AUSTRALASIAN HIGHER EDUCATION CYBERSECURITY SERVICE **(AHECS)**

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022: Australasian Higher Education Cybersecurity Service (AHECS) submission

Classification: Public

07 November 2022

The Australasian Higher Education Cybersecurity Service (AHECS) is the higher education and research sectors peak cybersecurity body. AHECS represents the sector on cybersecurity issues, leveraging the capabilities and expertise of its partner entities to strengthen the overall cybersecurity posture of the sector.

AHECS is delivered in collaboration with Australia's Academic and Research Network (AARNet), AusCERT, Council of Australasian University Directors of Information Technology (CAUDIT), Research and Education Advanced Network New Zealand (REANNZ), and the Australian Access Federation (AAF). This collaboration illustrates a joint approach by higher education institutes and key supply chain partners including the sectors internet service provider (both Australian and New Zealand), federation provider, and cyber emergency response team.

AHECS's purpose is aligned to the principles of being stronger together and 'all boats lift on a rising tide'. AHECS was developed specifically for the sector by the sector, to collectively mature the sectors capabilities and continuously evolve and strengthen cybersecurity defences in the ever-changing environment of cybersecurity threats. This is achieved through coordination of members and partners to inform direction, advocate, share intelligence, reduce barriers to the implementation of good practice, identify and act on capability gaps, and holistically defend the sector from continuously evolving cyber security threats in conjunction with key vendors.

AUSTRALASIAN HIGHER EDUCATION CYBERSECURITY SERVICE **(AHECS)**

AHECS welcomes this opportunity to engage with the Committee on the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022. Data security and privacy go hand in hand, and AHECS submitted a response to the National Data Security Action Plan in June 2022, noting support for the Australian Governments comments regarding the high value of data and the vision for data security by ensuring data is appropriately secured, accountable, and controlled.

After discussion with CAUDIT Members, AHECS note the following key recommendations to the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022:

1. **Reasonable penalties for serious and repeated, including clarification on these terms**

   The size of the proposed penalty payment is substantial and would have a considerable negative impact on small to medium enterprise, and not-for profit organisations such as CAUDIT. Furthermore, financial penalties don't address the core of the issues with the state of information security within Australian. These issues are multifaceted and include resourcing limitations, compliance requirements, increasing costs, and supply chain risks. By fining those unfortunate to suffer breaches, it deters a collaborative approach to information security, and is detrimental to increasing cybersecurity maturity in Australia. Fines are also a reactive outcome. Consideration for proactive measures to encourage risk reduction and mitigation should also be considered.

   The definition of serious and repeated is unclear in the proposed legislation and leaves significant room for interpretation. These definitions are crucial to the legislation and require clear guidance.

Key recommendations
- Reconsider penalties as a whole, instead consider education and early intervention (if penalties necessary, they should be appropriate to business size and turnover) - Provide clear guidance on definition of *serious* or *repeated*

2. Thought leadership

Whilst we understand the recent breaches in Australia has led to a quick call to action and response, this topic needs higher level thought leadership for long term success and to uplift cybersecurity across Australia. The Committee may wish to consider a collaborative industry thought leadership group, in which long term planning is undertaken that identifies the purpose of the legislation, Australia's cybersecurity needs, and evaluates the measures to best achieve the desired outcome and protect Australians privacy. There is confusion as to how much data needs to be retained as part of the meta data retention regime, and this should be reviewed, as well as clear guidance around data retention and consumer ownership of data (including opportunities to delete one's own data records).

Additionally, a 2-week turnaround for privacy reform legislation is not sufficient if seeking a true industry collaboration.

Key recommendations

- Instead, or in support of penalties, consider proactive legislation or support providing benefits or deductions for organisations undertaking information security certification reducing risk of breaches
- Consider an industry and Government collaboration to information security thought leadership in Australia
- Ensure engagement with industry and calls for submissions provide sufficient time frames to allow for appropriate and meaningful responses

3. Education and existing frameworks, including data retention and national data retention guidelines

Technical controls won't completely circumvent human error. Instead of legislation and penalties, the Government should consider the benefit of promoting and teaching cyber

safety, the value in data assets, and focus on the uplift of education and understanding of the entire Australian population as a collective group. Universities need to comply with a significant number of Acts and regulations which govern what, to whom, and how they provide services, and what we need to collect / retain to prove this. In essence, once the university has collected/captured or created something as required, the retention of that record is regulated, and data retention requirements vary state to state. The Government should consider a national approach to data retention. Additionally, instead of re-inventing policy, the Government may wish to consider the benefit of looking to others who have been successful in this area, for example GDPR (or explain reasons for not opting to use this existing framework).

Key recommendations

- Look to GDPR for guidance
- Review data retention requirements

Thank you for the opportunity to provide feedback on the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 202.

If you would like further information, or to explore any of these comments, please contact:

Greg Sawyer – Chief Executive Officer

Council of Australasian University Directors of Information Technology (CAUDIT)

Nikki Peever – Director, Cybersecurity Program

Council of Australasian University Directors of Information Technology (CAUDIT)