Office of the Victorian Information Commissioner

Submission

To the Western Australian Department of Premier and Cabinet on the *Privacy and Responsible Information Sharing for the Western Australia Public Sector* discussion paper

Overview of the Office of the Victorian Information Commissioner

The Office of the Victorian Information Commissioner (**OVIC**) was established in September 2017, by way of the *Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017*. The establishment of OVIC combined the functions of the former Offices of the Freedom of Information Commissioner and the Commissioner for Privacy and Data Protection. OVIC administers two pieces of legislation – the *Freedom of Information Act 1982* (Vic) (**FOI Act**) and the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**). This provides OVIC with regulatory oversight of freedom of information (**FOI**), information privacy, and information security for the state of Victoria.

The Information Commissioner is responsible for leading OVIC with powers and functions under both the PDP Act and FOI Act. The Information Commissioner is supported by two Deputy Commissioners – a Public Access Deputy Commissioner with powers and functions under the FOI Act,[1] and a Privacy and Data Protection Deputy Commissioner with powers and functions under the PDP Act.[2]

It is notable that in Victoria, the regulation of information privacy is divided between OVIC and the Health Complaints Commissioner (**HCC**). The Information Privacy Principles (**IPPs**)[3] under the PDP Act apply to personal information, but they do not apply to information of a kind to which the *Health Records Act 2001* (Vic) (**HR Act**) applies.[4] Individuals' health information[5] is instead covered by the Health Privacy Principles (**HPPs**), set out in the HR Act. Consequently, Victorians' health information is regulated by the HCC.

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

(a) Privacy oversight should sit with the Office of the Information Commissioner

Oversight of privacy law is well placed within an Information Commissioner's office, combining both information privacy and FOI functions.

The establishment of OVIC in 2017 saw the functions of the privacy regulator merge with those of the former FOI Commissioner, bringing the two areas under the remit of a single Information Commissioner. This approach had already been adopted in other Australian states before Victoria followed suit, leveraging off the success of this approach in other jurisdictions, particularly New South Wales and Queensland. The experiences of the New South Wales Information and Privacy Commission, Office of the Information Commissioner Queensland and OVIC have demonstrated that combined oversight of FOI and privacy has the potential to provide a coherent, consistent regulatory approach to governance and enforcement of information rights.

Despite the seeming tension between the notions of public access to government information and information privacy, in practice, it is rare for privacy law and FOI law to conflict. Where there is potential for inconsistencies between the two laws, having a sole regulator for both areas is likely to result in a better

[1] The functions of the Information Commissioner and Public Access Deputy Commissioner are set out in Part 1A of the FOI Act.
[2] The functions of the Information Commissioner and Privacy and Data Protection Deputy Commissioner are set out in Part 1A of the PDP Act.
[3] The 10 IPPs are contained in Schedule 1 of the PDP Act and set out the obligations of organisations in relation to their handling of personal information.
[4] The definition of 'personal information' is contained in section 3 of the PDP Act, and expressly excludes information covered by the HR Act.
[5] 'Health information' is defined in section 3 of the HR Act.

outcome when seeking to resolve tensions, in contrast to two regulators who approach their respective jurisdictions from single, potentially inconsistent perspectives.

In OVIC's view, the current Office of the Information Commissioner for WA (**OIC**) would be well placed to take on the role of privacy regulator. As an office that already receives and responds to complaints, and conducts reviews relating to information rights, the receipt of privacy complaints would be a natural extension of the OIC's functions. Given the existing structures and processes in place at the OIC, an expansion into oversight of privacy law would offer an effective and efficient model for implementing the regulation of privacy rights in WA.

This view is based on the assumption that the OIC would receive appropriate funding and resourcing for the expansion of its remit to oversight of information privacy.

(b) Privacy and information sharing laws should be in separate pieces of legislation

On OVIC's view, Privacy and information sharing laws should be in separate pieces of legislation. Information sharing, or data sharing laws were introduced in Victoria in 2017 with the passage of the *Victorian Data Sharing Act 2017* (**VDS Act**). The purposes of the VDS Act include to:

- promote the sharing and use of public sector data to support government policy making, service planning and design;
- remove barriers that impede the sharing of identifiable data with the Chief Data Officer or data analytics bodies, and facilitate sharing of data across the Victorian public sector; and
- provide appropriate protections for data sharing under the VDS Act.[6]

The VDS Act does not limit the operation of the PDP Act, and both pieces of legislation work together to facilitate appropriate data sharing within the Victorian public sector.[7] Based on the Victorian experience of privacy and data sharing laws, OVIC has formed the view that these laws are best placed in separate pieces of legislation. There are a number of reasons for enacting these laws separately, which are outlined below.

