the locational proximity of the customer. However, Microsoft contractually regulates and specifies the geographic regions in which particular cloud services are delivered. This allows for a transparent understanding of data location and supports a customer's compliance requirements to map where its data is stored and assess adequacy or related compliance obligations. In 2019, two data centre regions were launched by Microsoft in South Africa. Microsoft has adopted the EU Standard Contractual Clauses that provide additional contractual guarantees around transfers of personal data for in-scope cloud services. It is key to remember, however, that Microsoft will not transfer customer data to any third party (not even for storage purposes.

RECORD RETENTION

Responsible parties may not retain records of personal information for any longer than is necessary to achieve the purpose for which the information was collected. There are certain circumstances in which a responsible party may retain records of personal information for periods longer than is necessary to achieve the intended purpose, including:

- where retention is required by law;
- retention is required for lawful purposes related to the responsible party's functions or activities;
- retention is required by a contract between the responsible party and the data subject;
- the data subject has consented to the extended retention; or
- where the record of personal information has been used to make a decision about the data subject, the responsible party will be entitled to retain the record for such period as may be required or prescribed by law or a code of conduct, and where there is no applicable law or code of conduct, for a period which will allow the data subject a reasonable opportunity to access the information.

Records of personal information may be further retained in excess of those periods discussed above, where the personal information is used for historical, statistical or research purposes. Once a responsible party is no longer entitled to retain personal information, the responsible party must destroy, delete or de-identify the personal information in a manner that prevents its reconstruction in an intelligible or workable form.

[6] https://privacy.microsoft.com/en-US/privacystatement/

[7] https://go.microsoft.com/fwlink/p/?linkid=2126612

To facilitate compliance with this particular requirement, it is recommended that customers leverage Microsoft's Information Governance capabilities. Retention capabilities within Information Governance in Compliance Center can be used to preserve content whilst the organisation can lawfully retain that content and to delete it when retention is no longer lawful. Retention policies and labels enable organisations to retain data for a specific period after which content can be deleted or a disposition review can be triggered. In the latter case, at the end of the retention period, a review request is sent to a designated reviewer who can then choose whether to extend retention or to delete the data. Organisations can also choose not to retain content but to automatically delete it after a specific period. In this instance, manual deletion can take place prior to the specified deletion date. Retention policies are typically applied to locations such as SharePoint sites and Exchange Mailboxes whereas labels are applied at the file level. The two do have slightly different capabilities and it is therefore recommended that organisations properly plan their information management strategy before implementing the technology. Retention policies can also be applied automatically to all files containing certain specified sensitive information types which are discussed above.

COMPLIANCE MANAGER

Compliance professionals are encouraged to manage their POPIA compliance using Microsoft's Compliance Manager, an online compliance management tool within Compliance Center. Within the tool, Microsoft's compliance framework has been mapped against several laws, regulations and standards issued around the world, including POPIA. With the tool, customers can gain visibility into those controls Microsoft has implemented to protect its customers' data, some of which have been outlined above. Organisations can also use the tool to record implementation of their own controls as required by POPIA and other laws. As a compliance management tool, Compliance Manager allows users to assign responsibility for control implementation to other users within their organisation and sends a notification to those users that the task has been assigned. Where users undergo internal or external audits, audit findings and reports can be recorded and uploaded into the tool where they are kept securely should they be required by customers or regulators. Compliance Manager also provides invaluable guidance to customers on how to leverage Microsoft's technical capabilities to meet their POPIA requirements.