Australian Business Software Industry Association

Level 5, 45 Clarence Street
Sydney NSW 2000
info@absia.asn.au | www.absia.asn.au

15 October 2019

Office of the National Data Commissioner
PO Box 6500
Canberra ACT 2600

Response to Data Sharing and Release - Legislative Reforms Discussion Paper

Dear Office of the National Data Commissioner,

The Australian Business Software Industry Association (ABSIA) welcomes the opportunity to make this submission on behalf of the business software industry and our members.

We welcome the opportunity to speak with the Office of the National Data Commissioner (ONDC) in regards to this submission with ABSIA and our board members.

In the following pages, please find our responses to select questions and other comments as necessary. Overall, we support the work of the National Data Commissioner and we look forward to your response. We also look forward to our continued relationship.

For more information ABSIA's submission please contact either:

Simon Foster
ABSIA Director and Vice President
[redacted]

or

Karen Lay-Brew
ABSIA Director and Head of Government Partnerships
[redacted]

Sincerely,
ABSIA.

Questions 2 and 9:
A significant challenge for this framework is the unintended consequences of re-identifying individuals within a data set when openly releasing anonymised data. In order to mitigate this risk, while still gaining the economic benefits of data sharing, the focus should be on a controled access model of data sharing. Further, there should be a purpose test to determine the potential risks of releasing a dataset before it is shared or released.

On the flip side, the availability of open data for consumption by businesses and the industry presents exciting opportunities. Aggregated and summarised data, that will not allow for individual identification, can also be considered as that would still permit for the extrapolation of insights that can be utilised for research and identifying opportunities.

Question 3:
We believe this framework will enable streamlined and safer data sharing through the accreditation processes set out in the discussion paper. However, it is important to know how this framework will be funded and whether it will generate any costs for end users. If there is a significant financial barrier, it may prevent smaller businesses from being able to participate in the framework and benefit from shared data.

Question 4:
We understand that the focus may be shifting primarily towards data sharing, rather than release and therefore may require two different legislations. The names should be simplified to ‘Data Sharing Act’ and ‘Data Release Act’ to reflect the different considerations needed for each framework.

Question 5:
The purposes for data sharing meets our expectations for the simplification and accessibility of government services as a primary purpose of data sharing. Within the purposes, there are many opportunities to enhance the end user’s experience with government services, while also allowing the government to better analyse its own processes.

We understand and, at this time, support that the purpose of “compliance” has been excluded from the purposes of sharing data. Having said that, this exclusion may prohibit or prolong designing effective and efficient government services. The legislation should have a mechanism for regularly reviewing its effectiveness and adjustments as required to ensure that “compliance” can be within scope for the framework when appropriate.

Question 6:
From the discussion paper, we can see the value that data sharing can provide in commercial settings. We believe our industry would benefit greatly from accessing shared data in being able to find market gaps and new opportunities to create innovative products and solutions for businesses.

Here, we believe it could be difficult to prescribe detailed precluded purposes as the opportunities can be numerous. While existing legislative protections would work to prevent some commercial activities and exploitation, to allow for a better understanding of how they would work with the *Data Sharing Principles* and *Privacy Principles*, it may be beneficial to include worked examples of what would be considered a breach and what would happen if a breach were to occur.

Question 7:
Galexia's *Privacy Impact Assessment* and the *Data Sharing Principles* appear to consider relevant risks. However, a more detailed Risk Management Framework covering each of the five *Data Sharing Principles* would be required for the communities to feel more confident.

Question 10:
We support the two levels of accreditation (organisational and individual) and the core principles driving the accreditation criteria. However, we believe that individuals should restart the accreditation process if they change employers. A change in employer could impact on the user's ability to meet the accreditation criteria such as being able to protect the data in their new organisation at an appropriate level. Restarting this process would allow for data custodians to address these issues sooner rather than later.

Question 11:
It is evident that the ONDC supports transparency in the system and we support this approach as it will assist in increasing public trust in the framework.

However, while accountability is addressed, it is difficult to picture who is responsible for what and where and therefore who is accountable if something were to go wrong. To increase this understanding, it may be beneficial to create a visual representation of an example data sharing and/or release framework to show where accountability and responsibility lie and also the areas in which different legislations would apply.

Question 12:
On face value, the balance appears to be appropriate. However, a high level principle can only be tested through applying it rigorously to sample use cases. We recommend "privacy and security by design" as a philosophy to minimise complaints and redress options due to intended or unintended consequences of abuse of data. Review rights fit in the by-design part of the framework.

Question 13:
If this framework focuses on controlled data sharing rather than open data release, we would recommend the following penalty approach. Penalties should be more severe for intentional or unintentional breaches of controlled data sets, resulting from a lack of sufficient security or protections, when compared to an unintentional breach where all reasonable precautions have

been taken. This would encourage better security measures across the framework and deter non-compliance.

On a similar note, given this framework involves the sharing of data and connecting to various data custodians, it will be important to consider what type of security framework should be applied across this system. We would suggest opening up a conversation with the ATO to understand their ecosystem security initiatives. There may be scope to apply one security standard to secure all these data transaction processes. We would support this and could offer guidance alongside the ATO.

Question 14:
The ONDC is still a relatively new office, and at this time, the lines of responsibilities between the ONDC and the federal and state Office of the Information Commissioners are unclear. We would like to see the ONDC become the central organisation that oversees “all things data” in Australia, ensuring that the data landscape, both in the public and private sectors, are adequately and securely covered for Australia’s competitiveness on the global stage.

We encourage the National Data Commissioner to create and develop relationships with industry associations, organisations and businesses so we can all work together to support safe data sharing and work towards a national data sharing system. While it is important for the National Data Commissioner to be a leader here, it will be through these relationships and learning from one another that will aid in bolstering this system.

As we have mentioned previously, we would be very interested in assisting where we can. This could include a webinar between our members and the ONDC so you can learn from them about any missed opportunities or unintended consequences of data sharing that they understand best.

Further Feedback:
A further concern that we have is the use of the term ‘data service provider’ and its potential to become shortened to ‘DSP’. This could be confusing for those operating in the software space where DSP also has meant ‘Digital Service Provider’ in the finance portfolio. We suggest using another term such as data custodian to avoid any potential confusion down the line. Even though we understand that the ONDC is not interested in shortening the name to DSP, this does not stop the wider community from doing so.