10 June 2022

Department of Home Affairs
6 Chan St
Belconnen ACT 2617

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

By email: techpolicy@homeaffairs.gov.au

Dear Sir/Madam,

Department of Home Affairs' National Data Security Action Plan – Issues Paper

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.

Noting that the National Data Security Action Plan (the Plan) is the first ever plan to enhance the nation's data security and better prepare individuals, businesses and government to manage and secure data in an increasingly digital economy, we believe the Issues Paper raises valid and relevant questions and concerns. To help the Department to define the overall direction of the Plan, we suggest that it considers:

- working collectively with other jurisdictions on improving regulatory interoperability and developing harmonised data security standards/frameworks.
- critically evaluating international data security frameworks and assessing their fit for the Australian context.
- delivering guidance in a targeted manner, taking into consideration the needs of and communication channels used by different stakeholder groups.
- developing minimum data security standards/rules complemented by guidance.
- performing in-depth assessments of the potential implications data localisation rules may have for public sector entities and businesses.
- allocating oversight responsibilities of local government councils' and agencies' data security to the OAIC and/or the National Office of the Data Commissioner.
- introducing specific measures to help SMEs build and improve their understanding and uptake of data security practices.
- developing and publishing a register listing technology-vendors that offer data management solutions with integrated data security safeguards.
- developing and providing resources that assist businesses to identify and address data security risks in supply chains.
- publishing guidance material that is fit for purpose and tailored to businesses' size, risk and complexity of operations.
- requiring government agencies and businesses not covered under the Privacy Act 1988 to report data breaches to government and the OAIC, although not making this information available to the general public.

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

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy

Encl.

Attachment

Consultation questions:

1. What do you consider are some of the international barriers to data security uplift?

The domestic regulatory and practical data security complexities are opaque for most individuals and businesses. Therefore, we find it interesting that the first consultation question addresses international perspectives when the focus should be on how to bring Australian data security, data access and data sharing frameworks into closer alignment to support local businesses uplift their data security measures.[1]

At the international level, different jurisdictions impose different data security requirements, and there is no standard approach to how data security and data management including the collection, access, utilisation, transfer, storage and deletion of data, should be handled.[2] By way of example, the European Union's (EU) General Data Protection Regulation (GDPR) has specific requirements such as the use of standard contractual clauses and conducting transfer risk assessments (TRAs) for any data that is leaving the EU. On the other hand, China's Personal Information Protection Law (PIPL)[3] includes a strict data localisation principle and only permits data transfers in very limited circumstances (see also our response to **Q5**).

Different jurisdictions require the implementation of different measures to ensure the security of the data to be processed/transferred. In other words, while some data security safeguards may work for one jurisdiction, they may not fulfil the requirements of other jurisdictions. These interoperability issues and lack of harmonised data security standards must be overcome.

Recommendation 1: Consider working collectively with other jurisdictions on improving regulatory interoperability issues and developing harmonised data security standards/frameworks.

See also our response to **Q2**.

2. How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?

Rather than identifying and applying international frameworks to Australian regulation, the government should conduct a comprehensive analysis of Australia's data security needs and requirements. More precisely, the government should decide what Australia's domestic data security 'baseline' should be. It should also develop a thorough understanding of international frameworks first, before consulting on their applicability to Australia. The latter is of great importance as frameworks such as the GDPR have shortcomings. For example, technologies such as blockchain and artificial intelligence, which are increasingly being used by individuals, businesses, and public sector entities, challenge certain GDPR principles such as data elimination and data minimisation.

Blockchain, for instance, does not allow for data to be modified or to be eliminated once it has been added to the blockchain. Considering the GDPR principles, Article 17 of the GDPR ("right to be forgotten") seems to be unenforceable. Additionally, blockchain's underlying append-only architecture is likely to defeat the purpose of the

---

[1] See also CPA Australia's submission on PMC's the Australian Data Strategy – The Australian Government's whole-of-economy vision for data.

[2] See also Department of Prime Minister and Cabinet (2022): Australian Data Strategy Consultation Paper, available at: https://ausdatastrategy.pmc.gov.au/sites/default/files/2021-12/australian-data-strategy.pdf (accessed on 7 June 2022).

[3] For the original legislative document (in Mandarin), see: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed on 7 June 2022).

