1 July 2022

Department of Home Affairs
Commonwealth of Australia

(Submission lodged via DHA website)

Dear Madam/Sir,

RE: National Data Security Action Plan

Amazon Web Services (AWS) is pleased to provide comments to the Department of Home Affairs (the Department) on the *National Data Security Action Plan* (the Action Plan).

AWS understands the incredible opportunities presented by data. Every day, millions of customers – including the fastest-growing startups, research institutions, health services, large enterprises, and leading government agencies – safely use AWS to maximise the potential of data and the digital economy. We provide a powerful suite of services, from infrastructure technologies like compute, storage, and databases, to emerging technologies, such as machine learning and artificial intelligence, data lakes and analytics.

AWs is deeply supportive of the Action Plan's key focus of lifting the base for data security as we recognise the power of data, and know the importance of keeping data secure. Security will always be our number one priority. AWS customers trust us to handle their data securely, and we honour our commitment to build and operate infrastructure that satisfies the requirements of all organisations. We ensure that our customer's data is secure by (a) ensuring that our end-to-end supply chain is resilient and secure, from the networking layer, to physical data centre environments, hardware and equipment and the software supply chain, and (b) by ensuring that customers have appropriate controls to validate that no data exfiltration has occurred.

However, we would like to make several recommendations, based on our discussions and experience with governments globally, particularly where it relates to implementing and applying security and privacy frameworks and guidelines. Any new policies should be based on evidence; addressing a genuine policy gap; and be consistent with, and complementary to, existing policies.

Key Recommendations:

1/ The Action Plan should explicitly promote risk-based approaches to data governance and data security and avoid a one-size-fits-all approach to describing data security.

The Action Plan takes a broad approach to defining data – including personal information, public sector data, critical sector data, aggregated databases, as well as data of Australian companies. It also addresses the general value of data to the Australian economy and the potential concerns when data is not secure. However, the Action Plan fails to recognise that not all data requires the same level of protection and security. It also confusingly speaks to the need for "consistent frameworks" in a manner that suggests it should be broadly applicable to all data listed above – however, when delving further, the recommendation for consistent frameworks appears to be tied to public sector data.

Consistent with our previous submission on the Attorney-General's Department's *Privacy Act Review – Discussion Paper*, we believe the most successful data governance and security frameworks are those that take a risk-based approach allowing organisations the flexibility to determine the most appropriate measures to manage data security risks. AWS sees an important opportunity for the Australian Government to address a genuine policy gap through a clearly articulated approach to data governance. An important objective of data security laws is to encourage better internal data governance and improve data security hygiene-practices in organisations. Such an approach is also consistent with broader security principles.

Requirements that are over-prescriptive run the risk of actually creating security risks and increasing the cost of security for regulated organisations. Such overly specific requirements apply security obligations that are often designed for high sensitivity data and can often be ineffective, inefficient and even counterproductive to other entities' security outcomes. The inflexibility can cause unwanted outcomes such as unnecessarily limiting business operations, significantly reducing companies' ability to react to new threats and technologies, and forcing security teams to shift resources away from security operations to address reporting and compliance requirements.

A better approach provides organisations with the flexibility to choose an appropriate strategy for securing their data assets within a broad risk management framework based on widely adopted international standards. Such an approach allows customers to make security choices for their data that reflect their individual business models, the sensitivity of their data holdings, and balancing associated costs. Security policies are more effective when they take a risk-based approach that emphasise outcomes instead of rigid controls.

To this end, we recommend that the Action Plan more explicitly describes the need for organisations, as a first step to ensuring data security, to catalog the types of data they collect and the databases that they are collating. Organisations should then assess the appropriate levels of security against the risk profile of each set of data and databases. AWS has published Whitepapers[1] explaining how Data Classification is a foundational step towards secure cloud adoption – however, this can also be more generally applied to many other data processing activities.

Additionally, we recommend that the Action Plan more clearly link specific recommendations to specific use-cases of data. For example, if a specific recommendation is most applicable for Public Sector data sets (e.g. population statistics), then these recommendations should be more directly and clearly linked to that scenario, rather than provided generally. This approach ensures that laws and regulation not only remain relevant to the dynamic and complex digital landscape, but also helps to avoid the unintended consequences of outdated laws and regulations.

2/ The Action Plan should avoid conflating securing data against foreign threat actors with the location of data.

