

# SUBMISSION

## Digital Identity legislation

Thank you for the opportunity to make a submission in relation to the proposed Digital Identity legislation. The following comments are provided in relation to embedding appropriate protections in law for all Australians in relation to Digital Identity:

1. Digital Identity in Australia must respect individual human rights, individual rights to privacy and protection of individual freedoms for every Australian man and woman. These protections must be firmly embedded in Australian law and designed to prevent the misuse or abuse of Digital Identity.
2. The use of Digital Identity must be voluntary and physical forms of identity such as a physical passport, drivers license, birth certificate, or other suitable documents must remain acceptable forms of identification.
3. Governments, organisations and individuals must allow ongoing use of physical forms of identification. Governments and organisations must be required by law to continue accepting physical forms of identification.
4. Governments and organisations must be required to continue producing physical forms of identification for individuals such as a physical passport, drivers license, birth certificate, or other suitable identification documents. The fee for producing physical forms of identification must not exceed the cost of materials and time for them to be produced and must not be charged to an individual with the intent of making a profit.
5. All individuals must retain the right to discontinue use of a Digital Identity and use physical forms of identification.
6. A Digital Identity must not be linked to any government or private database, system or other similar information for the purpose of data collection, data storage or data analysis services without an individuals full knowledge and consent.
7. Any services linked to the Digital Identity must not be linked without an individuals full knowledge and consent. Every individual must be provided access and means to easily discontinue the use of Digital Identity linked services at any time.
8. Individuals must not be denied goods or services if they choose to use physical forms of identification.
9. Any data or information linked to a Digital Identity must be identified to the individual and they must be provided full access to this data or information if requested.
10. An individuals Digital Identity must not be shared with any government, organisation, individual or any other entity without an individuals full knowledge and consent.

11. All components of a Digital Identity system must remain specifically in the ownership and administration of the Australian Government on behalf of and guided by the wishes of the Australian people. This would include systems infrastructure, administration centres, data storage centres, data encryption and security services and any other associated resources, systems and infrastructure. Digital Identity and systems must be protected by the highest standards for data privacy and security.
12. No private organisation, private company or private entity should be given any administrative access or edit capabilities within the Digital Identity system.
13. A Digital Identity system must remain sovereign to Australia and Australians. No foreign government, foreign organisation or foreign entity should have any access to the system, system data, or the Digital Identity of any Australian man or woman.
14. The only condition to obtain and use a Digital Identity should be that an individual is born in Australia, is an Australian resident, or is an Australia Citizen.
15. No government organisation, agency or entity should be given access to the Digital Identity of any Australian without the individuals full knowledge and consent.
16. No private organisation, private company or private entity should be given access to the Digital Identity of any Australian without the individuals full knowledge and consent.
17. A Digital Identity must not be used on its own or in conjunction with any other system to infringe on an individuals right to privacy such as monitoring or tracking an individuals movements or purchasing habits.
18. A Digital Identity must not be linked to a persons biometric data or used for purposes without an individuals full knowledge and consent.
19. A Digital Identity must not be used on its own or in conjunction with any other system to implement measures that would limit an individuals ability to access private and public services, or to access private and public spaces and facilities, or to infringe on basic human rights and individual freedoms.
20. A Digital Identity must not be used on its own or in conjunction with any other system to implement measures that would limit an individuals ability to access and use funds from their own bank account or other financial accounts, or to access any other financial services.
21. A Digital Identity must not be used on its own or in conjunction with any other system to implement measures that would limit an individuals ability to unconditionally access and purchase goods or services at any location in Australia or the world.
22. A Digital Identity must not be used on its own or in conjunction with any other system to implement measures that would limit an

individuals ability to be employed or engage in work to earn an income.

23. A Digital Identity must not be used on its own or in conjunction with any other system to implement measures that would limit an individuals ability to access training and education services.
24. A Digital Identity must not be used on its own or in conjunction with any other system to implement measures that would limit an individuals ability to access food, clothing, property and housing, the internet, or other communication services.
25. A Digital Identity must not be used on its own or in conjunction with any other system to implement measures that would limit an individuals ability to obtain a drivers licence (or any other type of vehicle licence), or a passport, or to travel.
26. A Digital Identity must not be used on its own or in conjunction with any other system to implement a social credit score or rating system, or other similar score or rating system that could intentionally or unintentionally be used to penalise an individual for not complying with specified standards or rules, or for free thinking, or for free speech and expressing difering opinions, or for behaving as an individual.
27. A Digital Identity must not be used on its own or in conjunction with any other system that would intentionally or unintentionally allow the identifcation of a specified class or group of individuals. A Digital Identity must not be allowed to be used to identify a class or group of individuals based on personal information such as age, gender, religion, place of residence, vaccination status, or any other personal criteria.

While Digital Identity may introduce some conveniences and efciciencies, Digital Identity and associated systems could also introduce signifcant privacy and data security risks, or be subject to misuse. I would like to see the criteria and protections discussed in this submission embedded in Australian law to ensure Australians retain choice when it comes to the use of Digital Identity or physical forms of identity.

Once again, thank for the opportunity to make this submission.

