



# Digital Identity Services Trust Framework Act 2023

Public Act 2023 No 13  
Date of assent 5 April 2023  
Commencement see section 2

## Contents

	Page
1 Title	5
2 Commencement	5
<b>Part 1</b>	
<b>Preliminary provisions</b>	
3 Purpose	6
4 Overview of Act	6
5 Interpretation	7
6 Transitional, savings, and related provisions	8
7 Act binds the Crown	8
<b>Part 2</b>	
<b>Digital identity services trust framework</b>	
8 Trust framework	8
9 Tiriti o Waitangi/Treaty of Waitangi	9
10 Meaning of digital identity service	10
11 Trust framework participants	10
12 Requirements for TF providers dealing with personal or organisational information when providing accredited digital identity services	10
13 Accreditation marks	10
<i>Digital identity services outside trust framework</i>	
14 TF providers may provide both accredited services and services not accredited	11
15 Digital identity services outside trust framework	11

	<i>Relationship with other Acts</i>	
16	Relationship with Electronic Identity Verification Act 2012 and Identity Information Confirmation Act 2012	11
17	Application of Privacy Act 2020	11
	<b>Part 3</b>	
	<b>TF rules, accreditation, TF register, and record-keeping and reporting</b>	
	<i>TF rules</i>	
18	TF rules	12
19	Who TF rules apply to	12
20	Content of TF rules	12
21	Consultation required before recommending TF rules	13
22	TF board to report to Minister on consultation	13
	<i>Accreditation</i>	
23	Application for accreditation	14
24	Contents of application	14
25	Specified information	14
26	Decision by TF authority	15
27	Notice of decision	15
28	Regulations for accredited providers and services	16
29	Reconsideration of application	16
30	Duration of accreditation	17
31	Renewal of accreditation	18
32	Provisional accreditation	18
33	Obligation to tell TF authority of changes to key information or specified information	19
	<i>TF register</i>	
34	Register of TF providers and accredited services	20
35	Purposes of register	20
36	Form of register	20
37	Information to be contained in register	20
38	Amendments to register	21
	<i>Third party assessors</i>	
39	Certification of third party assessors	21
40	Accountability and immunity	21
41	Record-keeping and reporting by third party assessors	22
	<i>Record-keeping and reporting by TF providers</i>	
42	Record-keeping and reporting by TF providers	22

**Part 4**  
**TF board**

43	TF board established	22
44	Responsible department	23
	<i>TF board's functions and powers</i>	
45	Functions of TF board	23
46	General powers of TF board	23
	<i>TF board members</i>	
47	Appointment of TF board members	23
48	Voting rights	24
49	Removal of TF board members	24
50	Remuneration of TF board members	24
	<i>Māori Advisory Group</i>	
51	Māori Advisory Group established	24
52	Appointment of members of Māori Advisory Group	25
53	Role of Māori Advisory Group	25
54	Further provisions relating to Māori Advisory Group	26
55	Removal of Māori Advisory Group members	26
	<i>Committees of advisers</i>	
56	Appointment and remuneration of committees of advisers	26
57	Removal of committee members	27

**Part 5**  
**TF authority**

58	TF authority established	27
59	Responsible department	27
	<i>TF authority's functions and powers</i>	
60	Functions of TF authority	27
61	General powers of TF authority	28
62	Power to require information or documents	28
63	Extension of time to provide information	29
	<i>TF authority members</i>	
64	Appointment of TF authority members	29
65	Removal of TF authority members	29
66	Remuneration of TF authority members	29

