27 June 2022

Data Security and Strategy
Technology Policy Branch
Digital and Technology Policy Division
Department of Home Affairs

Dear Data Security Team

Data Security Action Plan Discussion Paper

The Australian Banking Association (ABA) welcomes the opportunity to provide input to the Data Security Action Plan Discussion Paper (discussion paper).

Effective protection of data, whether it's personal information or commercial or financial data, is integral to everyday activities and underpins businesses and consumers' trust in Government and the digital economy. Data security is also an important aspect of a nation's cybersecurity resilience. The banking industry has worked with the Department of Home Affairs on critical infrastructure and cybersecurity initiatives, and would welcome the opportunity to do the same on data security.

ABA's response draws on members' experiences and insights into creation, transfer, storage, use and on-provision of data, including across national and regional borders. Banks understand the importance of data protection as a key factor underpinning customer trust. ABA's key recommendations are:

- The Government's data security policy should seek to protect data commensurate with its sensitivity and the harm that can result from its compromise, unauthorised- or mis-use.
- The data security should apply consistently to all levels of Government (Commonwealth, state and local), via harmonised legislation and regulations, policies and practices.
- In applying the data security action plan to the private sector, identify regulatory actions to incentivise and support the private sector to enhance data security. Regulatory actions can take different forms including legislation and guidance.
- Identify opportunities for the Australian government to advocate for greater consistency in the data security and privacy laws of key overseas jurisdictions, which would enable security uplift for Australian entities that deal with overseas third parties or with cross-border activities.

ABA's submission includes a summary of the industry's views and proposed action that can be undertaken by Government, followed by detailed responses to the consultation questions in the discussion paper.

Yours sincerely

Rhonda Luo
Policy Director

Australian Banking Association

Summary

Defining the policy objectives and spheres of action

Data is increasingly a core part of many sectors of the economy, and integral to everyday consumer and economic activities. Cyber security is increasingly a top priority issue for industries, regulators and multiple government agencies. This environment has potential for fragmented, inconsistent or even conflicting data security requirements across different regimes or sectors, which can create weaknesses in Australia's data security and cyber resilience. The discussion paper seeks feedback on the broad range of risks and potential ways to enhance data security.

Policy objective

ABA considers the key policy objective of the data security action plan should be to protect data commensurate with its sensitivity and potential harm. In more specific terms, this may mean adopting a policy position of data flowing but ensuring effective protections apply to sensitive data (including personal information), and any exemptions or restrictions on data flows meeting genuine public policy or national security objectives without being discriminatory or restricting trade.

Applying this policy objective to all data including data about individuals, customers, private and public sector, would enable the banking industry – as well as the government and other industries – to adopt a consistent, strategic view of how to protect customer data.

Spheres of action

The data action plan should seek to achieve this policy objective in a consistent and harmonised manner across the public and private sector to maximise the effectiveness of data security uplift. This means the Commonwealth government can take actions in three areas:

- Finding ways to give effect to the data security policy in a consistent and harmonised manner across all levels of government: Commonwealth, state and local.
- Identifying regulatory actions to incentivise or support the private sector to enhance data security. Regulatory actions can take different forms including legislation and guidance.
- Advocating for greater consistency in data security and privacy laws of key overseas jurisdictions, which in turn affects Australia's capacity to adopt consistent and higher data security standards.

In terms of regulatory action, ABA suggests the Government consider whether the risk arises from:

- Gaps or loopholes in existing domestic law dealing with collection, retention, use and disclosure of data that may create a risk or do not address a risk.
- Non-compliance with existing laws, which may highlight a weakness in enforcement of the law or a need for clearer guidance, rather than a case for further law reform.
- Hacking or other unauthorised access, which may point to a technological weakness that the entity or a third party provider can address and/or a case for strengthened standards or regulation, under a private-public partnership approach.

Identifying the nature of the risk can help to identify the most appropriate mitigant. In some but not all scenarios, questions about the impact of overseas laws or geopolitical considerations may arise.

Implementing the data security action plan

When implementing the government data security policy, ABA cautions against relying on new, stand-alone legislation to impose data security requirements across the Australian economy. Instead, consider whether existing legislative vehicles can be used and/or how to ensure harmonisation between data security policy and existing requirements.

