Our ref: SRO/2019/052

Department of
Local Government, Sport
and Cultural Industries

GOVERNMENT OF
WESTERN AUSTRALIA

**DEPARTMENT OF LOCAL GOVERNMENT, SPORT AND CULTURAL INDUSTRIES / CULTURE AND ARTS PORTFOLIO AGENCIES SUBMISSION ON PRIVACY AND RESPONSIBLE INFORMATION SHARING**

This submission is made jointly by the Department of Local Government, Sport and Cultural Industries (DLGSC); and the culture and arts portfolio agencies: State Library of WA (SLWA), Art Gallery of WA, Perth Theatre Trust, State Records Office (SRO) and the WA Museum.

The submission addresses emerging policy positions and threshold issues considered at recent public sector engagement workshops conducted by the Department of the Premier and Cabinet (DPC). Recommendations are highlighted in ***bold and italics*** for consideration by the DPC.

The DLGSC and portfolio agencies support the broad intent, principles and approach set-out in the discussion paper and discussed through recent consultation. Comments and recommendations made in this submission are intended to contribute to strengthening and clarifying some aspects of the proposed approach.

**Access and Correction**

It has been observed that the proposed legislation may provide an additional and alternative pathway to Freedom of Information (FOI) for individuals to access and correct their personal information held by government agencies. However, it is not yet clear to the DLGSC and portfolio agencies what this pathway may be, how it would operate, or the value it would add for community. Part 3 of the *Freedom of Information Act 1992* allows members of the public to access and amend their personal information. These provisions were included because no privacy legislation was enacted at the time. Having two mechanisms for people to access and amend personal information is likely to cause confusion as to which process agencies should direct their customers to use.

It is noted that agencies are reluctant to provide access to documents containing personal information outside a legal framework. This is because personal information is often intertwined with information about third parties (both personal and business related). If requests for access to and the correction of personal information are to be processed under privacy legislation, there should be clear instructions on how to deal with those types of cases. Provisions for third party consultation are also necessary.

There needs to be clarity around which legislation prevails regarding the release of information. Some existing legislation includes provision for the protection of certain information related to investigations; and it is unclear at this stage how the proposed legislation may impact existing provisions. Consideration should be given to potential conflicts between the objectives of a Privacy Commissioner and the Information Commissioner.

The DLGSC and portfolio agencies note there are already methods to access and correct personal information outside FOI e.g. updating license details or contacting agencies directly regarding updates to customer details, and the ability for debtors/creditors to seek access to financial data such as outstanding invoices or payments. The DLGSC and portfolio agencies are not aware of any mapping of these existing channels that may inform decision making about how to manage and communicate new pathways to FOI created through the proposed legislation.

***It is recommended that:***

- ***clear guidance for both the public sector and the general public is developed on the scope and operation of any additional and/or alternative pathways to the existing FOI process resulting from implementation of the proposed legislation. The definition of "Personal information" in the two acts (FOI and proposed) should also align; and***
- ***existing alternative pathways to FOI and any potential new pathways to FOI likely to be created through the proposed legislation are mapped to facilitate opportunities to streamline processes across agencies, and specific consideration is given to the right to personal privacy and anonymity.***

As an example, the SLWA supports the right of the individual to use SLWA facilities and services with anonymity if they choose to do so, like other libraries throughout Australia and the world. The International Federation of Library Associations Statement on Libraries and Intellectual Freedom states that "Library users shall have the right to personal privacy and anonymity." Further, the Australian Library and Information Association Free Access to Information Statement states that "library and information services have particular responsibilities in supporting and sustaining the free flow of information and ideas including; protecting the confidential relationships that exist between the library and information service and its clients."

**Working with the Five Safes (Information Sharing Arrangements)**

In principle, the DLGSC and portfolio agencies are supportive of the Five Safes Framework (Framework) being uniformly implemented across the sector. It is critical that this Framework is applied consistently through whole-of-government policy; and appropriately supported by information sharing systems and infrastructure across government to ensure the integrity of information.

As an example, the SLWA and SRO collect, store and make accessible the records of Western Australians both living and dead. These records may have been collected through transfer to the State archive collection, or to other collections via donation or purchase directly from the person, descendants of that person or organisations and businesses that have collected this information. Some of this information is sensitive and there are access restrictions placed upon the materials. Any privacy legislation should consider existing access agreements to this type of information.

Implementing the Framework will have implications for a wide range of information management practices. For example, in relation to retention and disposal of documents created by one agency, but in the possession of another. These may be best addressed through practice and consideration could be given to how existing forums between agencies might be used to share experience and lessons learned; and whether a new forum may be needed – perhaps supported by the proposed Chief Data Officer (CDO).

Consideration should also be given to regular measurement of progress and effectiveness of this Framework, potentially captured through existing reporting means, such as the Public Sector Entity Survey.

***It is recommended that:***

- ***supporting guidance material, including a broad definition of key terms and worked examples be developed in consultation with agencies; and that appropriate training be conducted across the sector to encourage consistent application of the Framework; and***
- ***a pilot of the Five Safes Framework is implemented by several agencies to help develop guidance and training material; and that lessons learned from this pilot are communicated with other agencies to support broader implementation.***

**The Role of the Chief Data Officer**

The DLGSC and portfolio agencies support the role of a CDO to provide information sharing governance, assist agencies in uplifting their data analytics capabilities and to provide advice on information risk assessed against the Framework.