GDPR's data minimisation principle (see Article 5(1)(c).[4] In the context of AI, situations where personal data should be deleted due to the obligation to erase collected personal data that enabled the development of algorithmic models, give reasons for concerns. Erasing the data used for constructing an algorithmic model may make it difficult or impossible to demonstrate the correctness of that model.[5]

Businesses that trade with European nations are well placed to provide informed views on this consultation question as they are required to be comply with GDPR principles. Individuals and most SMEs would be unaware of the implications of Australia utilising GDPR principles for its own data protection framework.

Overall, some GDPR principles need to be critically assessed for their suitability for Australia. The government must avoid "copying and pasting" what other jurisdictions do. It is more important to critically assess international frameworks for the cultural fit to assure the suitability of international frameworks for Australia.

Recommendation 2: Critically evaluate international data security frameworks and assess their fit for the Australian context.

3. What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?

Additional guidance should come from a position of support. Many SMEs are lagging behind their larger counterparts in keeping data secure. This is due to several factors such as resource constraints and the limited uptake of digital technology solutions.[6]

We note that the government has made a multitude of resources available on its websites, however, individuals and businesses may not be aware of them. Resources and guidance must be delivered in a targeted manner, which demonstrates to specific groups (such as elderly people or small businesses) that they are understood and their needs are addressed.

Delivering guidance to specific groups includes identifying the best communication channel to reach those groups. For instance, younger and technology-savvy generations could be addressed through social media platforms, whereas elderly individuals may respond better to more traditional ways of communication such as emails and/or letters. Further, while larger businesses may have the resources available (human and financial) to invest in looking up and acting on government guidance, SMEs often are time-poor and budget-constrained. For SME-specific communication avenues and measures, see CPA Australia's submissions on the Australian Data Strategy – The Australian Government's whole-of-economy vision for data and Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper.

Further, additional government guidance should unpack several concepts related to data security. This would help individuals and businesses gain a better understanding of the importance of keeping data safe. For example, the concept of 'control' should be elaborated on. Control is relative to the perceptions of the data owner, the intention of the data user, the context within which data is applied and the potential impact of the application of that data.

Recommendation 3: Deliver guidance in a targeted manner, taking into consideration the needs of and communication channels used by different stakeholder groups.

---

[4] The principle of "data minimisation" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose.

[5] For more information see European Parliament (2020): The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, EPRS – European Parliamentary Research Service, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (accessed on 6 June 2022).

6 For more information, see Business Australia (2022): Almost Half of Australian Cyber Attacks Hit SMEs, available at: https://www.businessaustralia.com/resources/news/almost-half-of-australian-cyber-attacks-hit-smes (accessed on 10 June 2022), and CPA Australia's 2021-22 Asia-Pacific small business survey results, available at: https://www.cpaaustralia.com.au/tools-and-resources/business-management/small-business-resources/asia-pacific-small-business-survey (accessed on 10 June 2022).

Feedback provided by our members and other stakeholders indicates that a principles-informed approach is unlikely to be effective in enhancing businesses' data security practices. What is required is a set of (minimum) data security standards/rules businesses should be required to comply with. Like other jurisdictions that have legislated data security (e.g., China and the European Union), Australia should consider the improvement of the nation's data security as an important infrastructure investment. Cross-jurisdictional and cross-sectoral rules are needed to effectively improve data security in Australia. Guidance that is "best align[ed] with international data protection and security frameworks" (see **Q1**) should be complementary to data security standards.

Recommendation 4: Consider developing minimum data security standards/rules complemented by guidance.

4. How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market?
a. What obligations are you most commonly subjected to from international jurisdictions?

At the national level, data access, sharing and protection policies and frameworks across states must be brought into alignment before addressing how data security policy measures could be streamlined to better align with international frameworks. See also our responses to **Q1** and **Q2**.

a. Obligations to which our members and other stakeholders are most subjected from international jurisdictions are data privacy and data sharing permissions. They highlight that restrictions on international data transfers are not only imposed by the jurisdictions to which the data is sent. Businesses must also address the regulations of the jurisdiction from which the data originates, as well as the controls in place among third parties that may process or otherwise interact with the data.

5. Does Australia need an explicit approach to data localisation?

Several jurisdictions such as Germany (and other European countries) and China have implemented laws that require certain data to be stored on physical servers within the jurisdiction's borders. In other jurisdictions, data localisation or data sovereignty laws only apply to certain sectors and industries, such as government agencies and military contractors.

