CLOUD CHECKLIST FOR SOUTH AFRICA - GENERAL REGULATORY POSITION*

Source	Compliance Obligation	Microsoft Commitments	Azure	Dynamics 365	Office 365
Protection of Personal Information Act 4 of 2013 (POPIA) POPIA, which is expected to become effective soon, will regulate the collection, use and processing of personal data. Under POPIA, Microsoft will likely be considered an "operator", and each customer the "responsible party".	Secure integrity and confidentiality of personal information by taking appropriate reasonable technical and organisational measures to protect personal information from loss, damage, unauthorised destruction and unlawful access and processing. To give effect to this, take reasonable measures to (a) identify reasonably foreseeable internal and external risks, (b) establish and maintain appropriate safeguards against such risks; (c) regularly verify that safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated to address new risks and deficiencies; having due regard to generally accepted information security practices which apply generally or are required for a specific industry (s19).	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, availability, and integrity. Microsoft adheres to numerous internationally recognised standards addressing information security and privacy which can help the customer comply with their legal requirements. Microsoft offers many widely-recognized certifications, third party attestations and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements.	✓	✓	✓
	Operator must (i) process personal information only with the knowledge or authorisation of the responsible party and (ii) treat personal information as confidential and must not disclose it, unless required by law or in the course of proper performance of its duties (s20).	Microsoft specifically undertakes and agrees with its customers to only process personal information under authority of its customer. Microsoft also contractually commits not to disclose personal information unless legally compelled to do so.	✓	✓	✓
	Operator must notify the responsible party immediately where there are reasonable grounds to believe that personal information has been accessed or acquired by any unauthorised person (s22), thereby facilitating the responsible party's notification obligations.	Microsoft undertakes to promptly notify its customers of any data breach, including unauthorised access resulting in loss, destruction, disclosure or alteration.	✓	✓	✓
	Responsible party may not transfer personal information to a third party outside of South Africa save in specific circumstances (s72).	Microsoft holds itself accountable to and is subject to laws of general application applicable to information technology service providers and has binding agreements which, in its view, provide adequate protection.	✓	✓	✓
	Responsible party must be able to comply with requests for access, correction and and/or destruction of personal information.	Microsoft acknowledges the customer as exclusive owner of its data. A customer accordingly has complete control over its data in the Microsoft cloud and is able to address any requests for access, correction or destruction. In this way, Microsoft can help the customer comply with its legal requirements.	✓	✓	✓
	Retention of records for no longer than is necessary (s14(1)).	Microsoft acknowledges the customer as the exclusive owner of its data. A customer accordingly has complete control over its data in the Microsoft cloud and is able to address and comply with its own policies as regards retention and deletion. In this way, Microsoft can help the customer comply with its legal requirements.	✓	✓	✓
	Destruction or deletion in a manner that prevents its reconstruction in intelligible form (s14(5))	Microsoft acknowledges the customer as exclusive owner of its data. The customer accordingly has complete control over its data in the Microsoft cloud and is able to address and comply with its own policies as regards destruction and deletion. The customer determines and may set policy as to when its data is deleted. When a customer leaves the services and does not migrate its data, that data is deleted by Microsoft in accordance with agreed time periods (at the latest 180 days after leaving the service). Deletion of data is in accordance with industry standards. If a disk drive used for storage fails, it is securely erased or destroyed before return to the manufacturer for replacement or repair. Data on failed equipment is overwritten to prevent recoverability by any means.	✓	✓	✓

Source	Compliance Obligation	Microsoft Commitments	Azure	Dynamics 365	Office 365
		When devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation			
Electronic Communications and Transactions Act 25 of 2002 (ECTA)	Cryptography products and services, important for security of information, may only be provided by a duly registered cryptography provider.	Microsoft has registered and retains ongoing requisite registrations under ECTA for the cryptography technology used in its products and services.	✓	✓	✓