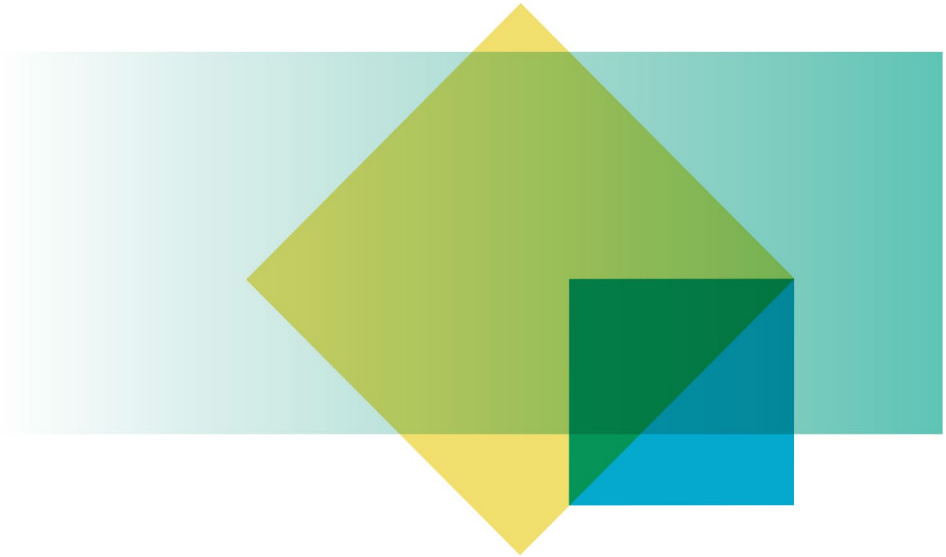
Australian Government

Office of the Australian Information Commissioner

# Digital Identity Legislation Position Paper

## Submission by the Office of the Australian Information Commissioner



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

15 July 2021

OAIC

# Contents

# Introduction

1.1 The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Digital Transformation Agency's (DTA) consultation on the Digital Identity Legislation Position Paper (the position paper).

1.2 The OAIC has engaged with the DTA over several years on the development of the Trusted Digital Identity Framework (TDIF). Most recently, we have participated as a member of the Digital Identity and MyGov Steering Committee, and as an observer on an interdepartmental committee to develop the legislation for the system. The OAIC also made a submission to the DTA's previous consultation paper on the Digital Identity legislation (DI legislation).[1]

1.3 The Digital Identity System (DI system) is a key part of the government's Digital Economy Strategy, aiming to provide 'secure and simple access to services from government and across the economy.'[2] The OAIC welcomes the government's commitment to embed privacy, security and fraud prevention mechanisms into the DI legislation to build trust in the DI system.[3] In addition to the specific privacy requirements in the DI legislation, it is proposed that entities who are accredited to participate in the DI system will be required to comply with the *Privacy Act 1988* (Cth) (Privacy Act) or a comparable state or territory privacy law.[4]

1.4 These privacy safeguards are critical to build trust in this voluntary system. When people have confidence about how their information is managed, they are more likely to support the use of that information to provide the services and value envisaged by Digital Identity and other digital economy initiatives.

1.5 Trust will also be secured through strong regulatory oversight of the DI system. The OAIC supports the proposed regulatory role for the Australian Information Commissioner under the DI legislation. Strong and consistent privacy regulation is critical to safeguard the privacy foundations of the DI system and secure consumer trust and confidence.

1.6 This submission highlights the importance of ensuring that the DI legislation builds on existing privacy protections and regulatory frameworks, to reduce overlap and duplication, create regulatory certainty for entities and ensure consistency of protection for individuals. The submission also makes recommendations about additional measures aimed at ensuring the trust and integrity of the DI system.

---

[1] OAIC, *Digital Identity Legislation Consultation Paper – Submission to the Digital Transformation Agency*, https://www.oaic.gov.au/engage-with-us/submissions/digital-identity-legislation-consultation-paper-submission-to-the-digital-transformation-agency/.

[2] Australian Government, *Digital Economy Strategy 2030* https://digitaleconomy.pmc.gov.au/sites/default/files/2021-05/digital-economy-strategy.pdf, p 2.

[3] Australian Government, *Digital Economy Strategy 2030* https://digitaleconomy.pmc.gov.au/sites/default/files/2021-05/digital-economy-strategy.pdf, p 43.

[4] Digital Transformation Agency, *Digital Identity Legislation Position paper*, https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/digital-identity-legislation-position-paper, p 7.