While we understand that data localisation rules seem beneficial from a national security perspective, we note that they may limit collaboration between law enforcement, intelligence, and other security actors by creating obstacles to accessing certain information across borders. For businesses, data localisation rules would increase costs. Even if certain businesses were not directly affected by data localisation laws, their customers or suppliers may be. This could have ripple effects both up and down the supply chain.

There is no "one size fits all" outcome for data localisation rules. Government should assess the potential implications of data localisation rules and hold in-depth conversations with public sector entities and businesses operating in different industries.

Recommendation 5: Perform in-depth assessments of the potential implications data localisation rules may have for public sector entities and businesses.

6. How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?

See our responses to **Q1** and **Q2**.

7. Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened? Do you think responsibilities should be shared across more bodies, or shifted elsewhere entirely?

To our best knowledge, the uplift of data security by local governments is currently not overseen by one single authority or body.

We note that the Privacy Act 1988 (currently under review) doesn't cover state and local government agencies, such as public hospitals and public schools. However, hospitals hold some of the most sensitive data.

For public sector entities in Victoria, Part 4 of the Privacy and Data Protection Act 2014 (PDP Act) sets out the information security obligations of Victorian public sector agencies under the Victorian Protective Data Security Framework (VPDSF). Councils are expressly exempt from Part 4, although, where a council performs the functions of other public entities captured by Part 4, any information relevant to those public functions will be subject to Part 4 of the PDP Act.

According to Information Privacy Principle (IPP)[7] 4.1, councils are required to take 'reasonable steps' to protect personal information from misuse, loss, unauthorised access, modification and disclosure. IPP 4.1 also states that organisations should anticipate foreseeable security risks to the personal information they hold and take reasonable precautions to protect the information from those risks.

Given the increasing amounts of sensitive data many local government councils and agencies hold, we believe that it will become gradually more challenging for those agencies and councils to take 'reasonable steps' to protect the data and to foresee security risks. Therefore, we suggest that the government considers imposing stricter data security obligations on local government councils and agencies. Councils and agencies across all states and territories should be subject to the same data security rules.

In our view, the government should consider allocating the responsibility to oversee local government councils' and agencies' data security practices to the Office of the Australian Information Commissioner (OAIC) and/or the Office of the National Data Commissioner. Both authorities are equipped with the relevant skills and regulatory powers.

Recommendation 6: Consider allocating oversight responsibilities of local government councils' and agencies' data security to the OAIC and/or the National Office of the Data Commissioner.

8. What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?

Some of the main challenges faced by businesses are costs and time spent requesting data access from public sector entities across all levels. What is needed is improvements to current data sharing practices and the setting of standards and norms. Likewise, data access should be made easier for organisations such as technology start-ups if 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.[8]

See also our response to **Q7**.

9. Which steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?

[7] The IPPs are the core of privacy law in Victoria and set out the minimum standard for how Victorian public sector organisations should manage personal information.

[8] 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).

See our response to **Q10**.

10. How can the Australian Government further support your business to understand the value of data and uplift your data security posture?

Overall, business data literacy must improve.

As noted in our submission on the Australian Data Strategy, data literacy is the ability to collect, manage, analyse, store, and use data. SMEs in particular often believe that the data they collect and process is not of sensitive nature. Due to their limited understanding of data and security obligations, they often do not have sufficient data security safeguards in place.

We highlight that the current economic situation makes it increasingly difficult for SMEs to invest in up- or re-skilling their staff. Therefore, we urge the government to provide support in form of, for instance, short courses made available online.[9]

Recommendation 7: Introduce specific measures to help SMEs build and improve their understanding and uptake of data security practices.

Moreover, given businesses' increasing use of third-party vendors offering data processing, storage and transfer solutions enabled by technology (e.g., data analytics, artificial intelligence, machine learning and others), the government could encourage businesses to deploy IT solutions that have integrated data security measures.

Such "security by design" principles set a baseline for robust data protection. It embeds security safeguards into the design, operation, and management of data applications, including IT systems, AI platforms, and digital business practices. The goal is to prevent privacy and security breaches. To help businesses source technology solutions with integrated data security measures, the government should consider publishing a register listing third-party vendors offering services with in-built "security-by-design".

Recommendation 8: Consider developing and publishing a register listing technology-vendors that offer data management solutions with integrated data security safeguards.

11. Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by Government to help your business identify these risks?

We do not believe that businesses appropriately consider data security risks in their supply chains. In our submission to the Department's consultation on Critical Technology Supply Chain Principles, we suggest that government should encourage business to focus their attention on technology solutions that allow for the secure engagement with and exchange of data with other relevant supply chain participants. See also our response to **Q10**.