- In Victoria, the Information Commissioner is an independent regulator who has oversight of information handling in the Victorian public sector. The Information Commissioner's functions are performed independently of government, whereas the Chief Data Officer and the Victorian Centre for Data Insights (**VCDI**) sit within the Department of Premier and Cabinet, providing advice and conducting joint projects with government organisations. Having the respective functions of the privacy regulator and Chief Data Officer set out in separate legislation signals to the public sector and the community that the work of the privacy regulator is performed independently of government.
- The VDS Act specifically gives the Information Commissioner – and the HCC – an oversight role of the activities of the Chief Data Officer. For example, the Chief Data Officer is required to report to the Information Commissioner annually on projects conducted under the VDS Act that relate to personal information.[8] The Chief Data Officer, and data analytics bodies, are also required to notify the Information Commissioner of any breaches of the PDP Act in relation to data handled under the

[6] The purposes of the VDS Act are set out in section 1 of that Act.
[7] Section 24(2) of the VDS Act states that that Act does not affect obligations under the PDP Act.
[8] Section 29 of the VDS Act.

VDS Act.[9] These mechanisms provide the public sector and the community with assurance that data sharing and data analytics activities involving personal information are subject to scrutiny and regulatory oversight. Should a similar model be proposed in WA, whereby the privacy regulator has oversight of the activities of the Chief Data Officer (or equivalent), incorporating both schemes under the one piece of legislation may have the perception that the privacy regulator is not independent of government. As such, OVIC recommends that WA DPC consider the model in operation in Victoria.

- Privacy laws around Australia and internationally provide privacy protections for individuals beyond when information about them is shared. The PDP Act, for example, also contains important protections for the collection, security, quality and destruction of personal information, to ensure individuals' privacy is maintained in the use and ongoing management of their information. By creating a single law to cover privacy protection and data sharing, the two concepts may become conflated, and the protection of privacy may be viewed as having significance in the context of data sharing, but not more broadly.

- The Victorian experience has shown that organisations are often reluctant to share personal information for fear of breaching the IPPs in doing so. Privacy law is still seen as a barrier to information sharing in many cases, even where the act or practice an organisation is considering is already authorised by the IPPs. Creating stand-alone data sharing legislation would provide an express authority for public sector organisations to share data (which may include personal information) for specific purposes, signalling Parliament's intention that data be shared and used across government. In Victoria, the VDS Act has created a clear pathway for data sharing to take place by separating the authority for data sharing from privacy law, and promoting a shift in cultural attitudes towards data sharing.

(c) Ensure there is a single source of privacy regulation and oversight

The *Privacy and Responsible Information Sharing for the Western Australia Public Sector* discussion paper (**the discussion paper**) notes that the regulation of privacy and disclosure of personal information in the WA public sector is currently governed by a combination of common law, entity specific legislation and regulation.[10] When developing a new privacy framework OVIC recommends that WA DPC undertake a holistic review of privacy and information handling provisions contained in existing and interrelated legislation and regulation, to minimise the potential for conflict or duplicate obligations.

To ensure clarity and consistency in the application of privacy protections, it is advantageous for there to be a single source of regulation setting out the law and principles to be followed with respect to information privacy, as opposed to multiple or duplicative sources. In the absence of this, the regulatory environment may become complex for regulated organisations to navigate and understand their obligations, and the public to understand their rights.

In addition to ensuring the regulatory environment is clear, it is recommended that oversight of, and external complaint pathways in relation to information privacy, resides with one regulatory body such as the OIC. As noted previously, the regulation of information privacy in Victoria is divided between OVIC (which regulates the IPPs under the PDP Act) and the HCC (which regulates the HPPs under the HR Act). As a result of this division, where a privacy breach involves both health information and personal information,

[9] Section 24(3) of the VDS Act.
[10] Page 12 of the discussion paper.

an individual has dual complaint rights to both OVIC and the HCC. Having multiple external complaint bodies can lead to confusion and inconsistency.

(d) Include mechanisms allowing for the authorised departure from privacy principles

The PDP Act contains mechanisms that permit organisations in certain circumstances to do acts or engage in practices that do not comply with the IPPs or an approved code of practice. The two mechanisms for achieving this are Public Interest Determinations[11] (**PIDs**) and Information Usage Arrangements[12] (**IUAs**).

