Australian Research Data Commons

Submission: National Data Security Action Plan Discussion Paper 2022

Rosie Hicks, CEO ARDC
24 June 2022

The Australian Research Data Commons (ARDC) thanks the Department of Home Affairs for the opportunity to comment on the National Data Security Action Plan Discussion Paper.[1]

About the ARDC

The ARDC is a transformational initiative that enables Australian research community and industry access to nationally significant, leading edge data intensive eInfrastructure, platforms, skills and collections of high-quality data. The purpose of the ARDC is to provide Australian researchers with competitive advantage through data, providing access to leading edge eResearch collections, tools, infrastructure and services. Its mission is to accelerate research and innovation by driving excellence in the creation, analysis and retention of high-quality data assets.

Building a Common Understanding

1. **What do you consider are some of the international barriers to data security uplift?**
   Nil 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)?**
   The EU's General Data Protection Regulation (GDPR) is an emerging global standard with which Australian organisations must increasingly comply because they either process data about Europeans or else wish to collaborate on personally identifiable data with organisations otherwise bound by the GDPR. Many commercial technology providers already offer services capable of enforcing GDPR requirements.

   The European Commission does not currently recognise Australia as having data protections equivalent to those provided under the GDPR.[2] Over time, this will become increasingly problematic for Australian researchers as the proportion of research data they can access and the ability to collaborate with GDPR

[1] Data Security
[2] Adequacy decisions | European Commission

bound counterparts declines. Australian researchers may prefer to move their data and research activity onto offshore research infrastructure and into environments recognised as being compliant with the GDPR.

Recommendation: The Government to ensure there is formal mutual recognition of equivalency between GDPR (and other relevant global standards) requirements and Australia's data security policy environment.

3. **What additional guidance or support from the Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?**
   Nil response

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?**

   Nil response

5. **Does Australia need an explicit approach to data localisation?**
   The government is increasingly introducing data localisation provisions that are challenging for the research sector to meet. Recent examples include MyHealth and CovidApp data as well as under the *Data Availability and Transparency Act 2022 (Cth)* (s16A). These present challenges because research is inherently global in nature and because contemporary technology (or business models) do not support data localisation. Likewise, in the absence of any easy mechanism to assess the overall risk to data in other jurisdictions, organisations will default to requiring all sensitive data to be stored in Australia, including the prevention of access by non-Australian citizens or people not in Australia.

   Data localisation and data residency provisions are often seen as a proxy for security in terms of access, privacy, data integrity or data availability even though local data storage does not itself improve data security. Additionally, there is a tendency for people to see their organisation or jurisdiction as automatically safer for data storage and processing.

   For the research sector, rather than data localisation, the focus is on ensuring trusted access and availability over time, and the nature of the governance and oversight mechanisms needed to ensure that occurs. Note that, a data governance body may very well decide that data localisation is the most effective way to ensure control over data access, data integrity or data availability.

   Recommendation: The Government aligns legislative provisions for data localisation and data residency nationally, clearly outlining when it is required and providing public advice on data policy risks by country.

Role of Government

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?**
The ARDC plays a key role in enabling semantic interoperability across the research ecosystem, such as by providing shared, machine readable data vocabularies as well as the services required to enable their use.[3]

   Under its Institutional Underpinnings Program, the ARDC is working with Australia's universities to develop consistent approaches to data management planning. This work includes 'crosswalking' between the various classification systems used for handling sensitive data.[4] This draft 'classification crosswalk' is currently open for comment. In addition, the ARDC is aware of commercial companies 'crosswalking' national security classifications of different countries, but these different 'vocabularies' and their respective 'crosswalks' are not yet publicly available. The absence of these vocabularies and their crosswalks inhibit the ability to automate or streamline the sharing of sensitive information between organisations.

   Recommendation: The Government should provide a range of enabling data services that facilitate trusted sharing of sensitive information between organisations both nationally and internationally.

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?**
The OECD recently released a Policy Paper on the 'Integrity and security in the global research ecosystem'.[5] This paper states, 'responsibilities for research integrity and security are distributed across multiple actors in the international research ecosystem. These include, national governments, research funding agencies, research institutions, universities, academic associations, and intergovernmental organisations'.

   Similarly, the ARDC is not aware of any coordinating body in Australia with primacy for data security policy across research. The landscape instead emerges from local decisions made by hundreds of institutional governing bodies within their jurisdictional and organisational contexts taking into account the demands of their respective stakeholders: research funders, research subjects, investigators, research ethics committees, data service providers, etcetera.

   In response, the Department may be aware of the G7 Research Compact from the 2021 G7 Meeting in Cornwall[6] during which Members committed to '...establishing a new Working Group on the Security and Integrity of the Research Ecosystem.[7] The G7 Research Compact was drafted by the S7 Grouping, comprising the Science Academies of each of the G7 nations. As an invitee that year, Australia participated both in the G7 and the S7 groupings. The ARDC is not aware if Australia is involved in the proposed Working Group.