**Part 6**  
**Complaints and offences**

67	Purpose of Part	30
68	Principles	30

	<i>Complaints</i>	
69	Who may make complaint	30
70	How to make complaint	30
71	How complaints must be dealt with	30
72	Referral of complaints to office holders	31
73	TF authority may decide not to consider complaint further	31
	<i>Preliminary assessment of complaints</i>	
74	Procedure for preliminary assessment of complaints	32
75	Notice of preliminary assessment	33
	<i>Dispute resolution scheme</i>	
76	Dispute resolution scheme	33
77	Ministerial approval of dispute resolution scheme	33
	<i>Investigations by TF authority</i>	
78	Investigation of breach	34
79	Commencing investigation	34
80	Conducting investigation	34
81	TF authority may regulate own procedure	35
82	Finding by TF authority	35
	<i>Remedies</i>	
83	Remedies following finding of breach	35
	<i>Public warnings</i>	
84	Public warnings	36
	<i>Additional record-keeping or reporting requirements</i>	
85	Additional record-keeping or reporting requirements	36
	<i>Compliance orders</i>	
86	Issuing compliance order	36
87	Form of compliance order	37
88	TF provider response to compliance order	37
89	TF provider must tell TF authority when compliance order complied with	38
90	TF provider may elect to forfeit accreditation	38
91	TF authority may vary or cancel compliance order	38
	<i>Suspension or cancellation of accreditation following finding of breach</i>	
92	Suspension of accreditation	38
93	Cancellation of accreditation	39
94	Suspension or cancellation if breach on 3 or more occasions	39
	<i>Suspension or cancellation of accreditation for other reasons</i>	
95	Suspension or cancellation of accreditation	39

<i>Offences</i>		
96	Offence to knowingly or recklessly misrepresent provider to be TF provider or service to be accredited service	40
97	Offence to misuse accreditation mark	41
98	Offence to knowingly or recklessly give false information to TF authority in application for accreditation	41
99	Offence to fail to give key information or specified information in application for accreditation	41
100	Offence to fail to tell TF authority of change to key information or specified information	42
101	Offence to obstruct TF authority	42
<b>Part 7</b>		
<b>Regulations, immunity from civil liability, and reviews</b>		
<i>Regulations</i>		
102	Regulations	42
<i>Immunity from civil liability</i>		
103	Immunity for members and staff of TF board and TF authority, members of Māori Advisory Group, and members of advisory committees who are not public service employees	43
104	Immunity for TF providers for actions of users	43
<i>Reviews</i>		
105	Review of TF board's operation	44
106	Review of complaints process and dispute resolution scheme	44
<b>Schedule</b>		
<b>Transitional, savings, and related provisions</b>		

**The Parliament of New Zealand enacts as follows:**

**1 Title**

This Act is the Digital Identity Services Trust Framework Act 2023.

**2 Commencement**

- (1) This Act comes into force—
  - (a) on 1 or more dates set by Order in Council; or
  - (b) to the extent not brought into force earlier, on 1 July 2024.
- (2) One or more Orders in Council may set different dates for different provisions.
- (3) An Order in Council made under this section is secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

---

<b>Legislation Act 2019 requirements for secondary legislation made under this section</b>		
<b>Publication</b>	PCO must publish it on the legislation website and notify it in the <i>Gazette</i>	LA19 s 69(1)(c)
<b>Presentation</b>	The Minister must present it to the House of Representatives	LA19 s 114
<b>Disallowance</b>	It may be disallowed by the House of Representatives	LA19 ss 115, 116

---

*This note is not part of the Act.*

---

## Part 1

### Preliminary provisions

#### 3 Purpose

The purposes of this Act are—

- (a) to establish a legal framework for the provision of secure and trusted digital identity services for individuals and organisations:
- (b) to establish governance and accreditation functions that are transparent and incorporate te ao Māori approaches to identity.

#### 4 Overview of Act

*Key definitions in Part 2*

- (1) The definition of the digital identity services trust framework is in section 8 along with a description of the main components of the trust framework. The definition of digital identity service is in section 10. The 3 types of trust framework participants are listed in section 11.
- (2) The ways in which the Act recognises and respects the Crown's responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi are listed in section 9.

*Other Parts in Act*

- (3) Part 3 relates to the TF rules, the accreditation of providers of digital identity services and the services they provide, and record-keeping and reporting by them once they are accredited. Part 3 also contains provisions relating to the TF register of accredited providers and services.
- (4) Part 4 relates to the TF board, the Māori Advisory Group, and committees of advisers to advise the board.
- (5) Part 5 relates to the TF authority.
- (6) Part 6 relates to complaints and offences. Part 6 also sets out remedies that may be granted by the TF authority following a finding of breach by a TF provider of the TF rules, regulations, terms of use of accreditation marks, or provisions of this Act.
- (7) Part 7 contains a miscellaneous group of provisions relating to regulations, immunity from liability, and reviews.

*Effect of overview section*

- (8) This overview is for explanation only and does not affect the meaning of this Act.