A PID is a determination by the Information Commissioner that an act or practice of an organisation contravenes or may contravene an IPP, but the public interest in the organisation doing the act or engaging in the practice substantially outweighs the public interest in complying with the IPP. When a determination is made by the Information Commissioner, the organisation is not required to comply with the specified IPP or IPPs when doing the act or engaging in the practice outlined in the PID. A PID can either be issued on an ongoing or temporary basis.[13]

An IUA is an arrangement that sets out acts or practices for handling personal information for a public purpose and for any of those acts or practices, the IUA may modify the application of an IPP or information handling provision,[14] or provide that the act or practice does not need to comply with an IPP or information handling provision. A 'public purpose' is defined to mean:

- compliance with a law;
- the performance of functions by a public sector agency or a Council, or an agency of the Commonwealth, another State or a Territory; or
- the provision of a service in the public interest to the public or a section of the public.[15]

Both these mechanisms are considered by the Information Commissioner on application from an organisation or organisations, and allow for a flexible and agile approach to the collection, use or disclosure of personal information in circumstances where it would not otherwise be permitted under the PDP Act.[16] In particular, these mechanisms can provide an opportunity for new information handling schemes to be tested, and assure that when legislation is later developed that alters how personal information may be collected, used or disclosed, it is fit for purpose and has a clear benefit to organisations and the public.

(e) Privacy laws should apply to local government and universities created under state legislation

The IPPs and information privacy provisions under Part 3 of the PDP Act apply to all local councils in Victoria and universities established under Victorian legislation.[17] It is recommended that WA's new privacy framework provides similar coverage for these organisations that carry out public functions.

[11] Part 3, Division 5 of the PDP Act.
[12] Part 3, Division 6 of the PDP Act.
[13] The mechanism for making a PID is contained in Part 3, Division 5, Subdivision 1 of the PDP Act, while the mechanism for making a Temporary PID is contained in Part 3, Division 5, Subdivision 1 of the PDP Act.
[14] See sections 3, 45(1)(b)(iii) and 47(4) of the PDP for further information on 'information handling provisions'.
[15] Section 43 of the PDP Act.
[16] A PID is approved by the Information Commissioner, however an IUA requires approval from the relevant Minister of the organisation, or relevant Minister responsible for each organisation subject to the IUA.
[17] Section 13 of the PDP Act.

Councils often have a very direct relationship with their constituents, perhaps more so than any other level of government. The personal information collected, held and used by local government can directly affect people's lives. This can include information relating to property, health and wellbeing, homeless services and childcare. Ensuring that this information is appropriately protected is an important component of privacy law and a critical function of a privacy regulator. OVIC encourages the extension of a WA privacy law to local government.

Similarly, while it is noted that universities established under state legislation have obligations to comply with the Australian Privacy Principles (**APPs**) contained in the *Privacy Act 1988* (Cth) (**Privacy Act**), those obligations only exist in relation to the handling of students' personal information.[18] Universities collect and use vast amounts of personal information from not only students, but also a wide range of individuals including staff, research participants, and users or attendees of university facilities, services, events or activities. Without state based privacy regulation, the personal information of individuals other than students is not provided with the appropriate level of protection, and in the case of a privacy breach these individuals do not have access to an independent complaint body. Again, OVIC encourages the extension of a WA privacy law to universities established under state legislation.

(f) Privacy laws should extend to contracted service providers

Outsourcing government services to an external service provider is common practice across all levels of government. Services may be provided directly to a government agency, for example, undertaking audits or providing ICT support, or may be provided to third parties on behalf of government, for example, the provision of community health services to the public.

Given the prevalence of government outsourcing, OVIC considers that it is essential that privacy legislation contains a mechanism to ensure contracted service providers are capable of being bound to privacy law when handling personal information in relation to government services under a contract. This is particularly relevant in the context of service providers that provide health and community services, where the information handled can be highly sensitive and confidential. The public has an expectation that their personal information will be handled with care and diligence when accessing government services, even when those services are provided by third parties.

In Victoria, the default position under the PDP Act is that the outsourcing party (the government or public sector organisation) is liable for any privacy breaches that may occur in relation to services provided under the contract, even if those breaches are the result of the acts or practices of the contract service provider.[19]

However, this default position can be varied by the contract to provide that the service provider is directly bound by the IPPs in the same way and to the same extent as the outsourcing party.[20] In those circumstances, the contracted service provider becomes responsible for ensuring its practices align with the IPPs, and is also responsible for any breach of the IPPs resulting from its acts or practices.

