24 June 2022

By Upload.

Dear Sir/Madam

Re: National Data Security Action Plan

AFMA welcomes the opportunity to provide comment on the National Data Security Action Plan.

Getting the settings right for the required uplift in national data security is important for the success of the project and we commend the Government on issuing a discussion paper for this purpose.

The finance sector is one of the most advanced in terms of both security requirements and achievement nationally. Our experience so far has highlighted the need for a truly coordinated national approach. Currently each regulator is motivated and empowered to create bespoke regulatory requirements and varied enforcement approaches. This has led to an inefficient overlapping and inconsistent set of requirements, none of which is aligned to the best international standards, and which are likely, given refresh cycle times, to fall behind best practice.

We also urge the Government to make data security a cooperative affair that avoids a punitive approach. An alignment of business and government working together will be far more likely to achieve the information exchange required to lift data security practices. A punitive approach will move firms to a more defensive posture and will leave clarity around requirements to the courts who are not well placed to provide it in a technically complete and timely manner.

We would be pleased to assist with further information as the project progresses.

Yours sincerely

Senior Director of Policy

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7907 Email: secretariat@afma.com.au Web: www.afma.com.au

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

AFMA makes no response.

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)?

We support the view that revisions to the current framework should be done in a way that is better aligned with standard practices elsewhere, where those practices have proved to work well and are compatible with Australian values and policies. This includes the approaches in the GDPR.

However, we caution against the wholesale importation of GDPR. The GDPR, notably its enforcement penalties are widely regarded as excessively punitive. Australia should avoid the excessive costs of the GDPR regulations.

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?

AFMA's issue in this is area is a multiplicity of overlapping inconsistent Government requirements as per our answer to question 4.

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?

AFMA supports the graded use of a single internationally consistent standard for regulatory purposes.

Currently different regulators including APRA, ASIC, and ACCC apply a mix of bespoke data security requirements, often to the same departments of the same firms. This is inefficient and reduces consistency in data security.

Where these regulatory requirements are drafted by the regulator they do not benefit from the continual updates and international participation which are involved in a more international standard.

Firms should be able to meet their obligations through the application of international standards and not be required to map these back to a particular regulator's bespoke framework.

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

AFMA supports Australia taking a risk-based approach to data security requirements.

AFMA understands, as the paper notes, that it may not be appropriate for national security reasons to allow some data to be stored in some overseas jurisdictions. However, this should not mean that the default is to require data localisation.

Allowing data to be managed internationally can assist ensuring Australia remains connected with global markets and businesses. Data localisation requirements, if they become generally popular, could be a significant barrier to international trade and finance. Australia should set a good example of prudent usage of data localisation with a view to preserving international data flows.

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?

We see significant potential to standardise across major jurisdictions to comprehensive standards.

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?

AFMA makes no response.

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?

Inconsistency leads directly to unnecessary costs that do nothing to assist with security. For example, where different regulators have different rules and requirements firms must map their practices to these multiple different rules when the substantive elements are actually the same and could be mapped to an international standard.

Where some regulators require lower security practices for the same data, for example in CDR which covers bank data when handled by non-bank firms, this can risk unnecessary loss of confidence in the more secure firms.

Where some regulators use litigation to explicate their requirements this leads to long delays before expectations are known and a lack of clarity in areas not considered by the particular cases.

Where regulators use non-specific general legislative requirements to litigate and as their basis for enforcement this creates a lack of certainty around requirements. This lack of certainty creates additional costs and risks and risks damage to the business environment.

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?

N/A.

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

The Australian Government could support a national data security standard that references international standards. Scaled application of this single standard proportional to the risk profile should be the single regulatory requirement reference point for information security.

AFMA views it as important that the Government, its agencies and regulators adopt an accommodative stance in relation to data security. Firms are inherently motivated to ensure security is up to standard, supporting firms to achieve this outcome is more likely to be timely and successful than a more adversarial approach that could limit communications and cooperation.

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?

Firms are aware of the need to manage supply chain risks. Where these supply chain firms are not directly regulated by a regulator more work on a viable structure is required as it may be beyond contractual powers for regulated firms to pass regulator expectations through in all circumstances.

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 risk-based approach can take into account factors including company size. Size in itself is insufficient to determine risk, as a small firm might be handling sensitive data.

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

Financial services firms are already implementing some of the most advanced data security regimes nationally.

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?

A single national standard that references international standards such as NIST can leverage international best practice and bring consistency to the current duplicative approach to regulating information security.

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?

AFMA does not support a move to a more punitive approach in the event of data breaches as we believe it would be counterproductive.

Such a shift may risk incentivising a focus on legal defensibility rather than information security itself. Firms are motivated to avoid data breaches, and in some cases, particularly with state sponsored actors, they may not be avoidable.

Improving public trust will occur if the Government works with industry to support improved practices to a common standard and moves away from duplication of regulatory requirements.