Moreover, we suggest that the government should provide case studies, examples and education material elaborating on supply chain data security risks and how to overcome them. Such case studies should include examples of third-party software providers and data storage services. By way of example, the United Kingdom National Cyber Security Centre (UK NCSC) provides case studies supporting its Supply Chain Security Guidance.

Recommendation 9: Develop and provide resources that assist businesses to identify and address data security risks in supply chains.

[9] For more SME-specific measures, see CPA Australia's submissions on the Australian Data Strategy – The Australian Government's whole-of-economy vision for data and Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper.

12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold.

What is needed is "fit for purpose" guidance not a blanket approach.

The size of the business, its resources, the complexity of its operations, its industry and its business model, are all relevant to determining what steps are required to protect the personal data the business holds. For instance, a franchise, e-commerce business or a business using outsourcing is likely to provide access to its personal data to third parties (franchisees, technology vendors, contractors). The reasonable steps it takes may be different to those it would take if it did not operate in this manner.

Thus, as a first step, guidance material should require businesses of all sizes to gain a better understanding of the nature of the data they collect and the processes they take to collect that data. This may require the conduct of data risk assessments. Questions businesses should ask themselves could include:

- Who sends sensitive personal information to your business? Do you get it from customers, credit card companies, banks or other financial institutions or businesses?
- How does your business receive personal information? Does it come to your business through a website / by email or mail?
- What kind of data do you collect at each entry point? Do you get credit card information online? Does your accounting department keep information about customers' accounts?
- Where do you keep the data your business collects? On an inhouse server, individual laptops, cloud service, employees' smartphones, tablets, or other mobile devices? Do employees have files at home?
- Who has – or could have – access to (personal) data? Which of your employees has permission to access the data? Do contractors and/or vendors who supply and update software you use have access to data?

Further, we note that larger businesses in Australia have been actively pursuing data security with significant resources including technology, people, and budgets. As a result, they have become much more difficult target for hackers and cyber criminals, who are now focusing more of their attention on less secure SMEs. Hence, there is a strong need to issue guidance addressing SMEs' data security challenges.

The guidance material should also aim to improve SMEs' understanding of the nature and impacts of data. This is particularly relevant for SMEs that are often (unknowingly) dealing with sensitive data. For SMEs, it is most important that the guidance material is easy to comprehend and implement. The government should consider structuring and presenting data security guidance for SMEs in a similar way to the ACSC's various sources and step-by-step guides for SMEs.

Recommendation 10: Publish guidance material that is fit for purpose and tailored to business size, risk and complexity of operations.

13. Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

Factors hindering business implementation of an enhanced data security regime include time and budget constraints, implementation and compliance cost, and a lack of understanding of risks. See also our responses to **Q3** and **Q12**.

14. Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?

As outlined in our response to **Q3**, existing government resources must be made visible to individuals (and businesses) and be communicated in a targeted manner. It is also crucial to provide information that is easy to comprehend and apply. Best practice case studies will be helpful in enhancing consumers' data security awareness.

Apart from the availability and dissemination of public information and guidance, the government should continue to raise awareness about the growing importance of data security and how it affects individuals' daily lives and business performance.

15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

Government agencies' unauthorised disclosure of (sensitive) data about citizens and businesses, whether accidental or through the result of malicious actors, can result in tangible harm and eroded trust in the public sector. Whilst we acknowledge the need to enhance government's accountability for data breaches, we highlight that the (enforced) public disclosure of such breaches would likely draw malicious actors' attention to hacked government entities.

Further, we note that under the Notifiable Data Breaches (NDB) scheme, any organisation or government agency the Privacy Act 1988 covers must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.[10] In our view, the government should consider requiring organisations and agencies not covered under the Privacy Act 1988 (see also our response to **Q7**) to report breaches to government and the OAIC as a way for those authorities to better understand common issues and trends. Information about those breaches should not be made available to the public in order to avoid attracting hackers to affected businesses and government agencies.

Enhancing the accountability of government entities and business for data breaches will incentivise an uplift of data security measures and safeguards.

Recommendation 11: Consider requiring government agencies and businesses not covered under the Privacy Act 1988 to report data breaches to government and the OAIC, although not making this information available to the public.

[10] For more information, see OAIC (2022): About the Notifiable Data Breaches scheme, available at: https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme (accessed on 9 June 2022).