# Strong and consistent privacy regulation

1.7 The position paper states that the DI legislation will include 'a range of new legislative safeguards to protect the personal information of individuals who choose to use a digital identity.' These safeguards are intended to build on existing laws and not 'duplicate or conflict with established principles in existing legislation, for example, the Privacy Act.'[5] Accredited Participants will also be required to be covered by the Privacy Act as APP entities, or by a comparable state or territory privacy law. It is proposed that the Information Commissioner will oversee the new privacy protections in the DI legislation, and will continue to regulate the handling of personal information by APP entities participating in the DI system.

1.8 The intention of the Digital Identity-specific privacy regime is to leverage the existing Privacy Act framework but provide more specificity in relation to the protections that should apply to Digital Identity information, in light of the special need for trust in a new DI system.

1.9 The OAIC acknowledges that there are policy considerations that will justify separate Commonwealth privacy regimes and stronger privacy protections in certain circumstances. The introduction of additional privacy protections is a recent trend occurring across the domestic data landscape. For example, the Consumer Data Right (CDR) scheme and the My Health Records (MHR) system contain specific enhanced privacy requirements within their legislative frameworks.

1.10 The OAIC performs various regulatory responsibilities under these, and other, regimes. Where privacy protections are included in other legislative regimes, it is critical that the Commissioner has full jurisdiction over enforcing those protections to ensure that privacy regulation is clear, consistent and effective.

1.11 The OAIC therefore recommends that the DI legislation provides the Information Commissioner with comprehensive regulatory functions and powers to effectively oversee the new privacy protections. The OAIC is supportive of the introduction of new civil penalty offences for contraventions of the additional privacy safeguards in the DI legislation. Consistent with the aim of not duplicating established principles in existing legislation, the OAIC recommends that the DI legislation draws on the Information Commissioner's regulatory functions and powers under the Privacy Act to the extent possible, including handling complaints, undertaking investigations and assessments, and enforcement.

1.12 In order to facilitate effective regulation, the OAIC recommends that the Information Commissioner is also empowered to issue infringement notices for breach of the new privacy protections. Infringement notice powers provide a cost-efficient deterrence mechanism, allowing the Information Commissioner to maximise the public benefit with fewer resources.

1.13 Finally, the position paper notes that the digital identity legislative framework will include a Bill passed by Parliament, rules and written guidelines and policies. The OAIC recommends that privacy requirements are embedded in the primary legislation to guard against inadvertent or unforeseen risks to privacy, such as the collection, use or disclosure of personal information that may not have been originally intended, known as 'function creep', or that which may not

[5] Digital Transformation Agency, *Digital Identity Legislation Position paper*, https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/digital-identity-legislation-position-paper, p 44.

be reasonable, necessary and proportionate to the relevant policy objectives. The DI legislation should also include a requirement that entities must have regard to any guidelines issued by the Information Commissioner about the privacy requirements in the legislation.

**Recommendation 1:** The DI legislation should provide the Information Commissioner with comprehensive regulatory functions and powers, drawing on existing regulatory functions and powers under the Privacy Act to the extent possible.

**Recommendation 2:** The Information Commissioner should be empowered to issue infringement notices for breach of the new privacy protections under the DI legislation.

**Recommendation 3:** Privacy requirements should be embedded in the primary legislation, rather than delegated legislation or guidance.

**Recommendation 4:** The DI legislation should include a requirement that entities must have regard to any guidelines issued by the Information Commissioner about the privacy requirements in the legislation.

## Data breach notifications

1.14 Consistency and efficiency in the regulation of data breach notifications is also important. This is required to ensure that individuals and regulated entities have certain and comparable rights and obligations, and that there is a consistent regulatory response in the event of a data breach incident relating to the DI system.

1.15 The position paper notes that Accredited Participants that are APP entities will notify the OAIC and affected individuals of any eligible data breach under the Notifiable Data Breaches (NDB) scheme in the Privacy Act. The DI legislation will require these entities to provide a copy of the notification to the Oversight Authority as well.

1.16 The position paper proposes establishing a new notifiable data breaches scheme under the DI legislation for state and territory government bodies that are Accredited Participants but not subject to the Privacy Act or a comparable data breach notification scheme. This new scheme would draw on the NDB scheme in the Privacy Act. These Accredited Participants will be required to provide a statement about an NDB to the Oversight Authority and the privacy commissioner in the relevant state/territory, and to notify affected individuals in a similar manner to the NDB scheme. The Oversight Authority would be empowered by the DI legislation to take administrative action against an Accredited Participant in response to a notifiable data breach.

1.17 The OAIC is concerned that creating a new data breach notification scheme for personal information under the DI legislation risks inconsistent application of core privacy concepts and fragmentation across mirror schemes. The Information Commissioner has statutory functions under the Privacy Act to make guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, including breach of the NDB scheme in the Privacy Act. Where other entities such as the Oversight Authority have responsibility for an equivalent regime there is a risk of inconsistent interpretation and regulatory response . It also

risks inefficiency by having to duplicate guidance, process, appeal rights, legal expertise and staff capability.

