DEPARTMENT OF JUSTICE – SUBMISSION ON PRIVACY AND RESPONSIBLE INFORMATION SHARING FOR THE WESTERN AUSTRALIAN PUBLIC SECTOR DISCUSSION PAPER

Consultation Questions

1. What issues should be considered when developing privacy and information sharing legislation for Western Australia?

The Department of Justice (the Department) has identified the following issues for consideration in the development of the Privacy and Responsible Information Sharing (PRIS) legislation for Western Australia (WA).

National consistency

The Department supports alignment with other Australian jurisdictions as one of the key principles guiding the proposed approach outlined in the Privacy and Responsible Information Sharing for the Western Australian Public Sector Discussion Paper (the Discussion Paper). It is understood that the Commonwealth and those States and Territories that have privacy legislation are reluctant to share information with the WA Government as the Government is not bound by similar privacy principles. To this end, the proposed PRIS legislation should aim to meet the requirements for data sharing in other Australian jurisdictions e.g. ABS, Centrelink.

The Department notes that while national consistency is important, the WA Government may also have regard to more modern privacy schemes such the European Union General Data Protection Regulation (GDPR) in the development of the PRIS legislation.

Intersection with current or new initiatives

It is important that the proposed PRIS legislation contemplates existing legislative provisions, Memorandums of Understanding, Protocols and Agreements which have already been established to authorise or restrict information sharing. In this regard, the Department would like to draw attention to the following examples of such current and future legislation or information sharing initiatives that may assist when considering the development of the PRIS legislation.

Current arrangements

Victims of Crime

The *Victims of Crime Act 1994 (WA)* (the VCA) allows certain information about victims to be shared between WA public sector agencies. The Director of Public Prosecutions principally works with WA Police Force, the Victim Support Service, the Child Witness Service, and/or the Criminal Injuries Compensation Assessor to assist victims. The VCA currently prohibits the use of such data outside of the provision of victim services.

There is significant research that demonstrates the negative impact of having to continually recite traumatic information on victims of crime. Effective information sharing between agencies will enable the development and delivery of better services by ensuring that victims of crime are not required to consistently provide information to different agencies about a crime or its impact.

Family and Domestic Violence

Information sharing is critical to an effective response to family and domestic violence (FDV), given the involvement of multiple Government and non-Government agencies. Relative to other States, WA has good FDV information sharing practices. For example, FDV Response Teams share information between WA Police, the Department of Communities (Child Protection) and non-Government service providers (Refuges).such as refuges) as part of a collaborative approach to improve the safety of child and adult victims.

WA also has existing legislative provisions that promote information sharing. For example, significant amendments were made to the *Children and Community Services Act 2004* (WA) in 2016 to strengthen and broaden information sharing to permit the sharing of information relevant to the safety of a person who has been subjected to, or exposed to, family violence.

Births Deaths and Marriages

The *Births, Deaths and Marriages Registration Act 1998* (WA) outlines the Registrar's responsibilities in respect of protection of privacy and how access to the Register may be obtained. Information sharing is permitted in various circumstances within this Act, and the Registry of Births, Deaths and Marriages also currently shares de-identified data with the private sector (generally for research purposes) and has in place numerous Memorandums of Understanding to this effect.

It is widely recognised that the document and data contained in a birth certificate is the most important life event and identification for a person, and therefore security and protections exist to ensure the information is not used for fraudulent purposes. As such, there are circumstances where the data held in the Register of Births, Deaths and Marriages should not be shared, and where the Registrar may refuse access.

Freedom of Information

Australian Privacy Principle (APP) 12 outlines the obligations of an APP entity when an individual requests access to personal information held about them by the entity. Development of the PRIS legislation and the creation of the role of Privacy Commissioner should consider any overlap or interaction with the current right to access personal information existing under the *Freedom of Information Act 1992* (WA), and with the role of the Information Commissioner.

New initiatives

It is also noted that the PRIS legislation will intersect with the following new information sharing initiatives:

- **FDV12** - A State Government election commitment to develop a database to share risk-relevant information relating to FDV between Government agencies and Courts; and
- **National FDV Information Sharing Framework** – A Council of Attorneys-General Family Violence Working Group project which intends to enable the sharing of risk-relevant information between the Family Court, and State Child Protection and Family Violence systems.
- **Royal Commission into Responses to Institutional Child Abuse** - Similar to FDV information sharing is critical to effective responses to reports of child abuse. The Department is currently working on implementing several relevant recommendations from the Royal Commission, such recommendations should be taken into account in the development of any new policy and legislation.

Scope of PRIS Legislation

As noted in the Discussion Paper the proposed PRIS legislation may cover organisations that would not ordinarily meet the definition of the public sector under the *Public Sector Management Act 1994* (PSM Act), such as those organisations prescribed under Schedules 1 and 2 of the PSM Act.

As previously stated, the Department wants to preserve and facilitate information sharing arrangements with non-government agencies, however it does not support including such agencies within the scope of the proposed PRIS legislation. Sharing information outside of the State Government could be facilitated under enforceable information sharing agreements.

