Australian Network

1. **Are these the correct factors to taken into account and to guide the legislative development?**

One of the main reasons commonly given for not sharing data is the “Risk of misuse”. Weighing up the pros and cons for sharing data, the missed opportunity costs should be considered. The potential for advancements, new insights and potential benefits cannot be overlooked. To weigh up the pros and cons we need to consider who benefits and who is at risk by carefully assessing the data concerned. One must also not overlook the need to take the audience on a journey, of not only why the data should be released, but also the benefits in releasing the data. Quite often, fear of misuse stems from a lack of clarity, rather than an actual risk of malpractice.

2. **What else should the Government take into consideration when designing the legislation?**

Irrespective of the funding scenario of the creating entity, the ability for non-government entities to produce data that includes information about citizens should be a deciding factor in legislation design. There are many data sets that fall into this category. It would be good if the legislation included an advisory segment that proposes all entities, including non-government entities should follow the same framework to establish best-practice process. This would stand for Multi-national entities as much as for small start-ups. All entities and operators in the data space should adhere to the same framework.

3. **Should the scope be broader or narrower?**

The scope should be broader to encompass all government funded entities and processes.

In case of fully, or close to fully funded by government entities, the entity should be forced to use the same legislation and framework. All entities and structures should be included from a research perspective.

In case of partial funding or project based funding, the entities should be persuaded or incentivised for using the same data sharing framework. A common framework will ensure transparency and a common method of measurement.

4. **Are there entities that should be included or excluded from scope? How would this be justified?**

As per the previous response, the inclusion should be for all partially or fully funded entities. They should adhere to the same regulation and framework, thus establishing a transparent and fair system. Where data has been paid for by the tax payer, as much as possible, it should be used to benefit the people. Whether the data has been created by a tax payer funded entity, or a Government agency makes no difference.

5. Should any specific categories of data be specifically out of scope? How should this be justified?

No single category of data should be excluded. Irrespective of who is creating or compiling the data set, all data may have a beneficial use-case. Once again weighing up the benefits versus risks will see opportunity costs for data usage determining access, even to sensitive data. It is important to remember that whilst the use-case for the data may not be instantly obvious, new innovations and innovators are entering the marketplace on a daily basis. This framework should govern both the current and future treatment of data.

6. Should exemptions, for example for national security and law enforcement, occur at the organisation level or for specific data categories?

The danger in maintaining two different frameworks is the confusion that can arise and thus paralysis under the fear of breaching privacy and standards. Whilst exemptions could be made in certain national security and law enforcement scenarios, these need to be adequately labelled and clearly defined. To extend on that theory, if desensitised data within these scenarios can be utilised for the common good, it should be released as a complete dataset as soon as possible. Strict timeframes for confidentiality should be attached to the affected datasets to ensure that they are released as soon as possible. The longer the timeframe, the less sensitive data seems to be, whilst still having historical or research interest. No single entity or department should be handed a blanket exemption, as not every dataset may contain sensitive or security afflicted information.

7. Are there instances where existing secrecy provisions should prevail?

Existing secrecy provisions should prevail, but not for an open-ended period of time. A review of secrecy provisions should occur on at regular intervals and obsolete and non-effective measures should be replaced with current processes and provisions.

8. Do you agree with the stated purposes or sharing data?

Yes, we agree that data should be used to benefit the greater good. This includes all factions of research, government and industry, they all benefit from service delivery of the policy. The inclusion of machine learning and artificial intelligence to gain insights from data should be considered. Increased data sharing will continue to ignite the research sector by allowing for increased primary and secondary insights and the overall innovation of products, solutions and technology.

9. **Are there any gaps in the purpose test that would limit the benefits of public sector data use and reuse?**

In the fields of innovation, data usage and sharing for clear and direct public benefit is suitable. In the fields of research, this excludes the ability to protracted of long-term studies, which are common. The proposed research and discovery limitations are too stringent. If the greater good measure can be applied, research and discovery should be permitted over an extended period. This would also apply to private or public organisations undertaking extended research and discovery.

10. **What further details could be included in the purpose test?**

As stated above.

11. **Should data be used for other purposes? If so, what are those purposes?**

As long as the end use has the greater good in consideration, all uses for data should be included in the framework. The benefit of using the data must be at the forefront, irrespective of the entity or the end use-case.

12. **Should there be scope to share data for broader, system-wide purposes**?

The concept of data-sharing amongst both government entities and agencies and between civic organisations is well documented and advanced in a number of international jurisdictions. As with all data sharing, the benefits must outweigh the actual, rather than perceived risks. Regulation should be created to allow this sharing if it does not already exist. As with all breaches of compliance, if entities are found to mis-use or breach the framework, it is important for the penalty to deter future incidents. This should apply irrespective of the entity being a government organisation, government funded, or a private entity. It is important to remember that any data can be mis-used, it is not the data itself that is responsible and locking away the data may lead to missed opportunities and missed insights that will lead to national development and growth.

13. **Should the purpose test allow the sharing of data to administer or enforce compliance requirements?**

The framework should have one set of rules for accreditation and penalties for mis-use. If an entity is found to have mis-used the data, they should risk losing their accreditations. There needs to be one central entity responsible for the accreditation process and it needed to be achievable in a timely fashion for a low-cost basis. This will ensure that barriers to entry do not form due to economics.

14. **Is the Five-Star framework the appropriate mechanism to ensure data is safeguarded?**

Yes it is an appropriate mechanism to safeguard data. Getting the last star right ‘appropriate use’ will require a good set-up process with representation of a multitude of entity demographics. This can not be government, nor research alone. Ensuring the purpose star is of value will make or break the proposed policy. International standards such as ISO27001 may simplify the verification process and other international standards will ensure a comprehensive environment for adoption and certification.

