WA Government data offshoring position and guidance

Cloud Policy Fact Sheet 1.2

Due to the off-premise nature of cloud computing, it is common for services to be offered worldwide via the internet—often from storage locations and servers in different countries. Under this position, the act of moving data to, creating it within, or storing it in a location outside of the Commonwealth of Australia is known as “offshoring”.

In many cases, the specific location of the offshored data in question may not be clear at any given time. Often it may be stored in multiple locations to guard against data loss. This is the case for a wide range of web services, including commonly used examples such as Dropbox, SurveyMonkey, SalesForce and Google Photos.

Even where offshored data is held very securely, its mere existence in foreign jurisdictions means that it is subject to different laws to Australia—which gives rise to potential legal access, security and privacy concerns, especially for personally sensitive information.

Western Australia does not currently have a legislative position on privacy and a whole-of-government data classification scheme. Agencies risk based decision making processes in the data space are therefore at a low level of maturity. As a results, agencies do not have the capability and capacity to adequately evaluate and determine protections for potentially sensitive data. If agencies are not confident in their own determinations, they will not be able to adequately manage and monitor security and privacy standards in their cloud service partners.

In this context, it is important that Western Australian public sector agencies give strong care and consideration to the nature of their data, and where it will be stored.

The Data Offshoring Position for the Western Australian Public Sector provides preliminary guidance for the sector, pending a more comprehensive approach (encompassing data classification, privacy and security) which are yet to be developed.

Offshoring Position

*The Western Australian Government’s Position on Offshoring is that agencies may offshore data—but only following a comprehensive and rigorous risk assessment process, and written endorsement from their Director General or Chief Executive Officer for each business case.*

*If agencies are not able to establish the sensitivity and potential risks of offshoring, and confidently manage the behaviour of their offshore partners, they should not proceed with offshoring of data.*

*As formalised definitions for classification of data (a data classification system) does not yet exist for the Western Australian public sector, agencies should use existing terminology from their risk assessment processes. This includes categories such as “cabinet in confidence”, “commercial in confidence”, “legally privilege”, and “sensitive information”.*

*Privacy is an especially important concern in offshoring of data. Until more comprehensive requirements and guidance for privacy in the Western Australian public sector are available, agencies must apply the Australian Privacy Principles as a mandatory minimum. This includes a definition of “sensitive information”, as defined in the Guidelines to the Australian Privacy Principles[[1]](#footnote-1).*

*This Position applies in addition to, and does not alter requirements under, the State Records Act 2000. Any other legal requirements relating to agency data are also undiminished by the Position.*

*If an agency offshores any of its data, it must actively monitor and manage the handling of that data by the vendor or responsible party, to ensure record-keeping obligations are met and all risks mitigated.*

This Position is further clarified in the headings below.

*State Records Act*

The *State Records Act 2000 (WA)* requires that agencies “undertake appropriate risk assessments of data” before selecting storage or data centres of any kind.

Unlike traditional procurement and consumption models where products are customised according to the agency’s needs, providers of offshoring services have standard contracts and service level agreements which are not open to variation. Therefore, it cannot be assumed that these cloud service providers will automatically meet your obligations.

*Privacy*

Lack of public trust in Government will hinder the uptake (and commensurate benefits) of better data-driven services, and sound privacy is a key component in building and maintaining that trust.

Western Australia is one of the last jurisdictions in Australia without legislative provisions relating to privacy, a fact highlighted with concern in the interim report of the Service Priority Review.

Until a more comprehensive legislative approach to privacy is available, the Western Australian public sector’s Interim Privacy Position is to adopt the existing Policy Framework and Standards for Information Sharing Between Government Agencies (the Framework). [[2]](#footnote-2) This is administered by the Department of Justice, and mandatory under Public Sector Commissioner’s Circular 2014/02.

The Framework requires information sharing by agencies to be consistent with appropriate minimum privacy standards, such as the Australian Privacy Principles.

*Personal and Sensitive Information*

The APP are established under the *Privacy Act 1988 (Cth)* as a baseline standard for a wide range of entities, including all Australian Government agencies, to protect the security and privacy of individuals’ information.

Not all information handled by Government agencies is sensitive, or likely to give rise to significant privacy and security concerns. In order to protect the data that is, without unduly restricting use of offshore services, the Western Australian Data Offshoring Position adopts the APP distinction between personal information and sensitive information.

“Sensitive information” is a subset of “personal information”, defined in the APP as follows:

B.138 ‘Sensitive information’ is a subset of personal information and is defined as:

* information or an opinion (that is also personal information) about an individual’s:
  + racial or ethnic origin
  + political opinions
  + membership of a political association
  + religious beliefs or affiliations
  + philosophical beliefs
  + membership of a professional or trade association
  + membership of a trade union
  + sexual orientation or practices, or
  + criminal record
* health information about an individual (see paragraphs B.74–B.78)
* genetic information (that is not otherwise health information)
* biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
* biometric templates (s 6(1)).

Source: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#sensitive-information>

*Data Classification*

Data classification is a business process by which data is assessed and labelled (where appropriate) according to the potential impact of its release. Data determined to be more sensitive (according to defined criteria) typically requires different treatment and handling.

A sector-wide data classification system is an effective way of determining offshoring requirements for data. As the Western Australian public sector does not yet have a data classification system in place, the Position adopts the APP definition of “sensitive information” as it is the simplest commonly understood framework to protect the most critical personal data in the WA public sector.

Data not captured in the APP definition, but to which an agency assigns higher sensitivity for other reasons, should not be offshored.

*Other Jurisdictions*

The Western Australian offshoring position adopts a similar standard for offshoring in other jurisdictions.

The Commonwealth, New South Wales, Victoria and Queensland all have legislative frameworks for information security and privacy. In these jurisdictions, CLASSIFIED data (typically national security-related) cannot be offshored. However, other data (including sensitive and personal data) may be—provided it is subject to rigorous risk assessment, and the agency can reasonably ensure that record keeping and privacy requirements for the data are being met.

Useful tools

[State Records Office of Western Australia. State Records Act 2000](http://www.sro.wa.gov.au/state-recordkeeping/legislative-requirements/state-records-act-2000)

[Australian Government, *Questions to ask about a cloud service*](https://www.communications.gov.au/sites/g/files/net301/f/questionstoaskyourprovider.pdf) (Department of Communications).

[Federal Australian Privacy Principles](https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles)

[Office of Digital Government, Open Data Policy, July 2015.](https://gcio.wa.gov.au/2015/07/03/open-data-policy/)

[Office of Digital Government, Digital Security Policy, June 2017.](https://gcio.wa.gov.au/2016/05/25/digital-security-policy/)

[Office of Digital Government, ICT Disaster Recovery for Business Continuity Policy, April 2017.](https://gcio.wa.gov.au/2016/05/25/ict-disaster-recovery-for-business-continuity-policy/)

1. <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#sensitive-information> [↑](#footnote-ref-1)
2. [Department of Justice, 2017, Policy Framework and Standards](http://www.department.dotag.wa.gov.au/_files/info_sharing_policy.pdf) [↑](#footnote-ref-2)