June 2024

Clubs Australia

Digital ID Rules, Digital ID Accreditation Rules and Digital ID Accreditation Data Standards

Clubs Australia Submission

Clubs Australia welcomes the opportunity to comment on the Digital ID Rules, Digital ID Accreditation Rules and Digital ID Accreditation Data Standards.

Clubs Australia represents over 5,000 licensed clubs that employ more than 140,000 people. Clubs are not-for-profit, member-owned organisations whose central activity is to provide sporting and recreation infrastructure to their members and the wider community. Clubs also provide facilities such as dining establishments and food offerings that support local communities utilising the club premises.

Clubs Australia notes existing cyber and privacy obligations and laws, such as the *Privacy Act 1988.* It is important that there is a consistent regulatory framework for matters such as cyber security incident reporting and data collection requirements to support an effective Digital ID system.

Recommendations

Clubs Australia recommends:

1. Any requirements for an entity looking to participate in the Digital ID system be streamlined to ensure there is no unnecessary administrate burden.
2. Streamlining relevant reportable requirements for the Digital ID system with existing regulatory requirements, including the *Privacy Act 1988.*
3. Reviewing how entities can comply with the relevant reportable requirement timeframes in this phase of the Digital ID system rollout.
4. Clear guidance be provided on how an entity determines when a matter would be 'reasonably expected to' cause a material effect to the Digital ID system.
5. The Government continue to complete consultation after the conclusion of each phase of the Digital ID, particularly prior to the rollout to the private sector.

Use of Identification in Licensed Clubs

Licensed clubs across Australia have a number of duties and functions under which it is necessary to conduct identity verification. These include:

- Complying with sign-in requirements imposed by state and territory legislation, where clubs must collect and retain certain personal information of all members and visitors.
- Evidencing that the club checked the age of a patron, to ensure the club is complying with requirements to turn away minors.

Clubs Australia Incorporated
ABN 32 691 361 915

Level 8, 51 Druitt Street
Sydney NSW 2000
P 02 9268 3000 F 02 9268 3066

- Holding a register of members, which is a requirement, per se, in most jurisdictions, and also enables clubs to notify members about general meetings like AGMs.
    - Undertaking customer due diligence under the *Anti-Money Laundering and Counter Terrorism Act 2006.*
    - Administering gambling self-exclusion schemes, as required by state and territory laws.

In some states, digital driver licences and identity documents are already in use. For example, in NSW, patrons can use the Service NSW app to sign into a club and evidence their age.

Some clubs also use Facial Recognition Technology (**FRT**) to identify excluded gamblers – in a number of jurisdictions this may be mandated via the regulatory framework or specific conditions imposed on a gaming licence. For instance, most clubs in South Australia are required under legislation to have FRT, and, in Queensland, using FRT is mandated for particular venues as a gaming licence condition and encouraged for other venues by the regulator.

1. Applications for approval of participation for relying parties

As currently drafted in the Digital ID Bill, the application for approval to participate in Digital ID includes a written cyber security plan, digital ID fraud management plan, disaster recovery plan, and business continuity plan. This obligation would be extremely difficult for clubs to comply with and would be a high barrier to entry, particularly for small clubs that are often run by volunteers.

Clubs do not have large, in-house fraud and security teams and many clubs outsource this work to a third-party provider (such as a cybersecurity expert).

Clubs Australia recommends that the Government streamline and simplify these requirements to participate in the Digital ID system. Consideration should also be given to simplifying the application process and requirements for small to medium businesses wishing to use Digital ID. Clubs Australia would welcome the opportunity to work further with the Government on this matter.

Clubs Australia recommends any requirements for an entity looking to participate in the Digital ID system be streamlined to ensure there is no unnecessary administrative burden.

2. Reporting Requirements

There is a requirement under the Digital ID Rules to notify the Digital ID Regulator of reportable incidents related to Digital ID[1]. Clubs Australia recommends that this reporting be streamlined with existing regulatory reporting requirements, such as the Notifiable Data Breaches scheme[2], that an entity must complete when it experiences a cyber security incident and/or data breach.

It is important that when a cyber security or Digital ID fraud incident occurs, a club is able to report this to the relevant government entities as soon as practically possible.

As part of Clubs Australia's submission to the Cyber Security Strategy 2023-2030, Clubs Australia supported non-legislative commitments raised in the Discussion Paper including providing clear cyber guidance for businesses. This will be important to include information on the Digital ID to ensure that clubs have clarity of their reporting requirements.

Clubs Australia recommends that cyber reporting requirements for Digital ID be streamlined with existing regulatory reporting requirements, including the *Privacy Act 1988.*

3. Timeframes for reporting cyber security requirements and Digital ID fraud incidents

The draft Digital ID Rules require an entity to report a cyber security incident and Digital ID fraud incident as soon as practically possible (but no longer than 1 day) or, if notification is given orally, in writing within 3 days.[3] There are also provisions to allow for an entity to provide information about an incident in a later time frame where they do not have the information available about the incident.[4]

In this phase of the Digital ID rollout, the Government should monitor how government entities are able to meet these timeframes to ensure that, if necessary, amendments are made to ensure that entities can meet the reporting timeframe.

Clubs Australia recommends that the Government review how entities can comply with the relevant reportable requirement timeframes in this phase of the Digital ID system rollout.

4. Events that could reasonably be expected to have a material effect on the Digital ID system

[1] Digital ID Rules 2024, Part 4 Section 12
[2] Privacy Act 1988, Part IIIC
[3] Digital ID Rules 2024, Part 5, Section 12 (5)-(6) & Section 13 (5)-(6)
[4] Digital ID Rules 2024, Part 5, Section 12 (7) & Section 13 (7)

The Digital ID Rules state that an entity must have effective written procedures to notify the System Administrator of any proposed changes to its information technology system or any planned or unplanned outage or downtime that will or could reasonably be expected to have a material effect on the operation of the Digital ID[5]. This is also a participation condition for an entity to use the Digital ID system.[6]

Whilst the Digital ID Rules define material effect, Clubs Australia recommends that clear guidance be provided to ensure entities can clearly understand their obligations when an event could be 'reasonably expected to' impact the operation of the Digital ID system. As currently drafted, this requirement is unclear and has the potential to cause significant administrative burdens for entities.

Clubs Australia recommends that clear guidance be provided on how an entity determines when a meter would be 'reasonably expected to' cause a material effect to the Digital ID System.

5. Phased Roll Out of Digital ID

Clubs Australia supports the Government's continued approach to a phased rollout of the Australian Government Digital ID system. It is important that this continues to ensure that the system is fit for purpose and has appropriate safety and privacy mechanisms in place. This will ensure that individuals can trust utilising the Digital ID system.

Clubs Australia recommends that the Government continue to complete consultation after the conclusion of each phase of the Digital ID, particularly prior to the rollout to the private sector.

Concluding Remarks

Clubs Australia appreciates the opportunity to provide a submission on this matter. Should you wish to discuss this matter further, please contact Alison Tehan, Deputy Executive Manager, at [redacted]

[5] Digital ID Rules 2024, Part 3, Section 6 (2)
[6] Digital ID Rules 2024, Part 3, Section