15. **Are there additional safeguards that should be applied?**

Giving consideration to advancements in international standards, such as ISO’s may expand safeguards for adoption.

16. **Are there any instances when the Five-Safes could not be applied?**

It is possible that not all datasets can be equated to the star rating. Consideration should be given to when this scenario occurs. Is the data set any less valuable? Does the data set still have a common good potential?

17. **Is the Five-Safes appropriate when data is shared and used for the specific purposes in the purpose test above?**

Yes.

18. **How should the responsibility for managing risks be shared in the framework?**

Whilst managing the risks of data shared should be the responsibility of all entities involved, definition needs to be given to whom is responsible at what part in the sharing cycle. Consumers should make sure that they apply strict controls and maintain rigour where required when accessing sensitive data sets for the life of the data usage. Not only shall the data creator take action to protect the data whilst in their possession, they should ensure the process of transmission, systems and technologies and also the labelling of the data sets be of the highest level. During the life-cycle of the data, when the purpose of the data changes, the consumer should request a change of data custodian detailing the proposed change of use. The custodians must ensure all measurements of compliance are tested and adhered to at all times, but especially with each transfer of data and request to access the data. In addition to consumers and custodians, there is a place in the ecosystem for data agents. They could act as safe habour for the data sets and also take care of the actual practice of data sharing. That being said we do not want to overcomplicate the process, nor create a role that could be exploited.

19. **How would you envisage Five-Safes principles be applied over the life-cycle of data to ensure data safeguards are continually met?**

As above.

20. **Under what circumstances should trusted users be able to access sensitive data?**

If the data has been categorised as sensitive and particulars such as identity can be readily accessed, the issue of trust and environment need to be considered. If the user is trusted and the environment can be declared safe, and the process can assure that disclose of identity will not be shared and that the purpose of accessing the data is appropriate with common-good outcome, access should be granted. Tight constraints need to be built into the framework to decide each of the factors for consideration.

21. **Would this arrangement overcome existing barriers to data sharing and release?**

Yes. Currently legal agreements and ethical processes are riddled with concerns over privacy delaying or in some cases acting as a barrier with no one wanting to make a decision.

22. **Would streamlined and template agreements improve the process**?

Yes, standardisation and a common approach would improve the process.

23. **Do you agree that data sharing agreements should be made public by default?**

Yes. Just as all legislation is published in the long-run, the nature of a transparent and accessible framework would require all agreements to be made public by default.

24. **What level of detail should be published?**

A summary of necessary details should suffice. The names of the parties, what is shared, and when.

25. What else should a data sharing agreement contain?

It could be interesting to reference previous agreements which will increase the trust between data custodians and data consumers.

26. What other transparency mechanisms could be mandated?

Publishing agreements in a open access portal, just like the open data portals should suffice.

27. How long should accreditation as an ADA or Trusted user last?

Five years to seven years to keep it in alignment with the majority of commercial agreements.

28. What could the criteria for accreditation be?

The five-safes and International standards such as ISO:27001. Using international standards which will help alleviate overheads and to establish global best-practice.

29. Should there be review rights for accreditation?

Yes. All rights should be accessible. There is a possibility of mistakes occurring due to interpretation and qualification of details.

30. Should fees be payable to become accredited?

Whilst it seems reasonable to request a fee as a function of the effort required to review an entity or individual, we need to ensure that this is capped and is not a barrier to some entities accessing the environment. Safeguards should be put in place so that it does not become a money-making accreditation scheme. Any fee will impact the start-up and innovation community adversely.

31. Is the Australian Government Charging Framework fit for purpose in this context?

It would depend on the stakeholders, and as above, may negatively impact those smaller entities and not-for-profit stakeholders.

32. Are these the right functions for the National Data Commissioner?

Yes, the National Data Commissioner is right for these functions.

33. What review powers should the National Data Commissioner have?

Audits, inquiries and investigation proposed in the document entail the review powers the NDC should have with respect to trusted users, accredited data authorities and data sharing agreements.

34. Should the NDC have the power to conduct an investigation into system-wide issues?

Yes. Costs and timelines should be considered.

35. What other actions could the NDC be able to take?

Nothing comes to mind.

36. Are there other ways community values and expectations can be captured and addressed?

The NDC should publish all data sharing agreements in an open and accessible format.

37. What aspects should be taken into consideration when considering consequences for non-compliance with the DS&R Bill?

Severity of non-compliance, intent and efforts made towards ensuring compliance. If accreditation is under consideration, penalities around removing or impeding this accreditation would need to be standardised based on severity of breach.

38. Should the consequences differ depending on the type of data involved or the type of misuse, e.g. harsher penalties for intentional misuse?

Yes. Intent, repeated violations and the mis-use of sensitive information must be taken into consideration. The consequences need to be based on the infraction and the entity involved.

39. Should penalties be strict liabilities?

A balanced approach should be employed. Strict liabilities in conjunction with an accreditation framework may work.

40. What would be an appropriate penalty for intentional misuse of data?

The first step would be a warning and potential retraction of accreditation of ADA or trusted user.

41. How would responsibility for misuse of data be shared across the data system?

In the same format as the data sharing agreements are shared, any misuse of data should be made public as soon as the misuse can be confirmed and validated. Peer visibility and peer review can be an effective deterent.

42. To what extent should there be a complaints mechanism and how should it work?

There needs to be a clearly defined avenue to channel complaints directly to the NDC. Standard mechanisms, as per other complaints processes can be used. The ability to complain anonymously is important due to the commercial arrangements that may exist with data sharing. A timeframe for investigations and determinations should be included in the framework. Once an outcome has been reached, this should be made accessible.

43. Should a complaints mechanism provide for complaints by the public?

Yes, anyone should be able to make a complaint.