30 July 2021

Consumer Data Right Division
Treasury
Langton Cres
Parkes ACT 2600

By email: data@treasury.gov.au

Submission to Treasury for Consumer Data Right rules amendments (version 3)

Thank you for the opportunity to provide feedback on the proposed amendments to the Consumer Data Right (CDR) Rules.

About Astero

Astero is an information security firm based in Australia with clients in the USA, UK and New Zealand. We specialise in helping high growth startup companies in regulated industries manage their cyber security and data privacy risks, while meeting industry compliance and accreditation requirements (including SOC 2 and ISO 27001).

Astero's experience assisting with CDR readiness

Astero has assisted multiple non-ADI organisations with meeting the information security requirements in the CDR Rules, successfully receiving ASAE 3150 independent assurance reports and becoming Accredited Data Recipients (ADRs).

As a leading provider of CDR readiness services, Astero has valuable knowledge in applying the CDR Rules in practice, notably the information security and data boundary requirements in Schedule 2 Part 1 and Part 2.

Feedback

In this submission we have focused on the following subset of amendments to the CDR Rules Schedule 2 Part 1 and Part 2:

> *Schedule 2 Part 1*
> *1.5 Step 3—Have and maintain an information security capability*
> *(1) The accredited data recipient must have and maintain an information security capability that:*
> *(a) complies with the applicable information security controls specified in Part 2 of this Schedule;*

- Astero is supportive of organisations implementing information security controls commensurate with the risks to their information assets, however the addition of "applicable" in this section is open to interpretation and contradicts the title and nature of Part 2 ("Minimum information security controls"). This introduces the risk of ADRs using their own judgement to determine the controls that are applicable to their CDR data environment, underestimating the full extent of controls required to meet the ASAE 3150 independent audit requirements.

- We acknowledge that this addition could be driven by the inclusion of the new third party management control in Part 2 that only applies to sponsors. Astero recommends that the table in Part 2 is amended to clearly label the minimum controls that are applicable to sponsors and affiliates, respectively.

- Additionally, if Treasury has a view to truly allow ADRs to determine the minimum controls that are applicable to their CDR data environment based on risk, Astero is supportive and recommends this is clarified in Part 1, 1.5 (1) (b).

Schedule 2 Part 2
2.2 Information security controls
(7) A sponsor must implement a third party management framework
(a) Implementation and maintenance of a third-party management framework
Affiliates must be managed by the sponsor in line with a defined third-party management framework, which should include requirements and activities relating to:

- *due diligence prior to establishing new relationships or contracts;*
- *contractual agreements reflective of responsibilities for the CDR data and data environment;*
- *annual review and assurance activities;*
- *reporting requirements;*
- *post-contract requirements.*

- We welcome the inclusion of third party risk management controls under Schedule 2 Part 2 and strongly support ADRs having the freedom to define their own frameworks. This is a welcome change from the overly prescriptive affiliate self-assessment proposed in the *Consultation on proposed changes to the CDR Rules* (September 2020).

- However, it is recommended that ADRs follow a risk-based approach for gaining assurance over third parties. This would promote flexibility and ensure ADRs prioritise rigour for third parties presenting the highest risk. We recommend that the threat and risk assessment requirements in Part 1, 1.5 (1) (b) are updated accordingly and are used to inform the implementation and operation of third party risk management frameworks under this new control.

- Given the ongoing rise in supply chain attacks in Australia and internationally, Astero recommends that this control extends beyond affiliates and includes other relevant third parties such as suppliers. In practice, we already see ADRs considering the risks and controls of third parties in their CDR data environment boundary documentation and information security policies. This recommendation seeks to consolidate existing process and standardise a critical component of information security risk management. Implemented at the discretion of each ADR in combination with the risk-based approach recommended above, we do not see an additional burden considering the heightened threat environment.

Astero thanks Treasury for the opportunity to make this submission and we will continue to constructively contribute to the ongoing development of the CDR Rules.

Please do not hesitate to contact me should you wish to discuss this further.

Yours sincerely,

Sandeep Kumar
Founder & CEO
Astero AU Pty Ltd