24 June 2022

COMMUNICATIONS ALLIANCE LTD
www.commsalliance.com.au

via email to: datasecurityandstrategy@homeaffairs.gov.au

Dear Sir or Madam,

RE: National Data Security Action Plan Discussion Paper

Thank you for the opportunity to provide feedback in response to the Department of Home Affairs (Department) National Data Security Action Plan (NDSAP) Discussion Paper.

Our members believe that data security is of critical importance to their organisations, the economy and to Australian society as a whole.

In the following, we offer some high-level observations in relation to the Discussion Paper and the topic more generally:

1. The Discussion Paper, appropriately, places the NDSAP within the context of, and as being partly contingent on, other national frameworks which themselves are still in flux or subject to reform processes, such as the *Privacy Act 1988*, the Critical Infrastructure Reforms (largely under the *Security of Critical Infrastructure Act 2018*), and the Consumer Data Right. In our view, it is important to give these processes sufficient time to be finalised and time to settle down, prior to embarking on further substantial projects in adjacent and overlapping areas.

   Generally, we welcome any opportunity for harmonisation of approaches and streamlining of Government initiatives. Given the current processes already on foot and the complex definitional delineation (also refer to our comments further below), we are unsure whether the NSDAP currently meets the threshold for immediate further progression.

2. We support the effort to help promote data security awareness and/or resources amongst all organisations, particularly small and medium sized businesses that may not have the capacity to devote resources to data security. We note that a better general understanding of data risk and governance might, in many organisations, initially yield greater returns in terms of managing risks associated with data. In order to be able to adequately address data security, organisations must have an understanding of data governance, i.e., the architecture, compliance requirements, processes, technologies and of data management techniques that surround the data; before they can apply detailed data security technologies and policies.

3. In principle, we advocate for a free flow of information across geographic borders to allow organisations' maximum participation in the global economy. We are pleased that the Australian Government recognises that digital trade is a key driver of

economic growth and has identified data localisation requirements and data flow restrictions as potential risks to digital trade[1].

4. In contrast, data localisation requirements complicate or impede operations and increase the cost of doing business for organisations that operate across regulatory jurisdictions. The OECD guidelines, which focus on economic benefits derived from a data protection framework, support the free movement of personal data. The OECD argues that restrictive data localisation requirements affect firms' ability to adopt the most efficient technologies, influence investment and employment decisions, increase the cost of innovation and lead to missed business opportunities. Arguably, similar points can be made for other types of data.

   Security, privacy, economic considerations and data efficiency (e.g., latency, proximity to other datasets, etc.) can be optimised when cloud-based services are free to leverage distributed network infrastructure without geographic restrictions. The physical location of data does not, in itself, make those data secure. Rather, what matters more are technological controls to establish and maintain data security and privacy, along with policies that ensure best practices are adopted.

   We recognise some geographic regions are susceptible to sovereign risk, and considering this, we recommend Government issue guidance – potentially with a view to trusted partnerships and alignment between like-minded nations with similar legislative frameworks – rather than rigid restrictions or regulation, to enable Australian entities (including Government, businesses and consumers) to effectively manage their data security risk.

   Data localisation requirements can also make data more susceptible to attack. Requiring data to be stored or processed in one location can make it an attractive target for bad actors (i.e., a larger 'prize' if the attack is successful) and hence, more likely to attract cyber-attacks.

   The global internet infrastructure is comprised of tens of thousands of independent networks that store and carry data across national borders, without knowing its content. Data localisation requirements may, directly or indirectly, impact the flow of data; affecting the internet's resilience, performance, efficiency and global interoperability.

   In addition, environmental efficiency (cooling is a significant cost factor in the operation of data centres, for example), human geography and financial considerations (cost efficient space, power and communications connectivity locations) also play a role in data localisation considerations.

   Consequently, we believe that in developing a data security strategy, the Department ought to focus on providing guidance on technical controls to uplift the security of data, rather than imposing data localisation policies which may have significant negative impacts on the adoption of technology in the Australian economy.