**5 Interpretation**

In this Act, unless the context otherwise requires,—

**accreditation mark** means an accreditation mark described in section 13

**accredited digital identity service** or **accredited service** means a digital identity service that is accredited by the TF authority to be provided by a particular TF provider (*see also* the definition in section 34(2))

**breach** has the meaning given in section 69(2)

**chief executive** means the chief executive of the relevant responsible department

**department** means a public service agency within the meaning given in section 10(a) of the Public Service Act 2020

**digital identity service** has the meaning given in section 10

**digital identity service provider** means an individual or organisation that provides a digital identity service, whether the provider or service is accredited under this Act or not

**digital identity services trust framework** or **trust framework** has the meaning given in section 8

**individual** means a natural person

**Minister** means the Minister of the Crown who, under the authority of any warrant or with the authority of the Prime Minister, is responsible for the administration of this Act

**organisation** means any organisation, whether public or private, and whether incorporated or not

**organisational information** means information relating to a particular organisation

**participants** has the meaning given in section 11

**personal information** has the meaning given in section 7(1) of the Privacy Act 2020

**personal or organisational information** means—

- (a) information that describes the identity of an individual or organisation:
- (b) other information about that individual or organisation

**public service employee** means an employee within the meaning given in section 65 of the Public Service Act 2020

**regulations** means regulations made under section 102

**relying party** means an individual or an organisation that relies on personal or organisational information shared, in a transaction with a user, through 1 or more accredited digital identity services

**responsible department** means the department nominated under section 44 or 59 that is, respectively,—

- (a) the department that the TF board sits within:
- (b) the department that the TF authority sits within

**TF authority** or **authority** means the authority established under section 58

**TF board** or **board** means the board established under section 43

**TF provider** means a digital identity service provider that is accredited by the TF authority to provide 1 or more accredited digital identity services (*see also* the definitions in sections 34(2), 95(6), and 104(3))

**TF register** or **register** means the register of TF providers and accredited services established under section 34

**TF rules** are the rules made under section 18

**transaction** means a transaction whether online or otherwise

**user** means an individual who—

- (a) shares personal or organisational information, in a transaction with a relying party, through 1 or more accredited digital identity services; and
- (b) does so for themselves or on behalf of another individual or an organisation.

## 6 Transitional, savings, and related provisions

The transitional, savings, and related provisions (if any) set out in the Schedule have effect according to their terms.

## 7 Act binds the Crown

This Act binds the Crown.

# Part 2

## Digital identity services trust framework

### 8 Trust framework

- (1) The **digital identity services trust framework** or **trust framework** means the legal framework established by this Act to regulate the provision of digital identity services for transactions between individuals and organisations.
- (2) The main components of the trust framework are—
  - (a) 2 administering bodies:



- (b) an accreditation regime for digital identity service providers and the digital identity services they provide:
  - (c) rules and regulations that include requirements for accredited providers when providing accredited services:
  - (d) approved accreditation marks to identify accredited services.
- (3) The 2 administering bodies for the trust framework are the TF board (*see* Part 4) and the TF authority (*see* Part 5).
  - (4) The accreditation regime is run by the authority (*see* sections 23 to 33).
  - (5) The board recommends draft TF rules and regulations to the Minister (*see* sections 18 and 102), and the authority is responsible for enforcing the rules (*see* Part 6).

## 9 Tiriti o Waitangi/Treaty of Waitangi

In order to recognise and respect the Crown's responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi, this Act,—

- (a) in section 21(1)(b), requires the TF board to consult and invite submissions from tikanga experts who have knowledge of te ao Māori approaches to identity before it can recommend draft TF rules to the Minister:
- (b) in section 45(3), requires the TF board, when performing its functions, to engage with Māori in the manner provided for under section 53(5) to recognise and provide for Māori interests in the operation of the trust framework:
- (c) in section 47(2)(a) and (b), requires the chief executive to ensure that members of the TF board include people who have—
  - (i) expert knowledge of te ao Māori approaches to identity; and
  - (ii) expert knowledge of the principles of te Tiriti o Waitangi/the Treaty of Waitangi; and
  - (iii) experience in engaging with Māori:
- (d) in sections 51 to 55, establishes a Māori Advisory Group to advise the TF board on Māori interests and knowledge, as they relate to the operation of the trust framework:
- (e) in section 53(5), requires the engagement policy between the TF board and the Māori Advisory Group to include details of how and when consultation with iwi and hapū will be undertaken by both the Māori Advisory Group and the board:
- (f) in section 68(a), requires the TF authority, when carrying out its functions under Part 6 (relating to complaints and offences), to be guided by the principle that processes for complaints should be fair and accessible and have particular regard to tikanga Māori:

- (g) in section 105(3)(c), requires a review of the TF board's operation to include an assessment of how other models might better provide opportunities for Māori engagement in the trust framework.