- The *Privacy Act 1988* (Privacy Act) and other legislation dealing with personal information.
- Sector-specific or activity specific legislation that also impose their own privacy, information security and risk management or outsourcing requirements. In some cases such as in banking and financial services, multiple existing regulatory regimes may already apply to one entity or the entity's activities. Regulations may require regulated entities to seek assurance from third party providers about their compliance, as is the case under Australian Prudential Regulation Authority (APRA) prudential standard CPS 234.
- Many businesses - as well as government entities - may have activities that are also captured under overseas law.

Data security in the banking sector

Banks are subject to a range of existing requirements and legislative regimes impacting data security:

- The Security of Critical Infrastructure (SOCI) Act requires critical infrastructure assets to have risk management programs, and for systems of national significance to have enhanced cyber security obligations. These obligations apply to banking assets unless the Minister has determined that banking assets are subject to equivalent sectoral regulation.
- Banks are subject to general legislation including the Privacy Act, and enhanced privacy safeguards in specific regimes such as the Consumer Data Right.
- Banks are subject to an extensive range of prudential and other regulatory obligations relating to risk management, information security, outsourcing. Refer pages 2-4 of ABA's submission to the discussion paper, *Protecting Critical Infrastructure and Systems of National Significance* (October 2020).[1]
- Banks have specific processes in place to deal with specific national security issues, such as addressing the risks associated with Politically Exposed Persons as part of a bank's anti-money laundering program.[2]

Key considerations for the banking industry, and potentially other highly regulated industries, are:

- Consistency between general and specific legislation and regulations, particularly with prudential standards made by APRA.
- Specifically, clear and consistent expectations from Government and regulators about managing the risks associated with outsourcing. The Government may also wish to consider the circumstances in which direct regulation of outsourced providers may be appropriate – noting the SOCI Act goes some way in this direction, and proposed regulations in the UK would give the Prudential Regulation Authority rule-making powers and some oversight over ‘critical third parties’.

Privacy Act and other data protection regimes

The Privacy Act is the key piece of legislation dealing with personal information in Australia, though it has some exemptions for state and territories governments and small business. The Privacy Act and Australian Privacy Principles (APP) address some of the issues raised in this discussion paper. APP 8 applies to sending personal information overseas, including disclosure to an overseas entity that is subject to a substantially similar law or binding scheme – to date the OAIC has not issued a list of countries that meet this requirement. APP 11 deals with the security of personal information.

---

[1] Available at: https://www.ausbanking.org.au/wp-content/uploads/2020/10/20200916-Ci-SoNS-ABA-submission.pdf

[2] See AUSTRAC, Politically Exposed Persons (PEPs): https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/politically-exposed-persons-peps

The Attorney-General's Department is currently undertaking a significant review of the Privacy Act. It would be more efficient and effective, and facilitate better compliance, for the Privacy Act and the Government's data security policy to align with each other. In particular, any prohibited use or disclosure of data for data security objectives should be consistent with the requirements under the Privacy Act and relevant APPs.

ABA also notes other specific legislative regimes contain additional provisions dealing with company or personal information, such as in the Consumer Data Right and proposed digital identity legislation. Similar considerations for consistency and alignment may apply.

Public sector data security

The public sector – comprising Commonwealth, state and local governments – make up a significant part of our economy. Data security in the public sector merits specific consideration for a few reasons:

- Public sector entities and authorities frequently have the legal power to compel individuals and businesses to provide data, or require businesses or individuals to provide data or personal information to carry out activities or obtain credentials.
- Commonwealth and state legislation often permit public sector entities to share information with each other (including from Commonwealth to state), or with third parties.
- State governmental entities are exempt from the Privacy Act.

For the banking industry, Australians hold a high level of trust in the banks manage their data, relative to other industries . Banks need assurance that the same level of protection will be maintained when sharing customer data with government agencies.

These factors make it crucial for the public sector to have robust data security, to maintain public confidence in Government, protect Australian businesses and safeguard citizens' personal information, credentials and identity. Investing in data security across all levels of Government is key to realising the data security action plan. Capability uplift may be particularly valuable for local governments that hold detailed data about residents and businesses, but may have fewer resources to invest in data security.

