Australia's Digital ID System

Key questions on the Digital ID legislation and Digital ID Rules

Your name	Phil Dawson
Your organisation	AUCloud (Sovereign Cloud Australia Pty Ltd)
Your email	[redacted]

Page # of guide	Question	Your response
14	What other types of Digital ID service should be included in the legislation, either now or in future?	**Digital driving licences and wallets will likely be additional requirements in the short-term. Longer term validation of relationships (guardianship), ownership (property, other assets, etc) could be services that government is able to validate based on digital identity and other related government services.**
14	Does the Minister's rule-making power to include new services over time provide appropriate flexibility to add new types of Digital ID services? If not, why not?	**Yes. But it's unclear how transparent the process of Ministerial decision making will be to the public on this (new type of Digital ID Services) or other elements. For example, if the Minister makes a decision to exempt an entity from storing any of the data in Australia, when and why was the decision made, against what criteria and what information has the beneficiary provided to support the Minister's decision.** **Ministerial decision making process will become especially important as legitimate technology or at least its use seeks to remain ahead of deep fake technology and its potential to undermine Digital-IDs**
16	Is the Regulator's power to impose conditions	**Yes.**

Page # of guide	Question	Your response
	on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the Regulator's power to impose conditions on accreditation be improved?	
16	Is the application for accreditation process appropriate, or should other matters be included or some excluded?	**Digital-ID is fundamental to a safer and more secure digital economy. Digital-ID is a service that can only reliably be provided by Government who have access to longitudinal information that will validate identity. The service is so fundamental to the sovereignty of the nation, that such applications and underlying data must be retained in country as sovereign data sets managed by governments and/or sovereign owned entities accredited under the Hosting Certification Framework but not overseas owned companies how may be Certified Strategic.**
17	Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?	**It is unclear if each instance of non-compliance is subject to the maximum penalty. If not the quantum is likely minimal compared with the amount that companies will spend on legal defence i.e. too low.**
21	Are the additional privacy safeguards sufficiently robust, clear and practical?	**The requirement for express consent is unclear as to the term, duration or purpose that limits the ability to consent to avoid broad based consent terms that users are co-opted into signing. Alignment with future privacy definitions on personal information and consent process will be critical for effective implementation of safeguards.**
21	Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric	**The requirement for express consent is unclear as to the term, duration or purpose that limits the ability to consent to avoid broad based consent terms that users are co-opted into signing. Lack of clear consent relating to specific decisions.**

Page # of guide	Question	Your response
	information?	
21	Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?	**It is unclear if each instance of non-compliance is subject to the maximum penalty. If not the quantum is likely minimal compared with the amount that companies will spend on legal defence i.e. too low.**
23	What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?	**Age verification is currently highly inaccurate and that in fact is one of the core benefits from an accurate national Digital ID solution** **Like all nations, the balance of approval as to what age a young person can effectively and legally consent to something is a balance of national age specific legislations, human rights legislation, national culture and the benefits that could accrue from securing the benefit. Even though the clearly fraudulent nature of many of their accounts, this is the key reasons why main social media companies across Western democracies limit account restrict sign-up to 12/13year olds or older.**
25	What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?	**No comment**
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	**Citizen sentiment (users are non-users) on trust in various factors relating to the use of Digital-ID and the related Relying Services based on performance, privacy characteristics for different services, data security, data sovereignty, etc.**
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	**It will enable stages of trust to be developed and proven before expansion to avoid the risk of negative service delivery and/or break of trust/privacy.**
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?	**Yes.**

Page # of guide	Question	Your response
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	**Definitions of data should be determined and recognition that data also includes metadata, monitoring data, support data, system analytics data. None of these data sets pertaining to any Digital-ID system should be permitted to be transmitted overseas as they create future vectors of cyber security compromise.**
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	**No comment**
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	**No comment**
34	Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?	**Definitions of data should be determined and recognition that data also includes metadata, monitoring data, support data, system analytics data. None of these data sets pertaining to any Digital-ID system should be permitted to be transmitted overseas as they create future vectors of cyber security compromise.** **Additionally, definitions of personal Information (PI) should be aligned to the definitions within the updated Privacy legislation**
34	What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?	**No comment**