Submission to the
Department of Home Affairs

National Data Security Action Plan – Response to Discussion Paper

Public Version

June 2022

INTRODUCTION

1. Optus welcomes the opportunity to provide a submission on the National Data Security Action Plan (NDSAP).

2. Optus is the owner and operator of significant national communications infrastructure and the supplier of important carriage and content services to a large portion of the Australian community (over 11 million services). We manage a vast amount and range of data on millions of Australians in an already highly regulated sector and we take our responsibilities in handling this data incredibly seriously. This also means we have an intimate understanding of the nuances of the data landscape in the sector and can draw on this experience in providing advice to Government on how to build an effective data security regime.

3. This submission offers some broad observations for consideration. These are summarised below while further detail is provided in the body of the submission.

4. Optus offers three broad observations on how to build an effective data security regime:

   (a) Focus on **harmonising existing mechanisms and regulations** to improve efficiency and enable more effective compliance.

   (b) Use the plan to **improve data literacy and counter misconceptions**.

   (c) Establish **core principles to underpin data regulation** in the future.

5. In addition, this submission provides Optus's response to the specific questions raised in the discussion paper. Further detail is provided below and Optus would welcome the opportunity to discuss these issues further.

6. As a member of the Tech Council of Australia and Communications Alliance, Optus also broadly supports their respective submissions.

SUBMISSION

Harmonise Existing Regulations

7. As the discussion paper notes, even at a federal level there are an array of mechanisms and regulations that govern (or soon will govern) data in some way. Some of these focus on a specific aspect of data such as cyber threats to critical infrastructure. Others have much broader application such as the ongoing reforms to the Privacy Act or the Consumer Data Right. Many of these create duplicative or even conflicting obligations for industry. For example, the Privacy Act reforms seek to further restrict access to personal information while the Consumer Data Right is premised upon greater access. While Optus appreciates the importance of effectively regulating data security and the handling of personal information, it is harder to effectively achieve this with the proliferation of duplicative regulations that are not always fit-for-purpose.

8. Optus therefore recommends that the National Data Security Action Plan ('the Action Plan') be used as a mechanism to harmonise these existing and forthcoming regulations. Mapping the various objectives and mechanisms that these regulations either have or will introduce would help clarify areas of overlap and conflict. This in turn would provide a sound evidence base to inform appropriate reforms that would improve outcomes for government, industry and consumers. More detail on some of the specific issues in the telecommunications sector is provided in response to question six.

Improve Data Literacy

9. Another issue that the discussion paper identifies is the varying levels of data literacy across government, industry and the broader community. Optus agrees that there are challenges that arise from this, both in terms of industry/consumer shortcomings (e.g. failure to follow core cyber security practices) as well as impractical policy outcomes (e.g. moves towards data onshoring).

10. On the former, most cyber breaches can be attributed to a failure to follow the 'Essential Eight'[1] actions as set out by the Australian Cyber Security Centre (ACSC). Continuing to educate and assisting businesses and other entities to implement the Essential Eight and other basic cyber security practices will therefore have a clear benefit for data security. Likewise, it will be beneficial for government to improve its data literacy in some instances and in turn produce better policy outcomes.

11. In recent years, for instance, there has been an increased focus from Government on the idea of 'data onshoring': moving sensitive data from overseas data facilities to Australian facilities. While Optus appreciates concerns about the risk of hostile foreign entities having access to sensitive data, it is important to note that the location of a data facility does not always correlate to the risk of a hostile entity accessing that data[2]. What is most important is the actual physical and technical security that exists at the particular data centre. It is also important in many cases to have redundancies to ensure ongoing access to business critical data, including for essential services such as telecommunications. This sometimes includes having offshore back-up servers.

12. Optus therefore recommends that a key focus of the Action Plan be coordinating an uplift in the outreach and education efforts of the Commonwealth. This could include developing useful policy toolkits in partnership with relevant industry bodies.

Establish Core Principles to Govern Future Regulation

13. As outlined earlier, one of the shared policy challenges in the data landscape is the proliferation of overlapping and sometimes conflicting regulations. To complement the recommendation around harmonising and reconciling this duplication and conflict, Optus recommends that the Action Plan be used to develop core principles that would guide any potential future regulation.

14. While Optus does not see a need for further regulation in the immediate future, we see a clear benefit in setting out principles to guide long-term regulatory design. Ideally this would be achieved through a co-design process with industry, experts and the public. Having well-designed, broadly agreed-upon principles would help reduce the potential for future regulation to be duplicative and/or contradictory, the benefit of which would be a reduced compliance burden for government and industry and a clear, transparent regulatory regime that would inspire confidence in consumers.

[1] Evidence given at the 16 March 2022 PJCIS public hearing on the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* by Abigail Bradshaw, Head of the ACSC.

[2] While there are cases where this is a clear risk in some offshore jurisdictions due to expansive legislative powers and intrusive Government actions, this is more of an exception.

Responses to Questions

Q1: What do you consider are some of the international barriers to data security uplift?

