CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

27 May 2022

Department of the Prime Minister and Cabinet
PO Box 6500
Canberra ACT 2600
Australia

By email: digitaltechnologytaskforceinbox@pmc.gov.au

Dear Sir/Madam,

Submission on the Australian Data Strategy – The Australian Government's whole-of-economy vision for data

CPA Australia represents the diverse interests of more than 170,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

The Australian Data Strategy (the Strategy) covers a range of topics. One of our key concerns is that small- and medium-sized enterprises (SMEs) are not sufficiently addressed in the Strategy. To join the data economy, SMEs need support to build data skills and capacity. Their ability to access and maximise the value of data should be an integral part of the Australian Data strategy.

Our key recommendations are:

- Provide criteria against which the quality of data can be assessed and measured.
- Harmonise and simplify data access criteria/standards across different levels of government.
- Develop data retention and disposal standards and/or guidance informed by e.g., the ISO/IEC 27000 series.
- Publish best practice examples for SMEs outlining how to safely and effectively manage data.
- Mandate digital corporate reporting for listed entities.
- Develop a technology-neutral data ethics framework.
- Develop guidance on how to test systems regularly to ensure they operate safely and are fit for purpose.
- Improve the community's data literacy and establish a data culture through targeted up-and re-skilling of current workers and integrating 'data skills' into school syllabi.
- Introduce SME-specific measures to help them build and improve their data skills and capacity to use data in their business.
- Ensure that software providers clearly advise clients on data storage practices and location.
- Improve coordination between government entities and digital economy policy development and consultation.

Responses to the Issues Paper questions are included in the Attachment.

If you have any questions about this submission, please do not hesitate to contact Dr Jana Schmitz, Digital Economy Policy Lead at jana.schmitz@cpaaustralia.com.au.

Yours faithfully

GR Pflugrath

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy
Encl.

Attachment

Data quality and value

Data quality

We note that the Australian Data Strategy (the Strategy) only vaguely defines data quality. The government should provide criteria against which the quality of data can be assessed. As a point of reference, ISO/IEC 25012 (data quality model) could be used to establish data quality requirements, define data quality measures, or plan and perform data quality assessments. Additionally, having strong data quality assurance frameworks is paramount to making sure Australia's data driven economy and society can keep up with the pace of technological development.

Recommendation 1:

Provide criteria against which the quality of data can be assessed and measured.

Data sharing and access

The use of technology within government requires access to and sharing of data between multiple agencies, including between different levels of government. We note that different states and territories have their own sets of data access requirements. What is needed is the improvement of current data sharing practice and the setting of standards and norms. Likewise, data access should be made easier for organisations such as technology start-ups provided that they meet government requirements. In our submission to PMC's consultation on Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation, we propose harmonising and simplifying data access request criteria/standards across different levels of government.[1]

Recommendation 2:

Harmonise and simplify data access criteria/standards across different levels of government.

Data lifecycle management

The government should emphasise the need for businesses to engage in good data management. This should include data protection and security considerations, data quality maintenance, data storage, data availability, and secure disposal or de-identification protocols.

Feedback from our members and other stakeholders highlights that the lack of clear standards and/or guidance for the retention and disposal of data causes burden in form of rising storage costs and ongoing maintenance and security requirements for many businesses. Clear data retention and disposal standards and/or guidance will create significant efficiencies in data management and enhance data security. It will also provide transparency for the community about how data is being managed.

The government should consider the ISO/IEC 27000 (Information Technology) series and other jurisdictions' data policies and legislation (e.g. the European Union's General Data Protection Right's (GDPR) right to erasure ('right to be forgotten')).[2] Additionally, best practice examples outlining how to safely, effectively and efficiently manage data end-to-end will be useful for businesses, particularly for SMEs.

[1] The UK Data Standards Authority has published standards and guidance on how to improve data sharing across government. For more information, see UK Government (2021): Metadata standards for sharing and publishing data, available at: https://www.gov.uk/government/collections/metadata-standards-for-sharing-and-publishing-data (accessed on 10/05/2022).

[2] In CPA Australia's submission made in 2020 to the Senate Select Committee on Financial Technology and Regulatory Technology, we note that blockchain technology, for instance, does not allow for data to be modified or to be eliminated once it has been added to the blockchain. In turn, this implies that the database grows as new data is added. Considering the GDPR principles, as data can only be added to the blockchain but not be removed the "right to be forgotten" seems to be unenforceable. Besides the inability to erase "blockchained" data, blockchain technology's underlying append-only architecture is likely to defeat the purpose of the GDPR's data minimisation principle. Additionally, data added to the blockchain may have been added due to predefined purposes,

Recommendation 3:

Develop data retention and disposal standards and/or guidance informed by e.g., the ISO/IEC 27000 series.

Recommendation 4:

Publish best practice examples for SMEs outlining how to safely and effectively manage data.

Digital Corporate Reporting

We recommend that the government makes digital corporate reporting a standard practice in Australia for listed entities. CPA Australia commissioned research, titled Digital Corporate Reporting: Global Experiences from the G20 and Implications for Policy Formulations, indicates that many of the countries examined as part of the study have adopted digital financial reporting practices within their jurisdictions. The research also found that in contrast to digital reporting mandates, voluntary approaches have been associated with limited uptake. Given the benefits of digital financial reporting outlined in our research, digital financial reporting should be mandated in Australia as has been the case in the US and the EU.

Recommendation 5:

Mandate digital corporate reporting in Australia for public entities.

Data ethics and accountability

AI ethics principles

The Strategy refers to the Australian AI Ethics Framework and its principles. In light of businesses' increased uptake of various different technologies processing vast amounts of data, the government should consider developing a technology-neutral ethics framework and principles and encouraging its uptake through, for example, using procurement processes to only purchase AI that complies with the framework. Such a framework should increase business and community trust in the use of technologies to manage personal and commercial data.

