Privacy Commissioner
Te Mana Mātāpono Matatapu

# Digital Identity Regulations Tranche 2

## 1 Introduction

1.1. We welcome the opportunity to submit on tranche 2 of proposed regulations under the Digital Identity Service Trust Framework (DISTF).

1.2. Under the Privacy Act 2020, the functions of the Privacy Commissioner include monitoring emerging privacy issues and offering guidance on how people and organisations can uphold their privacy obligations.

1.3. We have engaged with the development of the DISTF over many years, seeking to enable privacy-preserving sharing of information, to uphold the integrity of the privacy system, and to support good privacy outcomes for New Zealanders. Our submission below addresses proposed assurance standards as the main issue raising significant privacy issues to consider.

## 2 We support the approach to levels of assurance

2.1. We support the approach to assurance standards. We agree it is useful to establish clear and agreed language as discussed on page 8 of the paper. We also support the proposed approach of specifying levels of assurance in regulations, and the proposed 5-stage model presented as Option 1.

2.2. A key goal of the DISTF is privacy-enhancing ways to share personal information. We discuss aspects of this below, and in particular the need to balance enabling data sharing with upholding the principle of data minimisation.

## 3 We support a non-biometric default for assurance

3.1. We support the proposed 5-stage model for assurance, including a “standard” level of assurance which does not require biometric information. This is desirable from a privacy perspective for reasons of:

- **Avoiding overcollection:** use-cases at the “standard” level may not need or justify a biometric-level assurance of identity. A non-biometric option can avoid this overcollection of personal information.

- **Supporting informed choices:** some people may prefer alternatives to biometrics. Having other options at the “standard” level supports that choice.

- **Tikanga Māori:** biometric information such as fingerprints, face scans, or photographs raise specific questions and concerns from a tikanga Māori perspective. A non-biometric "standard" level of assurance may be helpful from this perspective.

- **Addressing overlaps with OPC's Biometric Processing Privacy Code:** some use-cases for the DISTF may involve automated processing of biometric information covered by the Biometric Processing Privacy Code 2025 (BPPC). A non-biometric "standard" level of assurance reduces potential confusion about what counts as "biometrics" in these different contexts and allows DIA and OPC to plan for more targeted communication about DISTF use-cases that are covered by the BPPC.

3.2. Assurance standards in regulations will play a key role in striking a balance between enabling data sharing and upholding data minimisation. On the one hand, it is desirable to make it quick and easy for people to share verified information about themselves where this is necessary for a particular purpose. On the other hand, it is important to avoid situations where people are asked to share personal information just because it is convenient to request it.

3.3. Avoiding over-collection and over-sharing is particularly important for biometric information, which is inherently sensitive and involves heightened security risks.

3.4. Broader issues of biometric privacy have been a focus for public concern and policy work for the past several years. Following a multi-year policy process with multiple phases of public consultation, the Privacy Commissioner recently issued the Biometric Processing Privacy Code 2025 (BPPC). This modifies how the Information Privacy Principles under the Privacy Act 2020 apply to automated processing of biometric information. We think it would be useful in the medium term for OPC and DIA to engage on potential overlaps and interactions between the DISTF and the BPPC. To be clear, use of biometrics under the DISTF does not necessarily fall within the code, but it will be useful to ensure that we can give clear information to people and organisations so they understand what opportunities and obligations apply if they use biometrics.

3.5. We again thank you for the chance to engage, and look forward to doing so in future.