SAP AUSTRALIA

SAP RESPONSE TO THE CYBER SECURITY REGULATIONS AND INCENTIVES DISCUSSION PAPER

SAP Australia

August 2021

THE BEST RUN SAP®

SAP RESPONSE TO THE CYBER SECURITY REGULATIONS AND INCENTIVES DISCUSSION PAPER

SAP Australia Pty Ltd, a subsidiary of SAP SE (referred to henceforth as '**SAP**') a leading global software provider, would like to thank the Australian Government for the opportunity to contribute to the Cyber Security Regulations and Incentives Discussion Paper (**the Discussion Paper**).

Australia's Cyber Security Strategy 2020 laid out a clear guide on how the Australian Government aims to achieve its goal to uplift the digital economy to be more resilient to cyber security threats. SAP welcomes the ambition and acknowledge the importance of this challenge. It is a challenge that will require behavioural change through education across the whole economy.

The impact to businesses and individuals from cyber security threats is real and increasing. While the Australian government has an accountability to protect its citizens and businesses, its actions must be proportionate to the challenge at hand.

For example, the impact to Australia's critical infrastructure (**CI**) by cyber-attacks has the potential to create massive disruption to operations. In recognition of this impact, the Australian government is introducing a range of powers and obligations to uplift the cybersecurity for CI businesses. While this will impose new mechanisms for reporting and compliance on these sectors, the regulation underlines the importance of having a high level of cyber security preparedness in the CI sector.

For large IT companies like SAP, cybersecurity underpins their market proposition. And investments are made accordingly. SAP provides business-critical software solutions to more than 440,000 customers worldwide and serves more than 200 million users worldwide with its portfolio of cloud solutions. Regardless of what regulation might direct, at SAP, cybersecurity is a top priority, our business could not operate any other way.

However, outside CI and the IT sectors a different approach is required. For many of these other businesses their size may make devoting internal management attention to cybersecurity difficult when balancing against many other critical business priorities. Any cyber-attack on a business has the potential for negative impact on livelihoods, however the impact to the whole economy from a cyber-attack on non-CI businesses is likely to be less severe.

The discussion paper has outlined possible regulations and incentives the government may use to address this business cohort. We would also encourage the government to also consider measures that may accelerate the Australian businesses onto cloud-based services as way of delivering whole of economy cyber security uplift.

Benefits of cloud to cybersecurity

We consider that accelerating the transition of the Australian economy to cloud-based Software as a Service (**SaaS**) offerings is an important opportunity to uplift the resilience of Australia's digital economy in relation to cybersecurity threats. We consequently encourage the government to look at ways to drive cloud adoption across Australian businesses.

Cloud solutions offered by trusted providers are delivered with vulnerabilities patched on an ongoing basis. This can be contrasted with the scenario where businesses use applications sitting on their PCs where security updates require manual intervention from the business.

SaaS solutions are also scalable so that real-time security monitoring can be deployed more efficiently than scenarios where the application is hosted locally.

Although cloud is no silver bullet and needs to be combined with good cybersecurity hygiene practices, as these protections are part of the SaaS, it reduces the management attention and effort required to adequately manage cyber-security for any business.

Governance Standards for large businesses

The Discussion paper raises the potential introduction of measures to address cyber-security governance standards. For example, business-wide risk management practices, internal accountabilities, and reporting arrangements.

SAP welcomes an ongoing conversation between the Government and large businesses to draw attention to and focus on the management of cybersecurity risks. An engagement with the business community where best practice and advice is documented and shared by the Australian Government with the business community is a good idea to help large businesses. This will help to provide clarity and guidance.

SAP supports this advice on a voluntary basis and does not support the imposition of regulation mandating governance standards on large businesses.

Minimum standards for the protection of personal information

SAP agrees that a greater take-up of cybersecurity controls at all levels of businesses will reduce the likelihood of breaches impacting personal information across the whole economy.

As a business SAP has established controls to protect the personal information of our customers and our employees.

SAP currently holds a BSI certificate BS 10012:2017 that certifies SAP's implementation and operation of a Data Protection Management System, and a certification of its ISO 27001:2017 for SAP's Information Security Management System. These certifications reflect the technical controls for data protection.

SAP also has in place a Global Data Protection and Privacy Policy (**Global DPP Policy**) that serves as SAP's group-wide minimum standard for the data protection and compliant processing of personal data via privacy principles based on the EU General Data Protection Regulation (GDPR). The principles in the GDPR are arguably more prescriptive than those set out the Privacy Act 1988.

The technical controls combined with our Global DPP Policy manages the protection of personal data, models relevant business practices and provides confidence to our customers that their data receives appropriate protection.

A complete documentation of SAP's standards, processes and guidelines for protecting data and information can be found on SAP's public website[1].

SAP does not support the introduction of a cyber security code under the Privacy Act. Instead, there should be increased investment in programs, policies and education that will encourage businesses of all sizes to move into a cloud environment. This would need to be combined with ongoing investment in education and stakeholder engagement on evaluating what constitutes relevant practices when it comes to the protection of personal information. The development of relevant practices should mirror international standards such as the BSI and ISO which in SAP's opinion provides for a good template to ensure that adequate data protection measures have been taken.

Transparency and Disclosure

SAP is committed to identify and address security issues that affect our software and cloud solutions. We have established processes to support the reporting of security vulnerabilities including a-web portal entry and the option for our customers to register for incident notification.

Many Australian businesses and global peers also have similar processes to support the reporting of security vulnerabilities to the business and the communication of incidents to customers. Security researchers are also able to report security vulnerabilities to ACSC.

SAP acknowledges the discussion paper's research that suggests low levels within the Australian market of documented policies. We therefore recommend that as a first step the Government undertakes an education campaign for businesses with tool kits on what reflects relevant practices when it comes to responsible disclosure.

[1] d.dam.sap.com/a/AUnma/70426_GB_43200_enUS.pdf