Recommendation 6:

Develop a technology-neutral data ethics framework.

Assurance over algorithmic decision-making

With increased volumes of data and decisions being made by algorithms, technology users and the broader community need assurance that their data is handled and processed as intended. We encourage the government to develop guidance on testing the behaviour of and learning by algorithms to minimise and prevent risks.[3] See also our submission on Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation.

Recommendation 7:

Develop guidance on how to test systems regularly to ensure they operate safely and are fit for purpose.

however, it remains questionable whether the processing and utilisation of the initially added data also serves the same purposes when parties utilise this data for further and/or other decision-making processes.

[3] See the UK's Centre for Data Ethics and Innovation's (CDEI) AI Assurance Guide.

Data literacy and skills

Data literacy

We understand data literacy as the ability to collect, manage, analyse and use data both individually and in organisations. For individuals and businesses, it is crucial to gain a fundamental understanding of what an increasingly data-based economy means, e.g., how value can be created or intangible value generated from data and what role data can and should play in our daily life and business. To be data literate also implies being able to identify and mitigate risks posed by data and to enable the handling of data in an ethical manner.

Upskilling and reskilling

To establish a data culture, workers across all occupations need to be upskilled and, under certain circumstances, reskilled, so that all workers have a basic level of data literacy. Initiatives such as short and full courses delivered online and/or virtually are essential. Such courses should be developed in collaboration with industry.

Upskilling workers is not only about teaching them data skills, it's also about providing them with the 'tools' required for other employment opportunities and future jobs that may not exist yet.

Data skills will remove the fear of the unknown and are likely to awaken interest in developing new data-driven business models. To create and further develop relevant learning opportunities, courses and training, the government needs to implement comprehensive long-term monitoring of the population's data skills.

Early (school) education

All Australians should be equipped with data skills at an early age. Data literacy should be anchored in school syllabi and taught in an age-appropriate format. It's essential for pupils to learn data skills at an early age as they start to handle data early on, for example, by using social media and other open data platforms. They need to be able to make conscious decisions and learn how to be responsible with their own data.

Teaching data skills should not be restricted to a specific school subject but should be integrated into a wide range of subjects. Such aspirations require teacher training programmes to ensure their capability to teach data skills.

Recommendation 8:

Improve the community's data literacy and establishing a data culture through targeted up- and re-skilling and integrating 'data skills' into school syllabi.

SMEs

SMEs often lack resources (time, human, financial) to offer on-the-job training for their employees or for the business owner.[4] The government should consider measures to build SMEs' data skills and capacity through:

- **Strategic outlook development**: Aimed at increasing the understanding of the strategic business opportunity of enhancing/improving employees'/owners' data literacy.
- **Strengthening SME ecosystems**: Being connected and embedded in existing advice means that regional, or sectoral support structures are essential for SMEs' data skills development. SMEs need to be embedded in networks comprised of their professional adviser/s, other SMEs, technology vendors, innovation hubs and education providers. They also need to have access to relevant support (knowledge, guidance, learning and tools).
- **Tailoring training to SMEs' needs**: Increase education and training offers. Build sustainable training offers that match SMEs' needs (content, form, set-up). Collect intelligence to increase understanding of SMEs' needs. Reduce direct costs for training for SMEs.

We make further recommendations on how to enhance SMEs' digital literacy in our submission on Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation.

[4] See also CPA Australia's 13th annual Asia Pacific Small Business Survey that shows that Australia's small business sector lags the region in tech adoption.

Recommendation 9:

Introduce SME-specific measures to help them build and improve data skills and capacity to use data in their business.

Data infrastructure and safeguards

Data security

We appreciate that the Department of Home Affairs is currently consulting on the National Data Security Action Plan which acknowledges that SMEs are particularly vulnerable to data breaches, due to a lack of resources, capability and expertise to manage data security risks. The government needs to invest resources in developing data security standards and/or guidance to minimise inconsistencies, prevent malicious actors from taking advantage of SMEs and encourage greater use of data in business decision making (CPA Australia's Business Technology Report 2021 found that concerns over cybersecurity and data privacy were key barriers to technology adoption).

We agree that government, industry and the community share responsibility for keeping data secure. We support the adoption of secure by design principles by manufacturers and software developers, to better support consumers and SMEs to strengthen their cyber security and protect their data.

Data infrastructure and storage

Data storage is a critical data infrastructure matter. Feedback we received from our members shows that businesses have limited transparency over how their data is being stored by software providers. Software providers may or may not store commercial and personal data in Australia. Data stored overseas may be subject to both the legal jurisdiction and privacy regulations of the country in which it is stored.

Businesses unaware of their software providers' data storage practices could be placing their business and their customers at risk. Therefore, it is crucial for business owners to know and be comfortable with the storage practices of their software provider(s). The government must ensure that software providers clearly advise their clients (business owners) as to where they store their data. If the provider stores client data overseas, business owners must be made aware that some countries may allow access to stored data for purposes of law enforcement and national security.

Recommendation 10:

Ensure that software providers clearly advise clients on data storage practices and location.

Data policy development

What is required is better coordination between government agencies and better linking-up of policies related to data across government. Currently many 'data issues', such as data security (e.g. National Data Security Action Plan), data sharing (e.g. Statutory Review of the CDR) and technology-specific 'data use' (Automated decision making and AI regulation), are explored separately with government focusing on one thread at a time. Further, data-specific regulation and policies should be technology neutral.

Recommendation 11:

Improve coordination between government entities and linking-up of digital economy policy development and consultation.