(g) Consent and privacy legislation

Under the PDP Act, consent is defined to mean 'express or implied' consent.[21] While consent is not the only basis by which information can be collected, used or disclosed under privacy law, it does provide individuals

[18] Section 19-60 of the *Higher Education Support Act 2003* (Cth).
[19] Section 17(4) of the PDP Act.
[20] Section 17(2) of the PDP Act.
[21] Section 3 of the PDP Act.

(in certain circumstances) with the ability to better control when, how and by whom their personal information is collected and handled. In the context of the PDP Act, consent of an individual provides one legislative basis for an organisation to use or disclose personal information for a purpose other than the primary purpose for which it was collected.[22]

Regardless of whether consent is express or implied, in both cases it should be meaningful. The five elements of meaningful consent are: voluntary, informed, specific, current and provided by an individual with the capacity to consent.[23] As such, OVIC suggests that thoughtful consideration is given to how consent is defined under WA's privacy legislation.

While OVIC recognises the value of consent in providing individuals with a greater ability to control the collection, use, and disclosure of their personal information, OVIC is also mindful that relying on consent as a means to protect privacy may be problematic in certain circumstances. The traditional (or transactional) approach to consent, which involves an individual providing their consent to the collection, use or disclosure of their personal information in exchange for a service offered by government, places the responsibility on the individual to inform themselves of the way in which their personal information will be handled, prior to making the decision to access that service. Often individuals will not have an understanding of the implications of what they are consenting to, or the full range of contexts in which the consent will apply. While express consent is generally provided, it is often not meaningful or informed. This problem is currently a matter of great interest to regulators around the world. Recognising the imbalance of power between states and corporations on the one hand, and individuals on the other, the General Data Protection Regulation of the European Union established rules aiming to improve the quality of notices and information provided for the purpose of obtaining consent.

In addition, consent should not be sought from an individual where legislative authority exists to collect, use or disclose personal information. Seeking consent in those circumstances may appear disingenuous to an individual where personal information can be collected, used or disclosed regardless of whether or not consent is provided due to express legislative authority.

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?

(a) Adopt principle-based legislation

Legislation that is principle-based, such as the privacy provisions in the PDP Act, is valuable in offering flexibility in how protections (such as privacy principles) can be applied in varying public sector organisations and contexts. Given the extensive diversity of public sector organisations, and the unique ways they each engage with the public, principle-based legislation would be more effective compared to prescriptive rules-based legislative approaches. With rapid advancements in technology and the increasing adoption of technological solutions in administering government services, privacy principles that are technology-neutral can be applied regardless of the way in which public sector organisations work.

Principles provide organisations with the flexibility to tailor their information handling practices to their diverse operational environments and the needs of the individuals to whom they provide services. In addition, a primarily principles-based framework lends itself well to adopting varying degrees of detail and

[22] IPP 2.1(b) in Schedule 1 of the PDP Act.
[23] See OVIC's Guidelines to the IPPs https://ovic.vic.gov.au/book/key-concepts/#Consent.

prescription within the principles as required.

(b) Ensure appropriate restrictions on use and disclosure for secondary purposes

Personal information that has been collected for a particular purpose (primary purpose) has the potential to be used for purposes outside of its primary purpose of collection and beyond what an individual may have consented to or may reasonably expect. Privacy principles in relation to permitted secondary uses or disclosures of personal information will require a certain degree of prescription, to ensure personal information is handled consistently and appropriately across regulated organisations.

In Victoria, IPP 2.1 allows personal information to be used for a secondary purpose (outside the primary purpose of its collection) where, for example, the secondary purpose is related to the primary purpose and the individual would reasonably expect that use, consent of the individual has been obtained, to undertake law enforcement activities, or to lessen or prevent a serious threat to an individual's life. When considering the secondary use of information, proportionality is also a factor in considering whether use is reasonable.

(c) Arrange privacy principles in the information lifecycle

When developing the overall structure of privacy principles, OVIC recommends that they are structured to reflect the 'information lifecycle' – an approach adopted in the APPs under the Commonwealth Privacy Act. An information lifecycle approach, detailing collection, security, use and disclosure, access and correction, and destruction, will assist organisations to better understand how the principles operate and interact with one another, as well as the obligations that flow from each principle throughout the lifecycle of information handling.