15. Optus sees two key international barriers when it comes to data security uplift:

    (a) A reliance on device manufacturers that are based in overseas jurisdictions;

    (b) The lack of a coordinated international framework for responding to and prosecuting ransomware attackers.

16. A particular challenge in the telecommunications sector is that mobile device manufacturers and software developers are almost entirely based outside Australia (exclusively so in the case of device manufacturers). Often these companies incorporate mechanisms in their hardware and software that manage customer data flows. In many instances there are no 'opt out' mechanisms for the customer to choose and little that can be done to mitigate this as the companies operate outside Australia's jurisdiction.

17. Similarly, the biggest current threat to data security is from ransomware but many of the most threatening ransomware actors operate from foreign jurisdictions. While Optus appreciates the significant legal and technical challenges in responding to this challenge, it is nevertheless a key concern that has a direct impact on data security.

Q2: How can the Australian Government guidance best align with international data protection and security frameworks?

18. Optus cautions against adopting/aligning with international frameworks before identifying and understanding the issues that are trying to be addressed locally. While there is likely to be some benefit to adopting or aligning with major international standards such as the EU's General Data Protection Regime (GDPR), Optus strongly recommends that the first step in policy development be to understand and articulate the problem. Only where this process identifies a clear risk or loss from a lack of alignment should it be pursued.

19. One illustration of this arose in the ongoing review of the Privacy Act. Optus's submission noted that there are issues with importing concepts from the GDPR such as 'controller' or 'processor' in relation to personal information and who is accountable for its management within an organisation. These concepts are quite broad and do not reflect the operational realities of how personal information is managed in a modern telecommunications company (and likely many other industries).

20. For example, personal information can be handled by a range of different individuals for different reasons and with differing levels of responsibility. Frontline sales staff, for instance, will have access to personal information as a necessary part of providing products and services to customers and will have commensurate obligations to protect this information. These staff will not, however, have responsibility for the technical security of the systems on which the data is stored. At the same time, the IT staff responsible for this technical security will not have access to the personal information on the system. Thus, responsibility for different aspects of protecting personal information is shared across different teams and no single individual or work unit can be reasonably designated as having control over the full breadth of personal information protection.

21. Another example is the data breach notice requirements under GDPR, which are quite prescriptive in terms of the thresholds and timelines for notification. While Optus strongly supports the need to have a robust data breach notification regime, our view is that this is already being achieved through the Mandatory Data Breach Notification regime under the Privacy Act. There is therefore no need to duplicate these requirements at this time, especially given the review of the Privacy Act that is under way.

Q3: What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be best delivered to you?

22. As noted earlier in our submission, Optus's view is that one of the most useful things that can be done is to harmonise and reconcile the existing and forthcoming array of data security regulations. This would in turn make it easier for Government to articulate clear guidance and provide more effective support to business.

23. In addition, Optus would caution against any proposal to implement a data classification regime for industry based on the current Government classification system in the Protective Security Policy Framework (PSPF). While this classification system makes sense for government data, its underlying motivation is protection of the national interest. While many businesses, including Optus, play a role in supporting the national interest, our underlying motivation is commercial and we do not hold the vast and sensitive array of information held by government (e.g. from intelligence agencies). Mature businesses such as Optus already have their own information classification systems in place based on their particular interests and commercial arrangements. We therefore recommend against any imposition of a data security classification regime.

Q4: How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions?

24. Optus suggests that Australia adopt a consistent set of principles, policies and standards aligned to industry norms for improving 'trust' required for data sharing. A standard protocol for defining requests and establishing data governance would improve the confidence and efficiency associated with data sharing projects by creating a safe environment for sharing data. This in turn would improve productivity and generate better outcomes for consumers.

Q5: Does Australia need an explicit approach to data localisation?

25. Optus cautions against the assumption that data stored locally is inherently more secure than data stored offshore. The most important elements of data security are the physical and technical security features that protect a data facility. While there are some jurisdictions where domestic laws and state actions create heightened risks, these are an exception and, precisely because of this threat, are unlikely to be relevant as little or no sensitive data is stored there.

26. Instead, Government should adopt a risk-based approach that considers the particular circumstances of a data storage location and weighs them against the cost of transferring the data to a domestic facility. Optus notes, for example, that the ongoing transfer of Australian Government data out of the Global Switch Ultimo (GSU) facility will have taken over a decade to complete at a cost in the hundreds of millions over the life of the project. Furthermore, this project only involves transferring data from one domestic location to another. Were the Government to adopt a localisation policy that required transferring data from an international to a domestic location, the cost in both time and money would far exceed that of the GSU project.

Q6: How can data security policy be better harmonised across all jurisdictions?

27. As outlined earlier, there are a number of existing or forthcoming regulations that create overlapping and/or conflicting obligations in relation to data security. Identifying and reconciling these overlaps and conflicts would be a valuable outcome of the Action Plan.

