


Public Sector Cloud Computing Determination and Directive


On 2 February 2022, the Department of Public Service and Administration released the Public Service Cloud Computing Determination and Directive Awareness notice to all Heads of National and Provincial Departments.

The purpose of the Determination and Directive was to provide clear guidance to public service departments on adopting and using Cloud Computing services and technologies. The prescripts set out in the Determination and Directive are to be applied to all cloud services; where government data is either stored or processed. We have extracted some of the key principles below:







The determination must be applied to **every cloud service**.




Where a department had implemented a cloud solution before the approval date of this Directive, **a risk assessment is conducted** and a risk assessment report is tabled at the departmental risk committee.




All requirements of the determination are **met within 6 months**. Failure to comply with the determination will be dealt with in terms of the Public Service Act, 1994, section 16A and 16B.




The Head of Department must **ensure that cloud services are the first option explored** before any on-premise infrastructure investment is made. **This option must be fit for purpose, and preference (not exclusive use) must be given to private government cloud** where the capability exists.




The Head of Department must **ensure that the proper procurement processes** concerning the procurement of ICT goods and services/ cloud are followed.




The Head of Department must ensure that **all data is classified according to the classification system prescribed in the Minimum Information Security Standards (MISS)**.




The Head of Department **must ensure that data always resides within the borders of South Africa. Where such is not practically possible, the Head of Departments must ensure that provisions of section 72 of the POPI Act are complied with.**




The Head of Department **must ensure that a comprehensive risk assessment is undertaken for each cloud service that the department intends to utilise.**



The Head of Department must ensure that **a Cloud Readiness Assessment is conducted before the decision is made to move to cloud-based computing services**. The Cloud Readiness Assessment checklist (Appendix A) can be used to guide departments.




The Head of Department must ensure that a **business case is developed**.




The Head of Department must ensure that a **valid contract exists between the department and the CSP before utilising a cloud service which must include the following:**


- Make **provisions for the safe return/transfer of data** should the cloud service provider be the subject of a takeover.
- Specify **what will happen to the data**, applications, infrastructure, etc., (e.g. transfer to a new provider, returned to the department, permanently deleted) **once the contract ends**.
- Define contract provisions relating **to the migration of data on termination of the contract** (i.e. CSP takes full responsibility for data migration and or who plays what role during data migration).



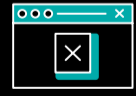
The Head of Department **must ensure the security of the data in line with the existing departmental information security policy.**




The Head of Department **must ensure that access rights to data stored or processed in the cloud are regularly reviewed.**



The Head of Department **must ensure that an inventory of assets (data or applications) is developed and maintained during the contract period.**



The Head of Department **must ensure that the department's business continuity plans are updated** following the implementation of the cloud service and ensure that the department conducts **regular business continuity testing**.



The Head of Department **must ensure that mechanisms exist to backup departmental data**. Backups of data must be regularly reviewed to ensure that the risk of data loss is minimised.



Should you require a more detailed discussion on any of the aspects contained in the Determination and Directive, please do not hesitate to contact Leishen Pillay – Deloitte Africa Data Privacy Leader (lpillay@deloitte.co.za) for more information.