## 10 Meaning of digital identity service

- (1) In this Act, **digital identity service** means a service or product that, either alone or together with 1 or more other digital identity services, enables a user to share personal or organisational information in digital form.
- (2) Examples of digital identity services are services or products that—
  - (a) check the accuracy of personal or organisational information:
  - (b) check the connection of personal or organisational information to a particular individual or organisation:
  - (c) provide secure sharing of personal or organisational information between trust framework participants.
- (3) The regulations must prescribe the types of digital identity services that may be accredited under this Act.

## 11 Trust framework participants

- (1) The **participants** in the trust framework are—
  - (a) users:
  - (b) TF providers:
  - (c) relying parties.
- (2) A single individual or organisation may be 1 or more of the participants listed in subsection (1) in the same transaction.

## 12 Requirements for TF providers dealing with personal or organisational information when providing accredited digital identity services

- (1) A TF provider must not collect, use, share, or otherwise deal with personal or organisational information in connection with the provision of an accredited digital identity service unless—
  - (a) they have reasonable grounds to believe that the collection, use, sharing, or other dealing with the information is authorised by the individual or organisation to which the information relates; and
  - (b) they do so in accordance with the TF rules and the regulations.
- (2) *See* section 17, which provides that nothing in this Act overrides the Privacy Act 2020.

## 13 Accreditation marks

- (1) TF providers may use accreditation marks approved by the TF board to identify the accredited services they provide as being accredited under this Act.

- (2) The board may approve the form and style of accreditation marks and may approve different accreditation marks to be used for different types of services.
- (3) The TF authority must set the terms of use of accreditation marks and must publish them on an Internet site maintained by or on behalf of the authority's responsible department.
- (4) TF providers must comply with the relevant terms of use when using an accreditation mark.

*Digital identity services outside trust framework*

**14 TF providers may provide both accredited services and services not accredited**

- (1) A TF provider may provide both accredited services and digital identity services that are not accredited under this Act.
- (2) *See* section 96, which makes it an offence for a person to knowingly or recklessly represent a digital identity service to be an accredited service when it is not.

**15 Digital identity services outside trust framework**

- (1) An individual or organisation may provide a digital identity service even if they and the service are not accredited under this Act.
- (2) *See* section 96, which makes it an offence for a person to knowingly or recklessly represent—
  - (a) themselves to be a TF provider when they are not:
  - (b) a digital identity service to be an accredited service when it is not.

*Relationship with other Acts*

**16 Relationship with Electronic Identity Verification Act 2012 and Identity Information Confirmation Act 2012**

Nothing in this Act limits or otherwise affects the Electronic Identity Verification Act 2012 or the Identity Information Confirmation Act 2012.

**17 Application of Privacy Act 2020**

Nothing in this Act overrides the Privacy Act 2020.

## Part 3

### TF rules, accreditation, TF register, and record-keeping and reporting

#### *TF rules*

#### 18 TF rules

- (1) The Minister may make rules for the matters listed in section 20.
- (2) The TF board may recommend draft TF rules to the Minister.
- (3) The Minister may make rules only if satisfied that the requirements for consultation under section 21 have been met.
- (4) Rules made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

---

#### Legislation Act 2019 requirements for secondary legislation made under this section

<b>Publication</b>	The maker must publish it in accordance with the Legislation (Publication) Regulations 2021	LA19 s 74(1)(aa)
<b>Presentation</b>	The Minister must present it to the House of Representatives	LA19 s 114
<b>Disallowance</b>	It may be disallowed by the House of Representatives	LA19 ss 115, 116

*This note is not part of the Act.*

---

#### 19 Who TF rules apply to

- (1) The TF rules apply to TF providers and the accredited services they provide.
- (2) The rules—
  - (a) may apply to TF providers only to the extent relevant to their provision of accredited services:
  - (b) must not apply to digital identity services that are not accredited services.

