Response to the National Data Security Action Plan (NDSAP)

Dear Department of Home Affairs,

Thank you for providing us with an opportunity to respond to the National Data Security Action Plan.

We support the view in the NDSAP that Australia needs to get data localisation correct. Data localisation only goes part of the way to ensure citizen trust, in some cases full data sovereignty is required. We also agree with the view in the NDSAP that the Australian Government needs to be an exemplar and must develop a unified security classification system and assessment.

Data sovereignty is vital for building the public's trust in the Government. To access vital services and benefits, personal information must be divulged and recorded. Often, there is little to no choice in what personal information is stored by the Government. The public, therefore, has a higher standard for Government when it comes to the management of personal data. When people provide personal data to the Government, there is an expectation that this data will be stored and managed within Australia.

Data sovereignty is a growing concern for Australians. The Federal Government Information Commissioner's Australian Community Attitudes to Privacy Survey 2020[1] states that 74% of Australians consider it to be "a misuse of personal information" if their data has foreign processing access — an increase from 68% in the 2013 survey.

Further, the same report shows, many Australians see loss of data sovereignty being the single biggest issue with 41% of people believing sending data to foreign companies or countries is the biggest risk to privacy today. 92% of Australians have some concerns about the sovereignty of their personal data.

[1] https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

Building Trust in Government

Trust in how the Government handles the personal data is particularly cognisant when considered in the context of the new e-Health record system. Concerns around digital privacy and access to data has led to over 2m people opting out of the system since 16 July 2018.[2] It is estimated that approximately 22,000 people died from drug/adverse reactions in Australian hospitals every year[3]. These deaths could have been avoided if health professionals had been able to access health records. A lack of access to health records leads to poorer health outcomes for Australians and has already resulted in the unnecessary loss of lives.

Analysis of personal data is also gaining traction in Government as a way to realise benefits for citizens. For example, Australia's public health data holds enormous potential, which could lead to future medical breakthroughs, especially if all Australians were confident in sharing their health records. Another example is the analysis of police, financial, medical and social security records; which could be used in combination to potentially predict which citizens are more likely to be exposed to domestic violence, thereby addressing one of the major health and welfare issues[4].

In the context of nearly one million Australians opting out of eHealth[5] and the expectations Australians have on security and sovereignty[6], the opportunity for policy to have a material positive impact on the lives of Australians is substantial.

Understanding data sovereignty

Data sovereignty refers to the concept that data is subject to the laws and governance of the country in which the data originated.

In order of importance, the main sub constructs of data sovereignty are:

[2]ABC News http://www.abc.net.au/news/2018-09-18/my-health-record-number-of-australians-opting-out-revealed/10260902
[3]Tony Kitzelmann, CISO, Australian Digital Health Agency, presentation to AISA Brisbane Meeting, September 2018
[4]https://www.aihw.gov.au/reports/domestic-violence/family-domestic-sexual-violence-australia-2019/contents/summary
[5]https://www.healthcareit.com.au/article/senate-inquiry-hears-900000-have-opted-out-my-health-record-%E2%80%9Csignificantly%E2%80%9D-less-adha
[6] Australian Community Attitudes Towards Privacy Survey 2017, Office of the Australian Information Commissioner

1. **Legal** - the data is subject solely to the laws of the country of data origin. Generally, this means that the custodian must be owned and operated within the country.

2. **Operational** - data, metadata, monitoring and remote access are managed solely within the country of the data's origin.

3. **Physical** - the data at rest and in transit remains within the originating country.

We support the need for an explicit approach to data localisation and sovereignty.

The importance of legal jurisdiction

When in-country data is stored on services, which are subject to foreign laws, an organisation retains substantial legal obligations concerning that data's protection. However, the information may no longer be under their control and could be impacted by the laws and actions of a foreign country. This includes the future (as yet unwritten) laws of a foreign country. While the privacy laws of foreign countries may align to Australia's today, there is no certainty that they will do so in the future. At present, some countries have sectoral coverage, while others have omnibus law, with at least one national data protection law in addition to sectoral regulations. In Europe, under GDPR a citizen must be informed if their data is subject of foreign law and have the right to opt-out of non-sovereign services.

Global trends

Sovereignty is a growing consideration in many countries[7]. Canada, USA[8], UK[9], Germany[10], China[11] and many other countries have strong sovereignty requirements and capabilities. Interestingly in the United States, home to many public cloud services, the US Government does not allow the use of public clouds for sensitive data. Instead they elect to use special sovereign variants[12] known as "Government Cloud", "Community Cloud", "Sovereign Cloud" or "Secure Cloud".

[7] https://www.computing.co.uk/ctg/news/3027494/data-sovereignty-is-the-biggest-concern-in-cloud-transition
[8] https://aws.amazon.com/govcloud-us/
[9] https://ukcloud.com/why-ukcloud/sovereignty-security/
[10] https://azure.microsoft.com/en-au/global-infrastructure/germany/
[11] http://www.china-briefing.com/news/2018/05/07/cloud-technology-china-businesses-need-know.html
[12] https://aws.amazon.com/govcloud-us/

Sovereign supply chain

Many global firms have started to adapt their globalised business models to better work with citizen expectations despite having to share revenue with local companies as a result. "[Microsoft] recognises as a company that many European governments want more customised cloud solutions for their sovereign technology scenarios"[13].

In the modern IT system, data can be subject to a complex supply chain. The impact of sovereignty and the difficulty of achieving sovereignty varies by the type of services involved.