1.18 To ensure consistent and efficient privacy regulation and clarity about rights and responsibilities for individuals and regulated entities, the OAIC recommends that state and territory government bodies that are not subject to a comparable data breach notification scheme should be required to comply with the NDB scheme in the Privacy Act. Alternatively, the OAIC recommends that the Information Commissioner regulate any data breach notification scheme under the DI legislation.

**Recommendation 5:** State and territory government bodies not subject to a comparable NDB scheme should be required to comply with the NDB scheme in the Privacy Act. Alternatively, the Information Commissioner should regulate any data breach notification scheme in the DI legislation.

# Minimising regulatory overlap and facilitating regulatory cooperation

1.19 In addition to the regulatory role of the Information Commissioner under the DI system, the position paper proposes the appointment of an independent Oversight Authority as a statutory officeholder to regulate the non-privacy-related provisions of the legislation. The Oversight Authority would be assisted by staff whose services are made available by an existing Commonwealth agency.

1.20 The position paper also proposes a regulatory role for state and territory privacy commissioners, who would regulate the handling of personal information under the DI system, should a state or territory government entity choose to comply with an existing, comparable state or territory law, rather than the Privacy Act. As noted above, the position paper also proposes that a state or territory privacy commissioner would receive data breach notifications relating to the DI system.

1.21 The OAIC welcomes the commitment in the position paper to ensuring that the DI system is subject to a robust and independent regulatory framework. The OAIC has extensive experience working within similar co-regulatory models and has entered into memorandums of understanding with other regulators to facilitate effective consultation and cooperation.[6] Legislative clarity about regulatory roles and responsibilities and strong regulatory cooperation are vital to the success of these arrangements, to avoid any unnecessary or inadvertent overlap and uncertainty for consumers and industry.

1.22 The OAIC notes that some of the Oversight Authority's proposed functions outlined in the position paper may intersect or overlap with the Information Commissioner's existing and proposed privacy functions, including the accreditation of entities, monitoring and enforcing

[6] For example, the OAIC has entered into a MOUs with the Australian Competition and Consumer Commission in relation to the CDR. All of the OAIC's current MOUs can be found at: https://www.oaic.gov.au/about-us/our-corporate-information/memorandums-of-understanding/mous/.

system rules, issuing notices to require entities to take remedial action to address a breach of their obligations, suspending or terminating entities' participation in the system, assisting with detecting and investigating privacy breaches and coordinating responses to security incidents.

1.23 The OAIC recommends that the DI legislation clearly defines the powers and functions of the Oversight Authority and the Information Commissioner and facilitates appropriate accountability and information sharing between the two regulators .

1.24 The OAIC notes that the Government's decision about the agency best suited to provide staff to the Oversight Authority will impact on these areas of intersection and overlap. Regardless of where the Oversight Authority is situated, it will be important for Oversight Authority staff to have the technical knowledge of the DI system, as well as the necessary experience, skills and capabilities in exercising regulatory functions, including audits and investigations. Experience in regulating or engaging with both the private and the public sectors would also be desirable.

1.25 The OAIC also recommends that the DI legislation supports efficient information sharing between the Information Commissioner and state and territory privacy authorities and promotes clarity for participants and individuals about the appropriate regulator to contact about privacy protections. Effective information sharing mechanisms are vital to address the potential scenario in which an Accredited Participant is being investigated by the Information Commissioner for breach of the privacy requirements in the DI legislation, and by a state or territory privacy authority for breach of a state or territory privacy law.

1.26 Creating effective information sharing mechanisms may require legislative reform beyond the DI legislation. For example, the Information Commissioner's existing secrecy provisions under the *Australian Information Commissioner Act 2010* (Cth) may need to be amended to ensure they allow the OAIC to share information appropriately. Similarly, additional provisions may be required in the Privacy Act, the DI legislation or other relevant legislation to ensure that the Information Commissioner has clear authorisations to share information in appropriate circumstances.

1.27 The OAIC also recommends that the DI legislation includes requirements for the Oversight Authority to consult with the Information Commissioner on issues that intersect with the Commissioner's privacy functions. For example, the DI legislation could include a requirement to consult with the Information Commissioner:

- in relation to any rules, guidelines or policies that relate to privacy or the handling of personal information
- in relation to aspects of the accreditation process relating to privacy, including the privacy impact assessments undertaken by entities seeking accreditation
- where the Oversight Authority proposes to impose administrative sanctions or take other enforcement action for breaches of the DI legislation, accreditation requirements or TDIF rules that relate to privacy.[7]

[7] A number of other legislative regimes require the Information Commissioner to be consulted in relation to privacy issues. For example, under Volume 1 Part IVD Subdivision B of the *Competition and Consumer Act 2010* (Cth), the Minister must consult with the Information Commissioner in relation to the likely effect of designating a sector under the consumer data right on privacy or confidentiality of consumer's information. Also see *Competition and Consumer Act 2010* (Cth) ss 56BQ(c),

1.28 There will also be a need to consult with the Information Commissioner and share information between regulators in relation to the offboarding of participants who are no longer able to meet the requirements of participation in the system due to a privacy incident or other concerns about their ability to meet the privacy requirements of the DI system.