Overall, the Action Plan takes a fairly nuanced view of the need for facilitating cross-border data flows, while recognising the need for data in some situations to be kept within the country. However, the Action Plan mistakenly asserts that keeping data on-shore would minimise the risks associated with foreign threat actors or cyberattacks. In reality, the location of data matters more for other reasons (e.g.

[1] https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification-overview.html

operational resiliency and latency), rather than to address data security. Instead of emphasising data localisation as a means for achieving general data security, the threshold for permitted cross-border data flows of high-risk data sets should be linked to a "comparable standard" of data security.

The most appropriate determinant of the security of data is the security controls applied to protect it, not its physical location. Practically, the most important aspect of an effective data security strategy is to ensure that organisations have access to the most state-of-the-art and advanced security technologies. Furthermore, characterisation of concentration risks arising from the "concentration of data centers" (pg. 24 of the Action Plan) are inaccurate as they fail to recognise that security resiliency can be achieved from reliance providers who deliver "resiliency-by-design" in their service offerings.

3/ Consistency should be an important consideration of the Action Plan.

As the Department noted in the discussion paper, the Action Plan will intersect with other reforms and consultations, many of which are in early implementation or formative stages. These include:

- The passage of comprehensive amendments to the *Security of Critical Infrastructure Act 2018*, significantly expanding the scope of industries and entities captured under existing security legislation and introduces civil penalties, offences and infringement notices for non-compliance;
- Conducting a comprehensive review of the *Privacy Act 1988*, intended to modernise and strengthen the Australian privacy regime; and
- The introduction of the Hosting Certification Framework, a landmark policy intended to provide assurance to Government on the secure management of government systems and data.

As AWS has acknowledged previously, these reforms are substantial and meaningful. AWS expects they will have a significant impact on building Australia's data and cybersecurity and boosting confidence in the digital economy, at a time where digitisation is fundamental to Australia's post-pandemic economic recovery. However, these reforms need time to take effect – and impacted entities allowed sufficient time for implementation – before the introduction of any new regulatory instruments or initiatives.

Summary

In general, the government should develop a roadmap for data governance, including broad considerations and guidance for (a) data classification; (b) types of security controls (e.g. IAM, encryption etc.); and (c) organisational controls. Given the constantly changing scale and variety of data held, variety of business models, and constantly evolving technology choices available, it is important that any roadmap is created in conjunction with all impacted parties. This should be developed in a risk-based way to ensure that the most important data is classified appropriately, without over-classifying low-risk data and preventing governments from innovating and using that data to the advantage of constituents.

Principles-based data security should also facilitate the free flow of data by establishing mechanisms for cross-border data transfers, such as requiring that data transferred out of the jurisdiction is protected to a standard comparable to that within the jurisdiction. To be clear, with AWS, customers choose where to store their data. They own and control their data, including where it is stored, how it is stored, and who has access. AWS does not move customer data without their consent, and customers who care about protecting their data can encrypt their data in motion or at rest.

However, it is important to make clear that localisation measures alone do not improve data security outcomes, nor do they consider all aspects of what it means for data to be secure. The resilience of computing services, for example, is an often-overlooked aspect of secure data. Moreover, policies should recognise that data security is not necessarily related to data location but on the controls applied to protect the data. We caution against an overreliance on data localisation measures, as the free movement of data across borders is central to the digital economy and digital innovation.

Government is in a unique position to positively influence the adoption of data security across the digital economy by promoting and supporting effective data governance practices. An important tool of government is conveying complex topics in a language and format readily accessible to non-experts, and we believe the Australian Government can make a substantial impact on data security in Australia through an approach that streamlines, simplifies, and effectively scales existing programs. To that end, we reiterate suggestions from our previous submission on *Strengthening Australia's cyber security regulations and incentives* for:

1. The development of a 'single door' for data security advice and guidance. Although cyber.gov.au is ostensibly intended to be this resource, advice relating to cybersecurity or data security – often conflated – can be found across multiple government departments or agencies. Consistent, clear, and 'plain language' messaging pointing to a single well-structured resource would be hugely beneficial across the Australian economy.

2. A single site would also allow Government to more effectively amplify the existence of ongoing programs and initiatives. Consolidating these resources and communicating the existence of a single source should see an increase in that awareness.

3. We believe that guidance helping SMBs make more informed technology investment decisions that will open them to the advantages of the digital economy, while reducing their cybersecurity risks, would also be a beneficial and welcome resource for these entities.

We look forward to continuing to engage with the Department on this important issue.

Best Regards,

Roger Somerville (somroger@amazon.com)
Head of Public Policy, Australia and New Zealand
Amazon Web Services.