(d) Include a positive obligation to implement privacy practices and governance

Regulation that promotes good privacy governance is a key element for upholding information privacy rights. This involves taking proactive steps to promote and protect privacy, and encouraging accountability for information handling practices. The way that organisations manage their privacy governance can also enhance public trust and confidence, and importantly for governments, build their social licence to collect and use individuals' personal information.

In addition to core privacy principles detailing how personal information is to be collected and handled, OVIC recommends that there be principles that embody and promote transparency and accountability. This can be achieved by including principles that draw on the concepts in APP 1. In particular:

- APP 1.2: to take reasonable steps to implement practices, procedures and systems that will ensure organisations comply with the privacy principles; and
- APPs 1.3 and 1.4: having a clearly expressed and up-to-date privacy policy detailing how personal information is managed.[24]

A principle such as APP 1.2 assists to create a culture that respects and understands the value of personal information. It also encourages organisations to adopt a Privacy by Design approach, which assists to protect privacy by ensuring that it is considered and built into the design, development, and implementation of projects and initiatives involving the collection and handling of personal information.

[24] See also IPP 5 that contains a similar requirement.

For example, a principle like APP 1.2 can encourage organisations to build privacy impact assessments (**PIAs**) into their project and risk management processes. PIAs serve as an important tool for organisations to identify the privacy impacts and risks of projects (particularly during the design and implementation stages) and in doing so, develop risk mitigation strategies to minimise any potential harms that may come to individuals from a privacy risk.

(e) Privacy and security go hand-in-hand

Information privacy and security are interconnected; an organisation cannot guarantee privacy without having proper security practices and mechanisms in place. OVIC suggests including a principle that requires organisations to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.[25]

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

(a) Provide education and guidance, promote compliance with privacy principles and handle complaints

In an environment where overarching privacy legislation has not existed previously, it is fundamental that the Privacy Commissioner promotes a culture across the public sector that aims to recognise the value and importance of handling personal information with respect and in accordance with the privacy principles. A Privacy Commissioner should be responsible for facilitating and promoting both transparency and accountability in information handling practices. This can be achieved in a number of ways, such as:

- *Undertake education and training*

  Public sector employees need to have more than just a general awareness of privacy laws and principles. As well as understanding their obligations under privacy laws, they also need to know how they can handle personal information in a manner that is transparent, meets community expectations, and recognises the value in protecting that information. This can be achieved by ensuring the Privacy Commissioner has express functions to undertake education and training activities and provide guidance for both members of the public and employees of the public sector.[26]

- *Develop guidelines in relation to privacy principles*

  An express function to develop guidelines that can assist organisations to interpret privacy principles would be valuable. In Victoria, OVIC has developed Guidelines to the IPPs[27] that explain how the Information Commissioner interprets and applies the IPPs, and the matters that the Information Commissioner may consider when advising organisations during consultations, dealing with complaints, or examining acts and practices or breaches during an investigation. They also provide guidance to organisations on the broad application of the IPPs, and how to embed privacy protections in their workplace culture and practices. Guidance materials will be an invaluable resource and tool for organisations or public sector employees, particularly for those with limited previous experience or

[25] For example, see IPP 4.1 and APP 11.
[26] Under section 8C(2)(a) of the PDP Act the Information Commissioner and Privacy and Data Protection Commissioner have a function to promote understanding and acceptance of the IPPs and the objects of the IPPs.
[27] OVIC's Guidelines to the Information Privacy Principles can be viewed via https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/.

exposure to privacy laws.

- *Handle privacy complaints*

The Privacy Commissioner must be able to handle complaints either by conciliation and/or determinative powers. This is discussed in detail in the next section of this submission.

- *Make submissions and undertake consultations*

An important function that OVIC undertakes is to raise concerns, identify issues, and comment on proposals (such as draft legislation or reform projects) that relate to or have an impact on privacy, particularly the privacy of Victorians. It is essential to ensure that any reforms or legislative proposals for WA have appropriate protections in place that reflect the value and importance of personal information.

An example of the value that a privacy regulator can have in this respect can be seen in the *Service Victoria Act 2018* (Vic) (**SV Act**) and VDS Act, both of which incorporate a requirement for mandatory data breach reporting to OVIC, which was included after encouragement with the Information Commissioner during consultations on the draft legislation.[28] The ability to inform legislation in this way enhances the oversight mechanisms that the regulator has, allowing for a more impactful regulatory role, resulting in increased trust and transparency for both individuals and organisations affected by the legislation.