#### 20 Content of TF rules

- (1) The TF rules must set requirements for all of the following:

##### *Identification management*

- (a) determining the accuracy of information, binding that information to the correct individual or organisation, and enabling the secure reuse of the information:

##### *Privacy and confidentiality*

- (b) maintaining the privacy and confidentiality of the information of individuals and organisations:

##### *Security and risk*

- (c) ensuring that information is secure and protected from unauthorised modification, use, or loss:

*Information and data management*

- (d) record-keeping and format of personal and organisational information, to ensure a common understanding of what is shared:

*Sharing and facilitation*

- (e) the sharing of information with relying parties, including authorisation processes.
- (2) The TF rules may set different requirements for the following:
    - (a) different types of TF providers:
    - (b) TF providers and accredited services:
    - (c) different types of accredited services:
    - (d) different levels of assurance for different types of accredited services.
  - (3) If a TF rule is inconsistent with the regulations, the regulations prevail.
  - (4) TF rules relating to personal information must be consistent with the Privacy Act 2020 (*see also* section 17).

**21 Consultation required before recommending TF rules**

- (1) Before recommending draft TF rules to the Minister, the TF board must consult and invite submissions from the following on the proposed content of the rules:
  - (a) the Office of the Privacy Commissioner; and
  - (b) tikanga experts who have knowledge of te ao Māori approaches to identity; and
  - (c) TF providers; and
  - (d) people or groups that are likely to have an interest in the TF rules; and
  - (e) any other individual or organisation that the board considers should be consulted.
- (2) The Minister must decide which people or groups the board must consult under subsection (1)(b) after taking into account the particular subject matter of the proposed content of rules.
- (3) The Minister must also consult the Ministers with portfolio responsibilities that relate to Māori development and Māori-Crown relations before deciding which people or groups will be consulted by the board under subsection (1)(b).
- (4) The Minister may decide that consultation under this section is not required if the proposed content of a rule or a proposed change to an existing rule is technical and non-controversial in nature.

**22 TF board to report to Minister on consultation**

Before recommending draft TF rules to the Minister, the TF board must report to the Minister on the consultation it has undertaken under section 21.

### *Accreditation*

#### **23 Application for accreditation**

- (1) A digital identity service provider may apply to the TF authority to be accredited as a TF provider. That application must be accompanied by an application to have at least 1 digital identity service that they currently provide accredited as an accredited service.
- (2) A TF provider may apply at any time to have a digital identity service that is provided by them, and that is not an accredited service, accredited as an accredited service. That service must be in addition to the 1 or more accredited services they already provide.
- (3) *See* section 32 for applications for provisional accreditation of providers and services.

#### **24 Contents of application**

- (1) An application for accreditation must—
  - (a) be in the form, and be made in the manner, approved by the TF authority; and
  - (b) contain—
    - (i) key information prescribed by the regulations; and
    - (ii) other information required by the regulations (if any); and
  - (c) contain the specified information listed in section 25(1); and
  - (d) be accompanied by the fee prescribed by the regulations (if any).
- (2) *See* section 99, which makes it an offence to fail to give key information or specified information in an application for accreditation.
- (3) The key information referred to in subsection (1)(b)(i) and the other information referred to in subsection (1)(b)(ii) may differ for—
  - (a) different types of applications;
  - (b) different types of digital identity service providers;
  - (c) TF providers and providers that are not accredited under this Act;
  - (d) providers and services;
  - (e) different types of services;
  - (f) different levels of assurance for different types of services.
- (4) The fee referred to in subsection (1)(d) may vary in amount to reflect the different costs of processing different types of applications.

#### **25 Specified information**

- (1) The specified information referred to in section 24(1)(c) is whether the applicant (whether already a TF provider or not)—

- (a) has been convicted of a criminal offence, whether in New Zealand or overseas:
  - (b) is being or has been the subject of a formal investigation or proceeding by or taken by the Privacy Commissioner:
  - (c) has previously—
    - (i) had an application for accreditation for themselves or a service they provided declined:
    - (ii) had their accreditation as a TF provider or of a service they provided suspended or cancelled:
    - (iii) not complied with additional record-keeping or reporting requirements or a compliance order imposed or issued under section 83.
- (2) In this section, **applicant** means the applicant and (as relevant) their officers and those involved in the management of, employed by, or contracted by, the applicant.