Data ownership

The proposed PRIS legislation should contemplate information that is held, but not owned, by public sector organisations. A particular example for this Department pertains to civil and criminal courts and tribunals, and the data and information collected by them. In this regard, it is imperative that the proposed legislation does not affect court and tribunal access to record provisions. The Department considers that a blanket exemption for courts and tribunals under the legislation may be appropriate similar to the exemption provided for under the Freedom of Information legislation.

Consent

The Department considers that any provisions requiring a WA public sector agency to obtain consent from an individual prior to disclosing his or her personal information within the WA public sector should provide for a documented process which includes timeframes, relevant parties, the information to be shared, and any exclusions. For example where there is a risk to safety. Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely, unless by agreement.

Further, the legislation should consider an individual's capacity to provide consent and what this means for a person's information if they are unable to make decisions for themselves, or rely on authorised representatives to act on their behalf.

2. What privacy principles should WA adopt for regulating the handling of personal information by the public sector? Are any of the existing Australian Privacy Principles, or principles in other Australian jurisdictions, unsuitable for WA?

As noted in the Discussion Paper, the APPs are designed to apply to a broader range of contexts and organisations than the WA public sector. The Department generally supports the adoption of the APPs where they are relevant to the regulation of information privacy between WA public sector agencies, subject to the following comments:

- The policy underlying the PRIS legislation should be less tolerant of direct marketing than the *Privacy Act 1988 (*the Privacy Act). When proposing to use information for the commercial reasons, agencies should generally seek individuals' prior consent to that use.
- APP 2 requires APP entities to give individuals the option of not identifying themselves. The Department notes it may only be able to provide individuals the option to remain anonymous in a limited number of circumstances.
- In New South Wales, Information Protection Principle (IPP) 10 provides that an agency can only use an individual's personal information for the purpose for which it was collected unless, inter alia, the information is used to prevent or lessen a serious or imminent threat to any person's health or safety. The Department supports a broader application of this exception to cover threats to public health and safety. Further, the Department notes that Victoria has removed the word imminent from several provisions in their Information Privacy Principles and Health Privacy Principles as a result of the Royal Commission into Family Violence in 2015. The WA government should also consider the necessity of this threshold when adopting privacy principles in this State.

3. What should the role of a Privacy Commissioner be, and how can this role best protect privacy and ensure public trust?

The Department recognises that an independent regulator will play a particularly significant role in the proposed principles-based privacy regime in WA. As evidenced in other jurisdictions, the broader privacy principles will need to be supplemented with specific guidance or legislative instruments to accommodate for different industries or different policy considerations.

The Department believes it may be necessary to have a legislative mechanism, similar to other jurisdictions, which allows the Privacy Commissioner to allow public sector agencies to be exempt from certain privacy principles or to modify the application of the privacy principles to the practices of the public sector agency.

The role of Privacy Commissioner can best build and maintain public trust in relation to the proposed privacy framework by:

- enabling the public to raise issues of concern through receiving, investigating and resolving complaints;
- identifying and reporting on breaches of privacy requirements;
- undertaking research and enabling privacy experts outside of Government to inform the public debate on related matters;
- providing guidance and advice to Government or Ministers consistent with the regulatory approach;
- undertaking monitoring and assurance activities to assess compliance with the privacy principles including third party compliance with the legislation or data sharing agreements, depending of the scope of the PRIS framework; and
- monitoring data sharing arrangements to ensure that privacy is being upheld across the public sector in accordance with the legislation.

4. How should breaches of privacy be managed, and what action should be taken in response to a breach?

The Department considers that an individual should have the option to complain to the relevant agency directly in relation to an alleged privacy breach or make privacy related complaints directly to an independent officer such as the Privacy Commissioner. The PRIS legislation could also contemplate a review mechanism for decisions made by the relevant agency or the Privacy Commissioner.

The Department supports a compliance policy that adopts a clear enforcement pyramid approach to encouraging compliance and enforcing the legislation. The Department advocates an emphasis on fostering and securing compliance through guidance, education and other facilitative methods. The Privacy Commissioner should identify whether changes to the process or policies of an agency are required to avoid similar breaches in the future.

Penalties for breaching PRIS should be proportionate and consistent with comparable existing provisions in Australia. Penalties should also apply to breaches committed by third parties who are bound by relevant legislation or agreement.

Subject to the type of offences that are established under the PRIS legislation, consideration should be given to the interaction of existing defences available to officers who disclose information in good faith under relevant legislation, see for example section 23(5) of the *Children and Community Services Act 2004* (WA). Such defences may also be necessary under the proposed PRIS legislation to protect officers from civil or criminal liability, if information is disclosed in good faith under prescribed circumstances.

The establishment of data breach notification schemes in other jurisdictions indicates a community expectation that individuals will be notified in the event of a data breach of a certain level of seriousness.

5. When should government agencies be allowed to share personal information? Are there any circumstance in which it would not be appropriate to do so?

The Department is completely supportive of the enabling of data sharing between State Government agencies to support service delivery and to benefit the community. PRIS should authorise agencies to collect, use and disclose personal information in certain circumstances,

such as where individuals have provided consent, where such activities are authorised by law, where the safety of an individual or the public is at risk, or where there is a defined purpose and benefit to the sharing of information in line with the objectives of the legislation.