OVIC recommends that express functions of the Privacy Commissioner should be to consult and cooperate with organisations on matters relating to information privacy, and to undertake research into matters relating to information privacy.[29] This would enable and encourage the Privacy Commissioner engage with the public sector on proposals that impact on information privacy, and to ensure the Privacy Commissioner is informed and aware of emerging privacy trends and issues.

(b) Oversight, but not administration of information sharing should sit with a Privacy Commissioner

Regulatory oversight of data sharing should sit with a Privacy Commissioner. As noted previously in this submission, this is the model that has been adopted in Victoria through the VDS Act, which provides an express requirement for the Chief Data Officer to report annually to the Information Commissioner on its projects involving personal information.

As a business unit of the Victorian Department of Premier and Cabinet, the VCDI is subject to the PDP Act in the same way as any other Victorian public sector organisation and is therefore required to comply with the IPPs and respond to any privacy complaints made against it. Having had two years' experience with this model in Victoria, it is an approach that appears to be working well.

The functions of a Chief Data Officer (or equivalent) should not rest with the entity that administers privacy legislation; the two functions should be separated, and the WA equivalent of a Chief Data Officer should be subject to oversight from the Privacy Commissioner. Maintaining separation between the Privacy Commissioner and Chief Data Officer provides assurance to the public sector and community that those implementing government policy and regulating the handling of personal information are separate entities.

[28] See section 24(3) of the VDS Act, and section 54(3) of the SV Act.
[29] Similar functions exist in under sections 8(2)(g) and 8(2)(h) of the PDP Act.

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

(a) The Privacy Commissioner should have determinative functions in relation to privacy complaints

The Privacy Commissioner should have a power to make determinations in respect of privacy complaints.

Under the PDP Act, the Information Commissioner and Privacy and Data Protection Deputy Commissioner have a function to conciliate privacy complaints made to OVIC;[30] however, the Information Commissioner and Privacy and Data Protection Deputy Commissioner are not able to make determinations. If conciliation fails, or is deemed inappropriate, a complainant is able to request their complaint be referred to the Victorian Civil and Administrative Tribunal (**VCAT**),[31] where VCAT can make a determination as to whether or not there was an interference with privacy.[32]

OVIC's experience in receiving and conciliating privacy complaints has contributed to our view that the Privacy Commissioner should have determinative powers as opposed to only conciliatory functions. The reasons for this are outlined below.

- The ability for a Privacy Commissioner to make determinations in a privacy complaint would provide an expeditious and informal complaint pathway, benefiting both the complainant and the respondent organisation. Complaints that have little merit can be resolved quickly where the Privacy Commissioner is able to make a decision that there has been no interference with privacy, potentially saving the complainant time and angst in going through a formal conciliation process, and in some cases, taking their complaint to a tribunal. Similarly, where the Privacy Commissioner is of the view that the respondent organisation has contravened one or more of the privacy principles, their determination could influence the organisation's future practices. This would be especially beneficial where the respondent organisation is a contracted service provider, that may not otherwise have obligations to comply with privacy legislation, save for those services provided under State contract.[33] As the current conciliation process under the PDP Act does not result in a determination from the Information Commissioner or Privacy and Data Protection Deputy Commissioner, neither party receives an independent view as to whether or not there was an interference with privacy, potentially causing uncertainty and doing little to influence organisational practices.

- Determinations made by a Privacy Commissioner, and published on their website, can guide and influence organisational practices beyond the respondent organisation. In July 2019 OVIC commenced publishing its notices of decision in relation to FOI reviews, with the intention of educating agencies and applicants, and providing certainty as to what future decisions by the Information Commissioner and Public Access Deputy Commissioner might be on similar matters. OVIC has experienced a positive reaction to this initiative from agencies, who are using the published notices of decision as guides when making their own decisions. Having the ability to make determinations in relation to privacy complaints, and publish them, would provide predictability and assurance to both respondent organisations and privacy complainants as to the outcome they can anticipate in a given matter. Previous decisions can also serve to educate and

[30] Section 8C(2)(d) of the PDP Act.
[31] Sections 66(2) and 71(2) of the PDP Act.
[32] Section 77 of the PDP Act.
[33] Section 17 of the PDP Act relates to the effects of outsourcing and the applicability of the IPPs in those cases.

promote best practice to other regulated organisations.

