

8 November 2021

Australian Competition & Consumer Commission
GPO Box 3131
Canberra ACT 2601

Via online form.

Re: Consumer Data Right sponsored accreditation - information security self assessment and attestation consultation

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to make this submission on behalf of our members and the business software industry. Please find our response below.

DSP View of Sponsored Accreditation & Schedule 2 Requirements

Under the current requirements, both DSPs and third parties receiving CDR (including CDR derived) data will need to seek an accreditation pathway, which in some instances will include the sponsor-affiliate model. The current definition of CDR derived data may mean that our members, who operate app stores and allow third party software to connect and share data, will have to sponsor between 20,000 and 30,000 apps which is just not feasible.

DSPANZ believes that a better model to regulate DSPs under the CDR rules is to recognise both the Operational Security Framework (OSF) and the Security Standard for Add-on Marketplaces (SSAM). The ACCC has already taken the first step and recognised the OSF as an alternative pathway to accreditation for DSPs at the unrestricted level. The next step would be recognising the SSAM as an alternative pathway for third parties in DSP ecosystems who would become affiliates under the CDR.

The creation of both of these standards is the product of a successful government and industry partnership that has resulted in the protection of millions of small businesses, individual taxpayers and intermediaries over the last four years. Before the OSF was introduced in 2017, the ATO recorded just two software breaches that resulted in 49,600 compromised TFNs and ABNs and the actual number is expected to be much higher as breach reporting was not a mandatory requirement for DSPs. Fast forward to 2020 and a total of 19 breaches resulted in only 1065 compromised TFNs or ABNs with DSPs now required to report all breaches.

What we have discovered through reviewing the SSAM from August to October this year is that there is very limited appetite from this ecosystem of developers to introduce the CDR Schedule 2 requirements. For these app developers, these requirements would involve a lot of work for

very little uplift in security considering that the SSAM already covers the security requirements of the industry well.

DSPANZ would be more than happy to provide more detailed information about the SSAM and how it works in combination with the OSF and how the two could be recognised under the CDR.

Alternative Accreditation Pathways

Without alternative accreditation methods for affiliates in the CDR model, it will create a significant barrier to entry for DSPs and their app ecosystems. As suggested above, we recommend recognising the SSAM alongside the OSF as an alternative accreditation pathway to meeting the Schedule 2 requirements.

Support for Businesses Seeking Accreditation

Meeting the Schedule 2 requirements will come at a significant effort and cost, especially for the businesses that do not have security expertise at their disposal. The ACCC should consider how they will support businesses looking to become accredited as there will be many questions along the accreditation process. This support could include regularly updating the accreditation and attestation document and providing further guidance on implementation.

Once sponsored accreditation is available, we anticipate that businesses will seek clarifications and support from the ACCC as they work their way through the forms. This support should be timely, around two to three business days, to be viable for businesses working through the accreditation process. We recommend following a model similar to how the ATO's Digital Partnership Office supports DSPs through the OSF process.

What has not been made clear on the form is whether the form should be provided to the ACCC completely populated or whether this can be used as a guide and submitted using a different format. More information should be included either on the form or on the website page where the form is hosted about the accepted submission formats.

Costs Involved

We anticipate that the costs of using a data aggregator is likely to increase under the sponsored accreditation model as the aggregators will now have additional responsibilities and liability. This will be a barrier to entry for many looking to become accredited.

This is in stark contrast to how DSPs work with and support the add-ons operating in their app stores. More often than not, DSPs provide free and public APIs and have developed extensive resources to support add-on applications through app development and meeting any security requirements.

DSPANZ would appreciate the opportunity to engage further on this submission. For further information, please contact Maggie Leese.

About DSPANZ

Digital Service Providers Australia New Zealand is the gateway for government into the dynamic, world class business software sector in Australia and New Zealand. Our members range from large, well-established companies through to new and nimble innovators who are working at the cutting edge of business software and app development on both sides of the Tasman.

Yours faithfully,

Simon Foster,
President & Director,
DSPANZ