5. Our industry supports efforts to further foster greater digital regulatory alignment and certainty through digital trade rules in bilateral agreements such as the Australia-

[1] Refer to p. 86, Department of Foreign affairs and Trade, *Australia's International Cyber and Critical Tech Engagement Strategy*: "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." (as accessed at https://www.internationalcybertech.gov.au/sites/default/files/2021-04/21045%20DFAT%20Cyber%20Affairs%20Strategy%20Internals_Acc_update_1_0.pdf, June 2022)

Singapore Digital Economy Agreement, and via Australia's role as a co-convenor of the digital trade negotiations at the World Trade Organisation.

Alignment with international standards helps ensure that best practices are utilised (also refer to our point 3 above on trusted partnerships), promotes interoperability, and avoids introducing unnecessary and burdensome complexity. Wherever possible, any frameworks attached to a future data security strategy should be aligned to international standards and best practices.

6. Importantly, we strongly advocate for the voluntary application of a principles-based approach of any future national data security framework, should one indeed be deemed necessary. This type of approach has built-in flexibility that will allow organisations to meet extremely diverse and rapidly evolving data security needs. As data technology shifts over time, a top-down prescriptive regulatory regime will become quickly outdated, potentially leading to an overall decrease in data security as a result.

7. The Discussion Paper notes a principles-based framework built on three pillars (accountability, security and control). It is unclear whether this framework was established through reference to existing standards or frameworks, such as NIST and ISO27001, or whether these are new concepts introduced by the Department for the purpose of discussion in the context of the NDSAP (or otherwise).

   We are raising this question as, in our experience, these terms are often not used uniformly across Government (and potentially also industry), and it would be beneficial if a common data security terminology was utilised across the whole of Government.

8. In a similar vein, we note that "inconsistent definitions [and] misused terms"[2] are being highlighted as a concern in the Discussion Paper. However, unfortunately, we are unsure if the Discussion Paper itself (in the section *Building a common understanding*) sets a clear baseline of what is intended by data and data security in this Action Plan.

   'Data' is, roughly speaking, described as 'information in any form', yet 'data security' is specifically restricted to protecting information on 'digital systems and networks'. What is 'digital information' and 'information in any form' is quickly becoming one and the same thing (i.e., almost all data is available or potentially available digitally) but it is worth addressing this apparent inconsistency (or if this is not an inconsistency, to elaborate as to why this is so).

   Moreover, the term 'data security' is often used in industry interchangeably with the term 'information security', and from most definitions of information security, it would appear that this is what the Discussion Paper is referring to when it uses the term 'data security'. However, the Discussion Paper does not expressly note this and, if our assumption is correct, it may be worth clarifying this equivalence.

   It may also be beneficial to spell out the description 'data security as distinct from 'cyber security'. As previously noted, references to common definitions (as found in common standards such as ISO 27001) ought to be used wherever possible. Whenever deviations from such common definitions are being sought, those ought to be

   - clearly articulated, and
   - used in a whole-of-Government approach.

[2] p. 18, *Department of Home Affairs, National Security Data Action Plan*, Discussion paper – a call for views, May 2022

9. Whilst the Discussion Paper offers a stocktake of federal regulations associated with data stewardship, we would encourage the Department to also include considerations as to how state legislative frameworks and industry-specific standards interact with federal regulatory activities.
10. It is also not entirely clear which entities the Department would consider regulated under a NDSAP; if there are indeed any regulated entities at all, and which entities would remain unregulated, and what the criteria for classification would be. Further clarification would be welcome.
11. We would also like to take the opportunity to stimulate discussion in relation to the operationalisation of reporting requirements: having one point for reporting for incidents (rather than the current arrangement of bespoke data security reporting obligations for different matters, industry sectors and/or state/federal jurisdictions) could help reduce the cost of doing business. For example, it could be conceivable to have a single reporting 'portal' for breaches of the Privacy Act, cyber incident reporting, ransomware reporting, etc.

We look forward to continuing our engagement with the Department of Home Affairs and other relevant stakeholders on data security and related matters.

Please contact Christiane Gillespie-Jones (c.gillespiejones@commsalliance.com.au) or myself if you have any question or would like to discuss.

Yours sincerely,

John Stanton
Chief Executive Officer