In addition to investing in enterprise information security, we call for action in two areas:

- Going beyond the security classification system, having consistent and rigorous policies to determine who should be able to access each set of sensitive or confidential data based on roles and responsibilities (ie, not every employee across the Commonwealth with a Top Secret clearance should have access to all data classified to that level).
- Enhancing requirements for governmental entities to review the data security capability and policies of entities that receive data and information from public sector entities, including those who may receive data under the *Data Availability and Transparency Act 2022*.

International context

Data localisation

The discussion paper asks questions about the impact of overseas laws and specifically about the merits of a data localisation requirement. The discussion paper identifies the concern that certain information may pose national security threats if transferred overseas, and the additional consideration that keeping data onshore can mitigate the impact of outages in overseas data centres.

The concept of data localisation can seem attractive as it can be viewed as a way to reduce dependencies on other countries, and to give regulators greater visibility into where data is stored and who it's shared with. However, ABA cautions against a general policy or prohibition on storing or moving data offshore.

- This practice may not safeguard against hacking and other cyber attacks, which by their nature is a borderless crime.

Australian Banking Association

- The discussion paper recognises other potential economic or trade detriments of a broad data localisation requirement. Data localisation can also weaken data security.
  - Many Australian entities use third party providers of software or platform services, including major global entities. Both Australian and overseas entities may use offshore data centres. Requiring data to be kept onshore would disrupt these existing commercial and infrastructure arrangements.
  - Data location is likely to require many entities to segregate data and maintain data infrastructure in more locations. This outcome can create additional security requirements (such as physical and staff), add complexity to a large entity's cybersecurity systems (with complexity in itself a potential source of weakness), while losing access to offshore data infrastructure that may be best-in-class.
- Australia's experience has shown that offshore data storage can be consistent with ensuring Australian regulators continuing to have full and timely access to the data needed to fulfill their regulatory and supervisory mandate.

ABA also highlights specific existing cross-border, regional and international arrangements and trade policies:

- Raising barriers to data flows can run counter to the government's stated policy objectives. The International Cyber and Critical Engagement Strategy notes that 'Australia seeks to shape an international environment that enables digital trade and reinforces the international rules-based trading system. Essential to this is the reduction of digital trade barriers, such as data localisation requirements and data flow restrictions'.[3]
- Consistent with this strategy, Australia is one of several countries leading the world in negotiating free trade and digital trade agreements that include clauses allowing for the free flow of data across borders. Two examples are the Singapore Australia Digital Economy Agreement and the Australia UK Free Trade Agreement. Cross border data flows is seen as a significant enabler of trade and requires a consistent policy approach.

ABA welcomes the discussion paper's proposed approach to consider how the Government can proportionately uplift security of citizens' personal information, while balancing the opportunities presented by international data flows and the global economy. Per above, ABA highlights *responsible* cross-border movement of data can be beneficial to data security and thereby national security.

- Responsible cross border data movement can be achieved in a range of ways, including using mechanisms in existing law.
- ABA encourages the Government, as part of the data security action plan, to identify factors that may make an overseas jurisdiction suitable or unsuitable for storing sensitive data about Australian citizens, and introducing a 'white list' of jurisdictions under the Privacy Act APP 8.
- If the Government proposes to distinguish between overseas jurisdictions, ABA suggests drawing a distinction between laws that govern privacy and commerce, and national security laws. For example, the EU is commonly regarded as having robust privacy laws under the General Data Protection Regulation (GDPR), however may have surveillance laws that give national security agencies powers to obtain access to data.
- Another, potentially complementary, approach is to introduce robust data security and associated controls, in line with international standards, to ensure appropriate protection and controls of data and an entity's operations.

[3] Available at: https://www.internationalcybertech.gov.au/our-work

International alignment

The discussion paper asks about international barriers to data security uplift. Any misalignment between Australian law and those of key overseas jurisdictions can create barriers to enhancing data security. As an example, Australian entities that rely on large, global, third party service providers or deal with overseas counterparts may experience difficulties using contract to ensure these third parties comply with Australian domestic requirements. These difficulties can be heightened where there are differences between the laws of key overseas jurisdictions, including Australia's key trading partners and security partners.

For these reasons, any initiative to enhance harmonisation between key overseas jurisdictions and/or the adoption of international standards would help the Australian government and businesses to take a robust, strategic view of data security.

In addition, while these differences do not pose an absolute barrier to cross-border commerce, they can raise the barrier to such activity and result in missed opportunities for Australia. Where Australian entities are directly subject to overseas data security or privacy laws, they face the resource intensive task of reconciling potentially significant differences between their domestic and overseas data obligations. in these circumstances, guidance about how Australian entities can comply with overseas laws can help to reduce the barriers to trade.