Supply Chain Layer	Importance of Sovereignty	Difficulty to achieve sovereignty
SaaS (Cloud)	Extreme *	High (Medium - low with sovereign IaaS)
PaaS (Cloud)	Extreme *	Medium - Low
IaaS (Cloud)	Extreme *	Low
Data Centre	Low	Low
Managed Services Provider	Low	Medium - Low
Data transit	Medium	Low

* Cloud providers generally have controlled remote access to customer data and encryption keys.

Assessing Data Sovereignty: A framework for the future

The framework below was created at the DTA Industry Innovation Day, where it provides clarity around assessing and communicating data sovereignty. The managed service provider, cloud and data centres are assessed across all aspects of data sovereignty (legal, operational and physical).

Service type	Legal	Operations	Physical
Managed Services Provider	[platinum, gold, silver, bronze, no rating]	[platinum, gold, silver, bronze, no rating]	[platinum, gold, silver, bronze, no rating]
Cloud	[platinum, gold, silver,	[platinum, gold, silver,	[platinum, gold, silver,

[13] https://blogs.microsoft.com/eupolicy/2022/05/18/microsoft-responds-to-european-cloud-provider-feedback-with-new-programs-and-principles/

	bronze, no rating]	bronze, no rating]	bronze, no rating]
Data Centre	[platinum, gold, silver, bronze, no rating]	[platinum, gold, silver, bronze, no rating]	[platinum, gold, silver, bronze, no rating]
Service rating	**(lowest of above ratings)**	**(lowest of above ratings)**	**(lowest of above ratings)**

Platinum: NV1 Staff, sovereign, change of control, financial remedy
Gold: Sovereign, NO Change of Control
Silver: Foreign owned/control, subject to foreign control, exit plan in place
Bronze: Current security policy compliant
No Rating: Foreign owned, no special protections.

This framework creates transparency around data sovereignty. A platinum rating means there are provisions to ensure future sovereignty. The ratings then progressively move down from “Platinum” to “No Rating” where there is no sovereignty.

If a foreign SaaS provider used an Australian Cloud or data centre, based on the framework a service could have a platinum/gold physical rating while having a bronze legal and operational rating.

Investment in Sovereign Capability

Sovereignty can only be lost once. Once a country loses its sovereign capabilities the effort required to build capability is substantial and often requires Government investment (e.g. Telstra and NBN). By creating a policy environment that supports sovereignty, the Government can organically foster domestic innovation and capability.

Nation building of sovereign capability has self-evident benefits:

- Improved national security capabilities.
- Improved trade balance.
- Increased tax revenue.
- Increased employment.
- Improved citizen trust.
- Reduced friction of digital transformation.

Data sovereignty provides an added layer of trust and protection for Australians. The knowledge that data is protected under Australian law and not subject to the laws of another country, provides Australians with a level of assurance that their concerns regarding data sovereignty are being addressed and goes a long way to building trust in Government and a better Australia for all Australians.

Transparency is important for citizens, government and industry. Home Affairs Secretary Mike Pezzullo made it clear in July of 2021 that the Government was going to take a hard line with Government suppliers. "What we would have in mind here, I suspect, to be very candid, would not be attractive necessarily to those companies," Mr Pezzullo said.

Consistency with other Government Policy

We support the current Government Buy Australian Plan[14] and encourage the NDSAP to align to these policies as well as have unifying role with the NSW Government Sovereign Procurement Taskforce[15].

Standards and Harmonisation

We support the existing standards outlined in the NDSAP, namely the:

- DTA HCF
- PSPF
- ISM

However we believe that the DTA HCF needs to provide more transparency through the addition of a new status:

- Sovereign Certified (new)
- Strategic Certified (existing)
- Assured Certified (existing)

Technical Mitigations

Implementation of technical mitigations such as encryption, Bring Your Own Key (BYOK) and access controls on first appearance seem to offer citizens protection when using foreign-based service providers. However, all technical mitigations that Vault has invested in have deep flaws or potential flaws. For example:

- Encryption - over time, most encryption technologies are compromised and once the service provider has someone's data there is no way to ensure that they no longer

[14] https://www.alp.org.au/policies/labors-buy-australian-plan
[15] https://buy.nsw.gov.au/ictdigital-sovereign-procurement-taskforce

hold that data at the point of compromise. This is particularly true when the laws of a foreign jurisdiction are involved.

- BYOK - in practice this is rarely implemented and when it is implemented, it requires the user to never provide the key to the service provider to be effective and for the technology to be flawless. In all practical cases, the provider will need some access to the key to provide their service. Even in end-to-end encrypted messaging services, the messaging app will need to have access to the key.
- Access control - in most cases, for a service provider to provide support, providers have privileged accounts that can override access controls.

Metadata

Metadata is data. An Internet of Things (IoT) device's metadata such as an IP address, time and location is in some cases more sensitive than the actual data. This was clearly demonstrated when a US defence base was located through metadata[16] and the actual data (heart rate and speed) was of almost no interest to an adversary.

Summary

Citizen trust in Government matters — a loss of trust will result in a loss of life and a dysfunctional economy. Data sovereignty represents an enormous opportunity for domestic organisations to bolster Australia's national security and drive Australia's economy.

Clear guidance from the NDSAP on data sovereignty requirements will result in increased and reliable investment from both global and domestic providers.

Data is becoming intertwined with the fabric of society. A balanced position from the NDSAP will set Australia on progressive, prosperous and safe path into the future.

Yours sincerely,

R Taylor-Price

Rupert Taylor-Price
CEO

[16] https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases