CONCENTRATION RISK OF GOVERNMENT DATA RISES FOLLOWING HOME AFFAIRS DECISION

AusTender information reveals yet another Government Department has selected the same, single provider that already holds 80 per cent of the value of Government data centre contacts.

The Department of Home Affairs has followed a long line of recent Federal Government agencies who have selected the same data centre supplier, including the Australian Securities and Investments Commission, the Australian Taxation Office, Services Australia, Australian Communications and Media Authority, Australian Fisheries, Department of Education, Department of Defence and the Department of Infrastructure.

All of these agencies entered into new contracts with this single data centre supplier within 2020.

This single-track approach is exposing the Government and Australians to significant risk by increasing the concentration of data with one data centre provider.

Research by the Australian Strategic Policy Institute (ASPI), commissioned by the SmartaData Alliance, found that of the 87 current data centre facilities contracts with Australian Government agencies, 54 per cent were with one data centre provider. That figure has risen following the decision by Home Affairs.

In terms of contract value, the Home Affairs decision means over 80 per cent of Government expenditure on data centres is now with one provider.

Spokesperson for the Smarta Data Alliance Armon Hicks, says this is a growing, significant risk which the Government must now recognise and address.

“It is extremely concerning that the Government continues to place all of its data eggs in one single basket, with one provider,” Mr Hicks said.

“That’s government data – yours and mine – with one provider, in one city, only five kilometres apart and it represents a significant sovereign risk for the Government, the community and every Australian.

“Data centres are critical infrastructure - Australia’s national security and the ability of the Australian Government to deliver services is contingent on the protection and the resilience afforded by Australia’s data centres.

“Our concern is that if there was a major incident that affected this single data centre provider like a bushfire or power outage or a serious cyber hacking or worse, a terrorist attack – will the government agencies that rely on that data to deliver essential services be able to access it?”.

“The potential damage that been caused by cyber-attacks was made clear with the recent attack on Nine Entertainment crippling its operations.

“If something similar were to happen to our Government departments the impacts could be catastrophic.”

In its 2020 Cyber Security Strategy, the Federal Government acknowledged the seriousness of the issue stating:

“Highly sophisticated nation states and state-sponsored actors continue to target governments and critical infrastructure providers. Australian Government or state and territory government entities were targeted in 35.4% of the incidents the ACSC responded to in the year to 30 June 2020

(see Figure 1). Around 35% of incidents impacted critical infrastructure providers that deliver essential services including healthcare, education, banking, water, communications, transport and energy. A successful cyber attack against one of these services could have significant ramifications for the broader economy and Australian way of life."

The Smarta Data Alliance argues that appropriate risk mitigation strategies must be applied to minimise the risk associated with major data loss or unavailability.

"Having over 80 per cent of the value of contracts for Government data with one service provider does not achieve this," Mr Hicks said.

"While each facility in itself may represent a secure environment, the fact of having both the prime and backup with one provider represents a risk aggregation that should be unacceptable given the catastrophic consequences of loss of that data."

"Our Government departments need to recognise the inherent risks to the public of storing so much data within a single data centre provider.

"We need to put a solution to this in place now, rather than waiting for an unmitigated disaster to happen first.

"This means a shift in the implementation of the procurement guidelines. We cannot go on inadvertently creating one big target because of the concentration of data to one service provider.

"The Federal Government must spread the risk across diverse data centre providers with separate management, corporate and operational structures, mandated distance separation, multiple connectivity, and other risk mitigations to keep all Australians' data storage infrastructure and data secure."

Government and data centre providers must work together to ensure Australia's data and the infrastructure protecting that data remains safe.

ENDS

About the Smarta Data Alliance

The Smarta Data Alliance is a coalition of peer data centre operators and cloud service providers in Australia who have come together to raise concerns about the inherent risk in the current concentration of critical national federal government data centre provision with a single provider. Membership of the Alliance is open to all data centre operators who share this concern.

Contacts

Sarah Michael
0401 591 286
mailto: smichael@apa.net.au