Finally, ABA encourages the Government to take opportunities to influence regional or international initiatives to harmonise privacy and data security regulations and promote responsible cross-border movement of data.[4]

Responses to consultation questions

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

Consistent with the summary:

- Legally, data localisation requirements under overseas laws create challenges for businesses operating globally and lack of global interoperability between regulatory requirements and infrastructure.
- Lack of alignment between Australian law and international standards, and a lack of consistency in international standards. ABA would support the Government seeking greater alignment between major jurisdictions.
- On a practical level, there can be an imbalance in negotiating power between domestic providers and large international third party providers. International providers may use their bargaining power to push back on contractual obligations that reflect Australian standards including on data security, and which Australian-based providers are subject to.

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)?

Per the summary, we suggest Government ensuring that Australian legislation and regulations do not hinder alignment with international / technical standards.

In many instances, legislation itself can be a reason for misalignment over time if legislation is detailed or prescriptive, and requires compliance with a particular technical standard. Legislative drafting best practice may require legislation or regulations to refer to the standard as it existed in a point in time,

[4] For example, while this initiative currently has limited application including for financial institutions, the APEC Cross Border Privacy Rules system (CBPR) is a scheme which helps advance the objectives of secure transfer of data across borders, while ensuring privacy and security. The Global CBPR forum is seeking to extend secure data transfer regimes beyond the APEC region and currently consists of the US, Canada, Japan, Korea, the Philippines, Taiwan and Singapore. See: http://cbprs.org/

rather than as the standard may be updated from time to time. This creates a significant risk that regulatory requirements can become misaligned from technical standards or instruments over time.

In relation to the GDPR and Australian government guidance, we note the GDPR is a detailed legislative regime on privacy, which includes a high level requirement relating to data security. It may not be appropriate material to incorporate in Government guidance. Any proposals to adopt the GDPR into Australian law should be considered as part of the Privacy Act review. At high level, we suggest identifying and adopting the regulatory outcomes or mechanisms that have been beneficial for protection of privacy, such as the use of equivalence assessments to identify 'white listed' jurisdictions. We caution against applying the GDPR framework as a whole into Australia, as aspects of the GDPR has created friction or barriers for consumers that may not be proportionate to privacy benefits. Some of these issues were identified in the current UK review of the GDPR.[5]

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?

Consistent with the summary, the guidance or support from government will depend on the size of the business and the sector concerned. For example:

- For small businesses, material such as the ACSC Essential Eight may be appropriate as a starting point, but there is scope for enhancements as capability matures.
- Banking and other CI sectors: make use of existing industry and govt forums rather than invent a new communications channel. For example, use the Trusted Information Sharing Network (TISN) run by Home Affairs.
- For cross border businesses, there may be merit in guidance material that can assist the business to comply with local and offshore or international data regimes.

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? What obligations are you most commonly subjected to from international jurisdictions?

Inconsistencies in overseas approaches is unlikely to prevent an entity from participating in the global market, but can increase cost and complexity, and can hinder the efficiency and effectiveness of local laws.

Some jurisdictions in Asia are more likely to impose prescriptive requirements relating to (for example) risk management. While other jurisdictions do not impose specific regulation but rely on an entity's familiarity with the regulator's expectations. Examples of overseas regulations applicable to Australian banks include:

- Hong Kong
  - HKMA Supervisory Policy Manual TM-G-1 on General Principles for Technology Risk Management
  - HKMA Circular on Enhanced Competency Framework on Cybersecurity (Dec 2016)
  - Hong Kong Monetary Authority Cyber Resilience Assessment Framework
  - HKMA Circular on Cybersecurity Fortification Initiative (May 2016)
  - PCPD Guidance on Data Breach Handling and the Giving of Breach Notifications

[5] See Chapter 1, Data: a new direction - government response to consultation (23 June 2022): https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#ch1

Australian Banking Association

  - HKMA Circular - Implementation of Cyber Resilience Assessment Framework (12 Jun 2018)
- Singapore
  - Cyber Incident Response Guidelines (ABS/GIA/LIA - 22 November 2016)
  - Cybersecurity (Critical Information Infrastructure) Regulations 2018
  - Cybersecurity Act 2018
  - MAS Notice 655 Notice on Cyber Hygiene for banks
  - Technology Risk Management Guidelines
- • USA
  - 9070 - NFA COMPLIANCE RULES 2-9, 2-36 AND 2-49: INFORMATION SYSTEMS SECURITY PROGRAMS
  - Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers.