- A determination process would make it less burdensome for a complainant to demonstrate a breach of their privacy. When a privacy complaint is referred to VCAT, the complainant is at a disadvantage as the onus is on them to provide evidence that their privacy had been breached. Where a complaint is able to be investigated by a Privacy Commissioner, a more inquisitorial approach can be taken in hearing the views of both parties, before an assessment is made by the Privacy Commissioner. This would result in greater benefits for the complainant, whose rights privacy laws are intended to uphold.

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

(a) When organisations should be able to share personal information

Ensuring information sharing is in line with community attitudes and expectations is paramount to maintaining the public's trust in how government uses and shares information. OVIC considers that any information sharing legislation that enables the sharing of personal information should include a provision that requires a consideration of competing public interests. For example, in deciding whether to share personal information there must be a balancing of the public value or purpose to be achieved with the public interest in protecting the privacy of personal information in the public sector.[34]

In Victoria, as has been noted previously, the purpose of the VDS Act is to promote the sharing and use of public sector data as a public resource that supports government policy making, service planning and design.[35] The VDS allows for identifiable data to be used in two instances:

- data integration[36] – meaning the combination or collation of data contained in two or more data sets; and

- undertaking data analytics[37] – however before any data is used for analytics, steps must be taken to ensure no individual can be identified from that data.

In each of those instances, and with all other data handled under the VDS Act, the purpose must only be for informing policy making or service planning and design.[38] These are the only approved purposes for sharing data under the VDS Act.

In addition to the VDS Act, there have been recent legislative reforms in Victoria permitting information sharing in the context of child safety and family violence. The Child Information Sharing Scheme,[39] under the *Child Wellbeing and Safety Act 2005*, allows authorised organisations and professionals who work with children, young people and their families to share information with each other to promote children's wellbeing and safety. Similarly, the Family Violence Information Sharing Scheme,[40] under the *Family Violence Protection Act 2008*, allows authorised organisations that work with victims and perpetrators of family violence to share information with each other in order to keep victims safe and hold perpetrators to

[34] A similar provision is contained in section 5(a) of the PDP Act.
[35] Section 1(b) of the VDS Act.
[36] Sections 16 and 17 of the VDS Act.
[37] Section 18 of the VDS Act.
[38] Section 5 of the VDS Act.
[39] For general information on the scheme see https://www.vic.gov.au/child-information-sharing-scheme.
[40] For general information on the scheme see https://www.vic.gov.au/family-violence-information-sharing-scheme.

account. In both these instances, Parliament has recognised the public interest and value in enabling information sharing to occur so that harm can be prevented and assistance provided to vulnerable cohorts.

(b) Permitted use and disclosure under the IPPs

Privacy legislation should also provide for instances of permitted use and disclosure of personal information beyond its primary purpose of collection – in effect permitting the sharing of personal information. In Victoria, IPP 2.1 outlines a number of circumstances that specifically permit the use or disclosure of personal information. These include:

- where the individual has consented to the use or disclosure;
- there is a reasonable belief that use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare, or a serious threat to public health, public safety or public welfare;
- the use or disclosure is necessary for an investigation into an unlawful activity, or in reporting an unlawful activity to relevant persons or authorities; and
- a number of other law enforcement purposes.

In the Victorian context, the IPPs do not override or replace existing authorities for information sharing under other legislation. The PDP Act is the default where an organisation is not bound by other information sharing provisions, such as within their own enabling legislation. However, if an organisation is required to comply with an information sharing provision in other legislation, that overrides any obligation or restriction on information sharing under IPP 2. Conversely, where another piece of legislation contains a secrecy or confidentiality provision, that provision will prevail despite information sharing authorities under the PDP Act.[41]

(c) Consent and information sharing legislation

As noted previously, while OVIC recognises that consent is an important mechanism for individuals to protect their privacy by allowing them to exercise control over their personal information (in certain circumstances), OVIC is of the view that consent may not always be practical or feasible in the context of information sharing legislation.

As noted in the Department of the Prime Minister and Cabinet's recent *Data Sharing and Release Legislative Reforms Discussion Paper* (**PM&C discussion paper**),[42] making consent a prerequisite for information sharing could have an adverse impact on the integrity of a dataset to be shared, and in turn undermine the purpose and intention of information sharing legislation.

When developing information sharing legislation, OVIC suggests a model where consent provides one avenue to permit information sharing, but is not the sole legal authority to allow the public sector to do so.[43]

---

[41] Section 6(1) of the PDP Act.
[42] Available at https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf.
[43] As has been noted, this is consistent with consent under the PDP Act, whereby it is one of several grounds under IPP 2 that permits organisations to use and disclose personal information.

