Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D22/15580

30 June 2022

Department of the Prime Minister and Cabinet

Online submission

Submission in response to the Australian Data Strategy

Thank you for the opportunity to make a submission in response to the Australian Data Strategy (**the Strategy**).

My office, the Office of the Victorian Information Commissioner (**OVIC**), is the primary regulator for information privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

OVIC recognises that data is important to a digital economy that delivers benefits for Australians, businesses, and governments. Crucially, data must be handled in a way that respects and protects individuals' human rights.

Given our remit, our comments in this submission primarily relate to information privacy and information access. OVIC has provided substantive comments on information security in its submission to the Department of Home Affairs in response to the consultation on the National Data Security Action Plan (**Data Security Action Plan**).[1] As the Strategy discusses the Data Security Action Plan, this submission will highlight some of OVIC's previous comments on the Data Security Action Plan that are also relevant considerations for the Strategy.

Trust and protection

National Data Security Action Plan

As the only jurisdiction with legislated information security standards, Victoria is at the forefront of information security regulation in Australia. Since 2014, OVIC has been responsible for setting the Victorian Protective Data Security Standards (**Victorian Standards**), and monitoring and assuring the security of public sector information against the Standards, under the Victorian Protective Data Security Framework (**Victorian Framework**). Part 4 of the PDP Act provides authority for developing the Victorian Framework and setting the Victorian Standards.

The Strategy discusses the Data Security Action Plan, which is intended to deliver a comprehensive, whole-of-economy approach to all aspects of data security. Some of OVIC's previous comments on the Data Security Action Plan include the following:

- OVIC supports the Data Security Action Plan's intention to clearly articulate data security settings and requirements for stakeholders. The security landscape has become increasingly

[1] OVIC's submission is available here: https://ovic.vic.gov.au/wp-content/uploads/2022/06/Submission-National-Data-Security-Action-Plan-June-2022.pdf.

complex in recent years due to the wide range of legislation, frameworks, strategies, and policies. For example, the Strategy discusses some of the initiatives that Government has introduced to use, share and store data safely and securely, such as the Cyber Security Strategy 2020, the Government Hosting Strategy and Hosting Certification Framework, and the Protecting Critical infrastructure and Systems of National Significance reforms.[2] It would be useful if the Strategy provided more comprehensive information on the various initiatives that contribute to Australia's data security landscape, and explained how they interact with each other. For instance, the Strategy mentions there are rules that govern how government releases non-sensitive data or engages in data sharing agreements.[3] OVIC suggests adding further information on these rules to provide a clearer picture of Australia's overall data security settings.

- OVIC agrees that inconsistent definitions and misused terms contribute to confusion and uncertainty for stakeholders hence it is crucial to agree on key data security terms and concepts.[4] OVIC notes the Data Security Action Plan distinguishes between 'data security' and 'cyber security' with data security limited to the protection of digital information and digital systems and networks. However, 'data' is defined broadly in both the Data Security Action Plan and the Strategy to include non-digital information.[5] Additionally, the Data Security Action Plan appears to suggest that protecting the confidentiality, integrity, and availability of information and systems only applies to cyber security.[6] In OVIC's view, the Data Security Action Plan must clearly define key data security terms, explain the types of information and information systems to be protected, and the protective security domains that apply. Better insight into how government intends to handle data will improve the Strategy.

Public trust and transparency

The Strategy discusses the value of public trust in the ways government uses data. It mentions the Consumer Data Right (**CDR**)[7], the Privacy Act Review, and the Data Availability and Transparency Scheme as some of the initiatives government has undertaken to build and maintain public trust. Broadly, these initiatives are intended to give Australians greater control over their data, and enhance the protections on sharing and use of data held by government and businesses. The Strategy also highlights the importance of ethical and transparent data handling practices to building public trust.

Given that government and businesses often collect significant amounts of data including personal information from the public to deliver services and make public policy decisions, and given the public often has no choice but to provide the data, it is positive to see initiatives being implemented to give the public more control over their data. When government and businesses are transparent about their data handling practices, particularly the handling of personal information, individuals are empowered to make informed and meaningful decisions about the collection, use and disclosure of their personal information.

Transparency also helps government and businesses develop the social licence needed to collect, use, and disclose the public's information.

---

[2] Department of Prime Minister and Cabinet, *Australian Data Strategy*, page 29.
[3] Ibid page 30.
[4] Department of Home Affairs, *National Data Security Action Plan Discussion Paper*, page 18 https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf.
[5] Department of Prime Minister and Cabinet, *Australian Data Strategy*, page 10.
[6] Department of Home Affairs, *National Data Security Action Plan Discussion Paper*, pages 18 and 19 https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf.
[7] The multiple changes to the CDR rules since it was implemented, and in particular the changes to accreditation controls and so-called "joint accounts", have contributed to some concern among civil society groups, and may not have improved public trust.

Access to information

OVIC notes the Strategy misses the opportunity to discuss access to information, a critical driver of public trust. Freedom of Information (**FOI**) legislation gives individuals a general right of access to information held by government, with some exceptions, and places a corresponding duty on decision makers to provide detailed reasons when access is denied. Notably, while the central mechanism to access government information is through a formal FOI request, FOI legislation also facilitates and promotes the proactive and informal release of information.

OVIC is a strong advocate of releasing information proactively and informally, and only relying on formal FOI processes for complex matters that require the careful balancing of competing valid interests. In the last few years, OVIC has undertaken several research projects to better understand how Victorian Government organisations approach and administer their FOI obligations with a view to influencing agency culture to be open by design.[8]

FOI legislation promotes transparency and builds public trust as it enables the public to have better insight into government's activities and to scrutinise them. It increases citizen participation in government processes and promotes better informed decision making as it enables the public to hold government accountable, which is essential to public trust.

Given the above, OVIC suggests adding further content to the Strategy highlighting the importance of the relationship between transparency, information access and public trust and its impact on the Strategy.

Conclusion

Thank you once again for the opportunity to comment on the Strategy. I have no objection to this submission being published by the Department of the Prime Minister and Cabinet without further reference to me. I also propose to publish a copy of this submission on the OVIC website.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague Anita Mugo, Senior Policy Officer, at anita.mugo@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner

[8] Further information on OVIC's research into the culture of FOI in Victoria is available on OVIC's website here: https://ovic.vic.gov.au/freedom-of-information/enhancing-victorias-foi-culture-to-be-open-by-design/#ovics-role-in-influencing-behaviour-recommended-actions.