**Recommendation 6**: The DI legislation should clearly define the powers and functions of the Oversight Authority and the Information Commissioner and facilitates accountability and appropriate information sharing between the two regulators.

**Recommendation 7**: The DI legislation should support efficient information sharing between the Information Commissioner and state and territory privacy authorities and promote clarity for participants and individuals about the appropriate regulator to contact about privacy protections.

**Recommendation 8:** The DI legislation should include requirements for the Oversight Authority to consult with the Information Commissioner on issues that intersect with the Commissioner's privacy functions.

## Clarity about the roles and responsibilities of participating entities

1.29 The DI system will involve different entity types accredited to undertake different roles within the DI system. The DI legislation will assign a different status to entities depending on whether they are TDIF-accredited, Accredited Participants, listed on the TDIF list or listed on the Participant Register.

1.30 Given this complexity, it is important that the DI legislation clearly defines the roles and responsibilities of the different types of entities involved in the DI system. In particular, the OAIC recommends that the DI legislation sets out which entity types are responsible for personal information as it flows through the system and assigns clear ownership of risk and liability for the design and security of the system at each stage of the information flow process.

1.31 This clarity is necessary to ensure that there is transparency and accountability in the DI system and individuals' information is protected to the same standard no matter which entity type is handling it.

**Recommendation 9**: The DI legislation should set out which entity types are responsible for personal information as it flows through the system and assign clear ownership of risk and liability for the design and security of the system at each stage of the information flow process.

56DA(4); *Telecommunications (Interception and Access) Act 1979* (Cth) s 183(2); *Telecommunications Act 1997* (Cth) ss 117-119A, 121-122, 134, 295M.

# Choice and alternative channels

1.32 The position paper proposes that creation and use of a digital identity will be voluntary, and that the DI legislation will require a relying party using the DI system to provide an alternative channel to Digital Identity to enable individuals to access its services. The Oversight Authority will be authorised to grant exemptions 'in certain circumstances where it may not be commercially or practically feasible to offer an alternative channel.'[8]

1.33 The position paper notes that these circumstances may include where the relying party is a small business, for example, a business with an annual turnover of less than $3 million, as defined in the Privacy Act. The OAIC notes that this would represent a significant proportion of the businesses currently operating in Australia. As at 30 June 2019, small businesses with a turnover of $3 million or less comprised 95.2% of the 2,375,753 businesses actively trading in the Australian economy.[9]

1.34 The OAIC notes that the voluntary nature of engagement with the DI system allows individuals to engage on the basis of providing consent. The existence of a viable alternative may influence whether consent is freely given. Accordingly the OAIC recommends that the DI legislation narrowly define the scope of permitted exemptions to ensure that the DI system remains truly voluntary and individuals are not compelled to create a digital identity due to the absence of other options.

**Recommendation 10**: The DI legislation should narrowly define the scope of any permitted exemptions to the requirement to provide an alternative channel for identity verification.

# Law enforcement access to Digital Identity information

1.35 The position paper proposes that provisions are included in the DI legislation to limit the ability of law enforcement bodies to access Digital Identity information, however, there are some scenarios in which law enforcement access may be considered appropriate, for example to investigate fraud.

1.36 The OAIC notes that strong community concerns that have been raised around law enforcement access in the context of COVID-19 check-in apps. To ensure that trust in the system is maintained, the OAIC recommends that the DI legislation narrowly and clearly defines any circumstances in which law enforcement bodies would be permitted to access Digital Identity information, and ensures that these situations are reasonable, necessary and proportionate to achieve a legitimate objective.

[8] Digital Transformation Agency, *Digital Identity Legislation Position paper*, https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/digital-identity-legislation-position-paper, p 46.

[9] Australian Bureau of Statistics, 8165.0 Counts of Australian Businesses, including Entries and Exits, Jun 2015 to Jun 2019, prepared for the OAIC in April 2020.

**Recommendation 11**: The DI legislation should narrowly define any circumstances in which law enforcement bodies would be permitted to access Digital Identity information, and ensure that these situations are reasonable, necessary and proportionate to achieve a legitimate objective.