[3] https://vocabs.ardc.edu.au/
[4] https://ardc.edu.au/collaborations/strategic-activities/national-data-assets/institutional-underpinnings/
[5] https://www.oecd-ilibrary.org/science-and-technology/integrity-and-security-in-the-global-research-ecosystem_1c416f43-en
[6] G7 2021 Research Compact - GOV.UK
[7] Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise

Domestically, one possible peak reference body could be from Recommendation 25 of the recent PJCIS ‘Inquiry into national security risks affecting the Australian higher education and research sector’. [8] While the Committee noted the University Foreign Interference Taskforce (UFIT), by definition, related to foreign interference specifically and not other national security risks, it also recommended that UFIT:

> …develop a national security legislation implementation working group to assist universities in actioning national security legislation and related policies. This working group should develop understanding within the sector as to the relationship between various pieces of national security legislation.

While this group may contribute to streamlining national security related considerations, it still leaves a broad swathe of data protection policy considerations out of scope. This includes considerations for personal data under Privacy Acts or the Consumer Data Right, or for sharing commercial data to stimulate the digital economy, or else those likely to occur under the accreditation scheme of the Data and Transparency Act for sharing public sector data. The research sector engages with all of these frameworks and wants data protections as coherent as possible across frameworks. This implies a need for a more generalised approach to data protection beyond just the function of national security.

Recommendation: The Government develops a more generalised and enabling approach to harmonising data protection both globally and nationally beyond the relatively narrow function of national security.

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?**
Researchers and research infrastructure providers face two key challenges regarding data security policy. The first is discovering all data security related principles and rules before determining which of those apply. The second is synthesising sometimes inconsistent requirements and semantics relative to their research context, which typically occurs in complicated technical, operating and governance environments.

To resolve these issues, the government should facilitate better policy discovery. This service would be a catalogue of data security obligations, permissions and prohibitions linked to each respective policy.[9]

As well as improved discovery, the government could facilitate smart, guided inquiry as to which of those may be relevant given the users’ context, similar to the Business Licence and Information Service (ABLIS).[10] This should operate as a web data service so that any organisation could use the same linked data approach to integrate their local policies. The aim would ultimately be to create services that can be used to facilitate the smart drafting of future, more harmonised data security policies.[11]

The challenges described above are typical for nationally or globally distributed systems. To resolve these and other challenges in the research data system, the ARDC promotes adoption of FAIR data principles - that data is made Findable, Accessible, Interoperable and Reusable.[12] These principles are now being applied more

[8] Inquiry into national security risks affecting the Australian higher education and research sector – Parliament of Australia
[9] https://www.w3.org/TR/odrl-model/
[10] https://ablis.business.gov.au/
[11] https://clearbrief.com/ is just one example from the legal technology domain of a similar approach to policy drafting.
[12] https://ardc.edu.au/collaborations/fair-principles/

broadly to other domains, such as data vocabularies and research software. Adoption of FAIR principles for data security policies (and policies more generally) would reduce some of the challenges being experienced.

Recommendation: The Government facilitates adoption of the FAIR principles for data security policies as a necessary first step to improving policy harmonisation nationally.

Clarity and Empowerment for Business

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?**
   Nil response

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

11. **Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by the Government to help your business identify these risks?**
    Nil response

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).**
    Nil response

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

Empowering and Educating the Community

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?**
    Nil response

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?**
    Nil response

Other Issues

To ensure an appropriate co-design process, we welcome feedback on any additional data security policy issues not addressed in this discussion paper or any other issue relating to data security that the Government should consider.

In April 2022, the Department of Skills, Education and Employment delivered a new National Research Infrastructure (NRI) Roadmap.[13] The Roadmap 'identifies needs and sets priorities for future investment in Australia's national research infrastructure. It will guide the 2022 Research Infrastructure Investment Plan, and seeks to maintain Australian excellence in research and innovation and support Australia's ability to address emerging research challenges. Recommendation 7 of the Roadmap includes development of a National Digital Research Infrastructure Strategy:

> …(t)he Strategy will coordinate and integrate the national digital research infrastructure ecosystem and underpin collaboration at scale. This Strategy will support researchers across all fields by also providing the computing resources, digital tools, **data governance frameworks** and expertise needed to make best use of the data. It will **streamline access to data** and address computing, storage and analysis needs for researchers. The Strategy should be consistent with, and supportive of, other whole of government initiatives in this area, such as the Digital Economy Strategy 2030 and Australian Data Strategy. The National Digital Research Infrastructure Strategy should be developed by government over the next year with any immediate insights feeding into the 2022 Research Infrastructure Investment Plan.[14](ARDC bold)

Recommendation: If accepted by the Government, development of the National Digital Research Infrastructure Strategy provides an opportunity for the Department of Home Affairs to collaborate in producing coherent approach across a range of issues identified in the Roadmap relevant to a National Data Security Action Plan including:

- Data access and interoperability
- Data storage
- Trust and identity, and
- Data governance frameworks.

Should you wish to discuss these or other matters, please contact Dr Adrian Burton, Director Data Policy & Publication Services (adrian.burton@ardc.edu.au) or Mr Shannon Callaghan, Senior Data Policy Adviser (shannon.callaghan@ardc.edu.au).

[13] 2021 National Research Infrastructure Roadmap - Department of Education, Skills and Employment, Australian Government
[14] Ibid. pp. 76-80.