28. A key example of this in the telecommunications sector is the contradictory purposes and obligations of the review of the Privacy Act on one hand and the Consumer Data Right on the other. The review of the Privacy Act is seeking to significantly strengthen the obligations that holders of personal information have to secure and manage that

information. In contrast, the Consumer Data Right is seeking to expand access to personal information and reduce the barriers to third parties accessing that information. On top of this, hundreds of critical infrastructure providers are being subjected to enhanced cyber security obligations under the reforms to the Security of Critical Infrastructure Act while telecommunications companies in particular are also preparing for major reforms to electronic surveillance powers.

29. Many of these regimes seek to impose their own bespoke obligations on the relevant entities which leads to a complex compliance burden. Optus in particular is subject to all of these regimes (as well as many others) so regulatory consistency is especially important not just for Optus but for Government too: clearer and simpler obligations will produce improved compliance and mutually beneficial outcomes.

Q7: Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened?

30. Nil response.

Q8: What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of government?

31. Two of the key challenges arising from inconsistent data security practices are the impediment it can create to sharing data and the increased cost of developing effective safeguards due to regulatory inefficiency.

32. Inconsistent data security practices can hinder or even prevent the sharing of data between entities. In such a technologically-driven age, data-sharing is crucial to productivity, product development and customer experience, among other things. This is not confined to the private sector either. Government is increasingly drawing on data for a range of services such as digital licences, natural disaster preparedness and e-health initiatives. Consistency is therefore crucial to optimising the sharing of data to enable these and many more services for all Australians.

Q9: 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?

33. Optus has been subject to rigorous data security and privacy regulations for over 30 years. This includes specific privacy and data security obligations under the Telecommunications Act as well as the broader rules applicable to all entities under the Privacy Act. Moreover, Optus has partnered with Government to achieve a range of important national security outcomes over this time, including providing satellite communications for the Australian Defence Force and working with law enforcement and intelligence agencies to provide crucial information for their investigations and operations. Optus is well aware of the value of the data it processes and stores and the importance of the data security obligations to which we are subject.

Q10: How can the Australian Government further support your business to understand the value of data and uplift your data security posture?

34. As outlined above, Optus has a very mature understanding of the value of our data and a sophisticated data security posture developed over several decades.

Q11: Does your business appropriately consider data security risks in their supply chains?

35. Yes, data security is critical to our business and, to the extent possible in complex modern supply chains, Optus carefully considers data security risks in supply chains. Optus also reports on some elements of these risks as a result of its obligations under the Telecommunications Sector Security Reforms, which require us to notify the Government of any material change in our network security architecture.

Q12: 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?

36. Optus notes that, especially with the growth of the tech industry in Australia, even organisations with smaller number of employees can be responsible for managing or handling critical and sensitive data sets. The main intent of any data sharing regulation is to foster a culture of good governance to improve confidence and trust among parties. Therefore, any proposed legislations should be applicable to the entire sector as this would not then hinder the growth and competitiveness of the sector. Optus recommends that a principle-based approach is adopted for data security.

Q13: Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

37. In our experience, Optus notes two broad challenges that could limit the effective implementation of a data security regime: impractical obligations and 'static' legislation (i.e. laws that do not evolve with changing circumstances).

38. On the former, there are a range of impractical obligations that have been imposed in other regulations that should serve as lessons to inform any data security regime. Often, these are based on a lack of technical understanding around how an industry or company operates. This underscores the importance of rigorous consultation and co-design processes.

39. Under the review of the Privacy Act, for example, a range of obligations are proposed, including the ability for customers to have a right to object to the collection of location data. However, given how deeply embedded the use of location data is in the operation of a network, activating this right would have the effect of preventing Optus from providing any telecommunications service to that customer. An effective consultation and co-design process is therefore crucial in order for policy-makers to understand the practical implications of any obligations they might seek to impose.

40. Legislation that fails to keep up with modern developments or lacks flexibility to respond to changing environments is another key challenge that should inform policy development for data security. Optus notes, for example, that the Government recently undertook a wide-ranging and costly review of the legal arrangements for and powers of the Australian Intelligence Community (known as the Richardson Review). While this review has produced a range of good outcomes and generated a much-needed reform process, it also exemplifies the extra time and cost that is required when legislation is not regularly reviewed and updated. Any data security regime that arises from the Action Plan should incorporate regular review mechanisms that allow for more regular reforms. This will ensure that the regime keeps pace with future developments and remains fit for purpose.

Q14: Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practices?

41. Nil response.

Q15: 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?

42. Optus notes that a regime already exists for mandatory data breach notifications under the Privacy Act, which is currently undergoing a review.Optus recommends no additional obligations be considered at this stage.

CONCLUSION

Optus has a longstanding record of and commitment to working with Government in support of national security outcomes and we take our obligations in this regard seriously. Optus welcomes the opportunity to contribute to the National Data Security Action Plan and we reiterate our three key recommendations for how the plan can contribute to improved policy outcomes for government, industry and the public:

1. Focus on **harmonising existing mechanisms and regulations** to improve efficiency and enable more effective compliance.
2. Use the plan to **improve data literacy** and **counter misconceptions**.
3. Establish **core principles to underpin data regulation** in the future.

Optus thanks the department for the opportunity to provide a submission and would welcome the chance to discuss these issues and our proposed recommendations in further detail.

[END OF SUBMISSION]