Consistent with OVIC's view on consent under privacy legislation, if consent is obtained it must be meaningful and, in addition should only be sought where it is necessary. Seeking consent may appear disingenuous to the public where information can be shared regardless of whether or not consent is provided, under another authority provided by information sharing legislation or another law.

(d) Sharing for commercial or compliance purposes

The PM&C discussion paper also noted the concerns of stakeholders who had been consulted in relation to what may be considered legitimate purposes for data sharing. In particular, the PM&C discussion paper notes that the views of stakeholders were diverse when it came to allowing information sharing for commercial or compliance purposes. OVIC acknowledges that data sharing for research and development can bring benefits to the community. However, sharing for commercial purposes should only occur where it is in the public interest and, importantly, meet community expectations.

Notably, the PM&C discussion paper concludes that data will not be able to be shared for compliance and assurance activities under the proposed Commonwealth data sharing and release legislation.[44] OVIC agrees that information sharing legislation should not permit sharing for compliance or assurance activities. While these are legitimate functions of government, as the PM&C discussion paper points out, compliance activities should be carried out under the legislation that governs the agencies that undertake those types of activities.

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?

(a) Promote an information sharing culture

A key function of the Chief Data Officer should be to create and promote an appropriate information sharing culture in the public service. While legislation may exist that permits information sharing to occur, if there is no culture across the public sector that encourages appropriate information sharing, then that legislation will not achieve its desired purposes. This will require the Chief Data Officer to educate the public sector on the benefits of information sharing, provide appropriate guidance on how, when and for what purposes information sharing should occur, and promote safe information sharing practices.

(b) Undertake analytics on behalf of government

As is the case in Victoria, it is also suggested that the Chief Data Officer be empowered to undertake data analytics and research on behalf of government. The Chief Data Officer, or their office, would presumably be uniquely qualified to assist government in undertaking analytics on confidential or sensitive data in a secure and controlled environment. The Chief Data Officer could assist government to understand how data can address business problems, design solutions to those problems, develop data analytics and statistical models, and provide analytics solutions to inform policy making and service design.

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

(a) De-identification risks

In the context of the Five Safes framework, a component of 'safe-data' is a consideration as to whether the

[44] See page 25 of the PM&C discussion paper.

data has been de-identified or could be de-identified. OVIC notes that successfully de-identifying personal information (particularly unit-record level data) to the point where it is permanent or cannot be re-identified, is especially difficult. It is also very difficult to determine the likelihood of re-identification for any given data set, for example, through matching information with publicly available data sets or other data sets that may be available either within government or to trusted third parties.[45] OVIC suggests particular caution is given when sharing de-identified personal information, particularly with third parties outside of government, and the risk of re-identification is built into the risk management framework. OVIC's recent investigation into the review of purportedly de-identified data about public transport usage highlights the risk in this regard.[46]

(b) Privacy and data security enhancements from the VDS Act

As noted previously, the VDS Act promotes the sharing and use of public sector data to support government policy making, service planning and design.[47] The VCDI employs a number of privacy-enhancing techniques that OVIC suggests should be considered when drafting information sharing legislation, including:

- express privacy and data security safeguards under the VDS Act, including mandatory breach notification and annual reporting requirements to OVIC;[48]
- an additional layer of protection for data analytics conducted in a controlled environment, ensuring that reasonable steps have been taken to ensure that data no longer relates to an identifiable individual or an individual who can reasonably be identified before data analytics work commences;[49]
- the provision of a clear legislative framework for the sharing of public sector data only, as distinct from the open release of public sector data; and
- the employment of the Five-Safes Framework in the context of a secure environment to conduct data analytics.

In practice, the de-identification of personal information, in accordance with the 'safe data' element of the Five-Safes Framework, is just one of the security measures applied to the data under the Victorian model, as this model provides that all of the elements of the Framework, including 'safe people', 'safe settings', 'safe outputs' and 'safe projects' can likely be assured in a secure environment. This is not true for data that is released to environments where these elements cannot be assured or determined, such as public release.

[45] See OVIC, *Protecting unit-record level personal information*, May 2018, available at: https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf
[46] See OVIC's investigation report Disclosure of myki travel information, available at https://ovic.vic.gov.au/about-us/regulatory-action/investigations-audits-examinations/
[47] See section 1(b) of the VDS Act.
[48] Under sections 24 and 29 of the VDS Act, respectively.
[49] Under section 18 of the VDS Act.