[redacted]

27 October, 2021

The Hon Stuart Robert
Minister for Employment, Workforce, Skills, Small and Family Business
Parliament House
Canberra, ACT 2601

Dear Minister Robert

Trusted Digital Identity Act and supporting Legislation 2021

We would like to commend the Australian Parliament, with the strong assistance provided by the Digital Transformation Agency, in pursuing a thorough and detailed review of the requirements of the Trusted Digital Identity legislation shortly due to be introduced for debate in parliament. We applaud the extensive and continuing consultation process being followed to ensure the legislation covers the needs of all Australians.

It has been critically identified that in order for the Trusted Digital Identity Framework (TDIF) and legislation to be successful it needs to achieve a very high level of trust with Australian consumers in their belief that the information about their identity will be held at the highest level of security and only used with their explicit consent in a manner which prevents misuse of their data. To achieve this level of public trust it is important that the Government ensures that at all stages of the process that data about an individual is technically held in a way that it cannot be misused intentionally or unintentionally and that the governance framework surrounding the platform is sufficiently robust to address unexpected issues in a way the public would consider their interests are at the heart of how the information is accessed and used.

[redacted] is a public-listed entity which for over 10 years has championed the safe and secure collaboration of data in a way which ensures that only the necessary piece of data, pre-agreed by data owners, is exposed to another party for beneficial collaborative purposes. We provide the [redacted] Secure Collaboration Platform to customers in Australia, the United State and the United Kingdom to enable them to match and learn across private and sensitive data whilst it remains encrypted, without any parties ever seeing the data and without it ever leaving the control of the approved data holder/owner.

Globally, we see an accelerating trend towards both private and public sector organisations collaborating to share data, with digital identity being critical to the way data is securely and equitably utilised to provide enhanced and personalised interactions for citizens.

[redacted]

In the US, [redacted] has been selected as the platform of choice by gaming regulators and large health insurance funds to ensure their highly sensitive customer data can be utilised to provide a service without ever being decrypted.

We believe the current draft of the Trusted Digital Identity Framework needs to reflect the emergence of well-established Privacy Enhancing Technologies, similar to as supported by the United Nations. We refer the reader to the United Nations Handbook on Privacy Preserving Computation Techniques.

Our global experience and the work undertaken by the UN demonstrates that it is now well accepted that security, privacy and trust can be uniquely enhanced by keeping data encrypted not only whilst it is at rest or in transit but also whilst it is in use.

The diagram below outlines the various states of security that are now seen as important to be incorporated in data collaborations and matching. [redacted], as an Australian owned entity has built a unique platform to deliver capability to enable matching and analytics to occur whilst the data remains encrypted – ie whilst "in use" a sector now growing very quickly due to data owner demand.


[redacted]

[redacted]

There currently exist a series of approaches to encryption during use of the data which include the highly secure fully homomorphic encryption approach (as used by [redacted]),

differential privacy techniques, multi-party secure computation and partial homomorphic encryption.

These add a further level of security through internationally accepted encryption standards such that data cannot be "hacked" or misused during the use/matching phase.

Recommended Amendments

The current draft of the Trusted Digital Identity Framework Accreditation Rules at Chapter 4, Part 4, Clause 4.2.8(1) has limited the Protective Security Requirements to only a need to encrypt data whilst at rest and in transit as per the extract below:

"4.2.8 Cryptography (A, C, I, X)

(1) An entity must ensure that all digital identity information held or processed by or on behalf of the entity in connection with its accredited facility is protected in transit and at rest by approved cryptography."

We believe it is more in keeping with industry trends and citizen expectations for the clause to be amended to add the requirement for **encryption to also be required whilst the data is in use for matching or other approved analysis** and the clause amended to read as follows:

"Amended 4.2.8 Cryptography (A, C, I, X)

(1) An entity must ensure that all digital identity information held or processed by or on behalf of the entity in connection with its accredited facility is protected in transit, **in use** and at rest by approved cryptography."

Conclusion

We believe the addition of the requirement to include information and data be encrypted whilst in use will significantly increase the level of trust in the Trusted Digital Identity

framework by impairing any opportunity for misuse of data being held or used by accredited providers.

We would welcome the opportunity to elaborate or clarify our recommendation further as part of the consultation process and to ensure Australian citizens can be confident that have the most secure and trustworthy framework managing their digital identity.

Yours sincerely

[redacted]