The Department recognises that requiring consent for all data sharing is often impractical and will lead to biased data that delivers sub-optimal service delivery and research/policy outcomes. Additionally, there will be situations where the requirement of consent could jeopardise individual or public safety. While the Department supports the default position of sharing identified information with other Government agencies in accordance with the proposed approach, we do not believe that same information sharing arrangements should apply to non-government organisations. In terms of providing information for research, the Department is amenable to providing aggregate information to non-government organisations who request data to assist with (for example) decision making or evaluations (see response to question 7 for more information).

Data collected by one agency should be shared with another agency for use solely for an agreed purpose which should be linked to the best interests or wellbeing of the individual and/or the wider community. Additional use of the shared data by the other agency should be subject to review by the original agency prior to use. This is to ensure the data or information is fit for purpose for the additional use, and to confirm the validity and benefit of the additional use to the WA Government and the community

6. What should the role of a Chief Data Officer be? How can this role best support the aims of Government and the interests of the public?

In order for the PRIS legislation to successfully achieve its proposed objectives, attitudes across agencies will need to be consistent with regard to data sharing, meaning that data sharing will need to be seen business-as-usual rather than the exception. Consequently, the Chief Data Officer (CDO) will need to foster a data sharing culture across the WA public sector through the development of enabling frameworks in the form of policy, standards, process and procedure that focus on building a data governance capability and shared language for data management.

The success of the PRIS legislation will also be contingent on the ability of responsible organisations to classify their data. That is, identifying which laws govern what kinds of information, and which particular handling or approval criteria apply. The CDO could also facilitate these capabilities within each agency.

Key areas of focus for the CDO role should include:

- ensuring that all government staff are aware when there is an authority to share personal information, for example under certain circumstances in the context of family and domestic violence and child safety.
- identification and prioritisation of capability development that enables government as a whole, and by extension each agency, to access and utilise data for community and citizen service delivery outcomes;
- supporting the development of data sharing agreements in accordance with the proposed legislation;
- provision of arbitration and advice to agencies in disagreement regarding data sharing;
- assisting public sector agencies with data analytics, if requested by agency;
- development of a state architecture for data management that enables agencies to access citizen and service delivery master data; and
- maintenance of a catalogue of datasets and support to agencies trying to find information.

The Department does not support any proposal to confer powers to the CDO to compel agencies to share data.

7. Should the WA Government facilitate sharing of information outside the WA public sector? What should be considered when making a decision to share outside the WA public sector?

The Department currently shares information with non-government organisations within the limits of the law and has in place several Memorandums of Understanding and Protocols to facilitate information sharing for particular projects.

As previously stated the Department supports a narrow interpretation of the term 'public sector'. While the Department is committed to encouraging research by universities and non-government organisations, it is not recommended that universities etc. be captured by the information sharing provisions. This Department has a robust research committee which considers research proposals and facilitates access to information where appropriate. Any sharing of information required for research being conducted by a third party (such as a university) on behalf of a State Government agency would likely already be subject to privacy and information sharing agreements.

If information is transferred outside of the WA public sector, there should be enforceable legislative or contractual requirements that protect that information and ensure it is only used for the identified purpose. The legislation or agreement should contemplate:

- Appropriate disposal of the data once the project is completed.
- Restrictions on the on-sharing of data. Data should be shared with another agency for use solely for an intended purpose.
- Controls to ensure effective de-identification of data.

8. What criteria should be included as part of a risk management framework such as the Five Safes?

The Five Safes appear to be comprehensive for smaller data sharing initiatives, however, to be more effective the framework should be assessed in relation to currently accepted information communications technology controls, standards, and frameworks. The Department submits that any risk management framework should align with Commonwealth and State approaches to ensure consistency in the frameworks application.

The Five Safes framework may not be adequate for large data linkage projects (e.g. SIDR) where the various specific projects or analyses to be undertaken with the data may be unknown at the time, but not possible without the linked data.

Further, consideration should be given to how the privacy principles and the Five Safes can be communicated as a cohesive framework, rather than as standalone silos, so as to enable the community and public sector to be able to efficiently navigate, interpret and apply legislation efficiently and effectively.

9. Under what circumstances would it be considered acceptable to share confidential information within the public sector?

The Department does not support PRIS legislation that generally overrides a duty of confidence or provides authority for disclosure of information that is already required to be held in confidence. However, it is acknowledged that there may be some exceptions, such as case management across multiple agencies, risks to safety, or when consent is provided.

The legislation should set higher protections for sensitive data with strict limitations on categories of sensitive data such as commercial-in-confidence, legally-privileged, security-classified, confidential, or culturally sensitive data. Further, it would be beneficial if there was some clarity as to what may be considered confidential information.

10. What should the WA Government be doing to support successful implementation of privacy and information sharing?

The Department would welcome the opportunity to provide further feedback on any implementation issues once the scope of the proposed PRIS legislation is established. In general terms, the provision of support (and resources, if required) to agencies undertaking the necessary internal procedural changes to implement PRIS will be central to its success.