There is no clear consensus across the DLGSC service areas and portfolio agencies as to whether a CDO should have the power to compel the sharing of information between agencies. Supporting arguments are that this power might help resolve uncertainty regarding information sharing in a timelier manner than leaving resolution to agencies; and that this function would enable the CDO to maintain awareness of any recurrent issues that could be resolved through improved guidance to agencies. A potential issue with the power to compel agencies is that agencies may, to some extent, come to rely on this function to resolve issues that are better addressed directly by the agencies concerned to develop a culture of improved information sharing over time. Some service areas at the DLGSC have also expressed a concern about liability for adverse outcomes should they be compelled to share sensitive information by the CDO. A set of defined clearly defined exemptions from information sharing may be helpful, for example, criminal investigations. Consideration should be given to potential conflicts between the objectives of a CDO, a Privacy Commissioner and the Information Commissioner.

The Discussion Paper discusses the importance of shared data standards and the sharing of data between agencies, which implies common or interoperable platforms. The DLGSC and portfolio agencies note that a myriad of systems are currently used across the public sector, which can present challenges to complying with data standards.

The DLGSC supports the notion of a centralised analytics capability for the sector that would have capacity and capabilities including:

- undertaking special projects that address key government priorities in collaboration with other agencies;
- providing an information governance strategy, best practice guidelines, and assistance to agencies in the development of policies and procedures to align with the Framework;
- establishing a risk matrix and other guidance materials to ensure a consistent decision making across government;
- providing advice to agencies on what data they should collect and how it is collected to ensure the best outcome for the whole of government;
- establishing and maintaining a register of re-useable and linked datasets; and
- providing access to training to up-lift analytics capability across the sector.

***It is recommended that:***

- ***potential impacts of any new standards for sharing data and information between systems are considered in consultation with agencies to ensure any changes to systems and processes required are understood, planned and appropriately resourced; and***
- ***a matrix of strengths and weaknesses of the power to compel agencies to share information is developed and assessed in consultation with agencies to identify the best overall outcome for the public sector and broader community.***

**Third Party Access to Government Information**

The DLGSC and portfolio agencies agree that the Framework will assist in considering how sensitive and/or personal information should be managed regarding third party access to this information.

The DLGSC notes that existing policies, procedures and agreements may provide additional assurance to the Framework. For example, some existing Common Use Agreements allow for access to personal data for vendors contracted to provide services. It would be helpful for the DLGSC, portfolio agencies, and likely other agencies to better understand how existing and any potential new arrangements for third party access to information created and/or maintained by government relate to the proposed new legislation. This will enable the DLGSC and other agencies to have confidence that providing the information to a third party would not be in breach of any confidentiality provisions set out in other legislation.

Special consideration should also be given to engagement with culturally and linguistically diverse communities, and the rights of Aboriginal people as custodians of their cultural information. This would assist with continued support and communication to our community and help ensure there are mechanisms in place to engage with Aboriginal people around information sharing processes and provisions.

***It is recommended that the CDO, or other authority responsible for implementation of the Framework, work with the Department of Finance, Public Sector Commission and in consultation with other agencies, to standardise some of the existing controls across the sector. Examples include, licence agreement templates, contract terms and confidentiality agreements.***

**Mandatory Data Breach Notification**

The DLGSC and portfolio agencies support the notion of a mandatory breach notification scheme modelled on the Commonwealth scheme on information sharing arrangements; however, clarity is required on how local regulatory bodies will participate in this process, and how this would overarch and support existing processes.

It is noted that there is already a process in place in WA for notification about breaches of security (which includes access to data) via Office of Digital Government, WA Police Force and Australian Cybercrime Online Reporting Network. The role of these agencies and others should be considered as part of any new mandatory breach notification scheme. Further clarity is also required on what happens after a breach notification i.e. the process of identifying who is affected, how they may be affected, what information was breached, contact methods for those affected and potentially public alerts where appropriate.

***It is recommended that the CDO, or authority responsible for implementing a WA mandatory breach notification process, develops a consistent and clear process in consultation with agencies to determine risk, management and communication of a data breach.***

**Secondary Use of Personal Information Without Consent**

The DLGSC and portfolio agencies agree with the emerging position where data sharing arrangements enabling personal information to be shared would be covered under conditions based on the South Australia *Public Sector (Data Sharing) Act 2016*.

Further guidance on any new arrangements will be required for both agencies and the public, particularly regarding:

- the sharing and use of the personal information is in connection with a criminal investigation or criminal proceedings or proceedings for the imposition of a penalty;

- the sharing and use of the personal information in connection with the wellbeing, welfare or protection of a child or children, or other vulnerable person;
- the sharing and use of the personal information considered reasonably necessary to prevent or lessen a threat to the life, health or safety of a person; and
- the purpose of the sharing and use of the personal information when it cannot be achieved using de-identified data and it would be impracticable in the circumstances to seek the consent of the person to whom the information relates.

Careful consideration should be given when sharing personal information without consent. An example provided by the SLWA is, all State and public library users must be free to seek, access and share information within existing censorship and copyright legislations. Library users must be free to enter the SLWA and access basic services anonymously. Existing restrictions regarding the use of data about library visitors must be protected, for example the search and access history of a user would not be made available for other agencies for the purpose building profiles or drawing inference regarding the intentions of that user to use that information. Where CCTV is used for the protection of important collections, staff and other patrons' information is only be shared for other purposes upon appropriate legal demand; and not made available to determine the present or past location of a person, including the use of facial recognition software.

***It is recommended that terms such as 'vulnerable person', 'wellbeing', no reason to think' and 'personal Information' be clarified; and the provision of worked examples would be useful for agencies.***

For transparency, simple statements could be included in forms (preferably online) used by the public to remind them their information may be used under certain circumstances (including information on the controls over secondary use of the information).