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

See ABA comments in the summary addressing data localisation.

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?

Legislative/regulatory requirements: Per the summary, within Australia various legislation have established different privacy or information security safeguards. Internationally, we see a lack of alignment between major jurisdictions; alignment between key trading partners and security partners will benefit data security while facilitating cross-border commerce.

Technical standards: There are international technical standards on data security, information security. In many cases, the private sector such as the banking industry have already taken steps to adopt international technical standards for security. Per the summary, legislation should be 'future proofed' to facilitate adoption of updated technical standards, rather than become misaligned or conflict with updated standards.

A practical barrier for Australia is the division of responsibility and resourcing between levels of government: for example, the OAIC is responsible for Comprehensive Credit Reporting and privacy and they do not have the resourcing to proactively assist or ensure compliance of local government. An inter-governmental arrangement similar to the Council of Financial Regulators may be useful.

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?

It's not clear whether there is a single government agency with this responsibility. Refer summary about the need for a holistic data security policy and local government capability uplift.

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?

Australian Banking Association

Consistent with the summary comments about public sector data security, inconsistent practices between levels of government can result in weaknesses and security breaches. These incidents can undermine public confidence in our digital economy and government.

- There may not be a clear reason for differences between data security practices or governing regulatory regimes. This can create arbitrary differences in data security requirements, gaps or grey areas, which can undermine data security objectives and protections for citizens.
- Some differences are complex to explain to customers, so it also hinders individuals and SME customers having a better understanding of what can be done with their data.
- Inconsistent practices across levels of government can reduce the efficiency and effectiveness of data security systems that need to accommodate differing requirements.

9. What 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?

Banks have a robust understanding of their customers' placing trust in banks re: safeguarding their money and increasingly their financial information. Banks also invest significant resources to understanding their regulatory obligations on data security. However, refer ABA opening comments about the risks created by fragmented or inconsistent legislation and regulations.

On a practical level, many large companies – especially those that have had M&A or merger activity – may face cost or other technology challenges to getting a holistic view of customer data.

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

Refer summary comments about a holistic data security policy.

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?

Refer summary comments about data security in the banking sector, and about clarity of expectations about outsourcing.

The UK is considering legislative reform to manage potential systemic risks stemming from 'critical third parties' or concentration in the simultaneous provision of material services to multiple firms. The proposed reforms would give regulators specific powers to directly oversee services that critical third parties provide to firms including the power to request information directly from critical third parties on the resilience of their material services to firms, and have a last resort power to prohibit a critical third party from providing future services, or continuing to provide services to firms.[6]

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).

A tiered approach that is risk-based would be appropriate. Data held by a small company is still subject to a very high risk from a potential compromise, this should be a determining factor, not just the size of a business.

[6] See: https://www.gov.uk/government/publications/critical-third-parties-to-the-finance-sector-policy-statement/critical-third-parties-to-the-finance-sector-policy-statement

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

Consistent with the summary, the answer to this question will depend on the approach that Government takes to implementing an enhanced data security regime, including whether new requirements are reconciled and aligned with other existing laws and regulations, and whether legislation is prescriptive and risks misalignment with best-practice technical standards over time.

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?

Refer:

- ABA response to consultation on Cyber Security Regulation and Incentives.[7]
- The Australian Cyber Security Centre's Small Business Cybersecurity Guide.[8]
- The success of financial literacy initiatives such as ASIC's MoneySmart website, which can provide learnings for cybersecurity uplift.[9]

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 accountability: refer summary comments about public sector data security and local government capability uplift.

Industry accountability: also refer summary comments about a holistic data security policy which is implemented in a way that is aligned with existing legislation and regulations.

[7] Available at: https://www.ausbanking.org.au/wp-content/uploads/2021/08/20210827-ABA-submission-Cyber-security-regulations-and-incentives.pdf
[8] Available at: https://www.cyber.gov.au/acsc/small-and-medium-businesses/acsc-small-business-guide
[9] See: https://moneysmart.gov.au/