## 26 Decision by TF authority

- (1) The TF authority may accredit a provider or service if it is satisfied that—
- (a) the application meets the requirements of sections 23 to 25; and
  - (b) the application, provider, or service meets any criteria for the assessment of applications, or any other requirements, set by the regulations.
- (2) The authority may grant the application in full or in part. However,—
- (a) a provider may be accredited only if they will provide at least 1 accredited service:
  - (b) a service may be accredited only if it will be provided by a TF provider.
- (3) An application that meets the requirements of this section may be declined only if the authority is satisfied that the provider’s past conduct, or that of a related individual or organisation, indicates that the provider or a service they provide may pose a risk to—
- (a) the security, privacy, confidentiality, or safety of the information of any trust framework participants:
  - (b) the integrity or reputation of the trust framework.
- (4) For the purposes of this section, the authority may take into account information that it reasonably believes is likely to be accurate.

## 27 Notice of decision

- (1) The TF authority must give notice of its decision to the applicant and if it declines the application (whether in full or in part), the authority must also—
- (a) set out its reasons for declining the application or part of it; and

- (b) tell the applicant of the right under section 29 to request a reconsideration of the application, if it was declined in full, or of the part that was declined.
- (2) If an application is successful in full or in part, the authority must give the applicant the following information along with its decision:
  - (a) the terms of use of the relevant accreditation mark or accreditation marks; and
  - (b) the expiry date that applies to the accreditation of the provider or service; and
  - (c) any requirements set by regulations under section 28.

## **28 Regulations for accredited providers and services**

- (1) Regulations may prescribe—
  - (a) requirements for—
    - (i) periodic self-assessment by TF providers to check their compliance with the TF rules;
    - (ii) periodic reporting by TF providers about their compliance with the TF rules;
    - (iii) complaints processes and dispute resolution processes that must be operated by TF providers;
  - (b) requirements for other matters related to the operations of TF providers and the accredited services they provide as the TF board and the Minister think fit;
  - (c) fees for recovering the costs of operating the trust framework.
- (2) Regulations referred to in subsection (1) may set different requirements or fees for the following:
  - (a) different types of TF providers;
  - (b) in relation to fees, different types of TF providers to reflect the different costs associated with administering the different types;
  - (c) TF providers and accredited services;
  - (d) different types of accredited services;
  - (e) different levels of assurance for different types of accredited services.

## **29 Reconsideration of application**

- (1) An applicant may apply to the TF authority for it to reconsider—
  - (a) an application for accreditation that it declined;
  - (b) the part of an application that it declined.
- (2) The application for reconsideration must—



- (a) be in the form, and be made in the manner, approved by the authority; and
  - (b) be made within 20 working days after receipt of the notice of the decision.
- (3) When assessing the application, the authority must consider any new, or additional, relevant information provided by the applicant.
- (4) A reconsideration decision by the authority is final. However, this section does not affect the right of an applicant to apply to a court for judicial review of the decision.
- (5) Except to the extent that this Act or the regulations set different requirements for applications for reconsideration, sections 23 to 25 apply to the making of an application under this section as if it were an original application for accreditation.

### **30 Duration of accreditation**

- (1) The accreditation of a TF provider or an accredited service commences on the date of the relevant accreditation decision by the TF authority and ends on the earliest of the following:
- (a) the date the TF provider tells the authority is the date on which they no longer wish—
    - (i) to remain accredited as a TF provider; or
    - (ii) for the service to continue as an accredited service;
  - (b) the date on which the accreditation of the provider or service is cancelled under section 83 or 90;
  - (c) the applicable expiry date;
  - (d) the date on which the accreditation of the service ceases under subsection (3);
  - (e) the date on which the accreditation of the provider ends under subsection (4).
- (2) Under subsection (1)(c), the accreditation of a provider or service expires at the end of the relevant period set by the regulations. The regulations may set different periods for—
- (a) different types of TF providers;
  - (b) TF providers and accredited services;
  - (c) different types of accredited services;
  - (d) different levels of assurance for different types of accredited services.
- (3) If the accreditation of a TF provider ends under subsection (1), all accredited services provided by that provider cease to be accredited services.

- (4) If a TF provider does not provide at least 1 accredited service in a 12-month period or a longer period agreed by the authority (the **applicable period**), their accreditation as a TF provider ends unless subsection (5) applies.
- (5) If a TF provider applies for or obtains provisional accreditation for a digital identity service in the applicable period, their accreditation continues,—
  - (a) in the case of a TF provider that has applied for provisional accreditation for a service, until the application is refused or, if provisional accreditation is granted, for the duration of that provisional accreditation;
  - (b) in the case of a TF provider that has obtained provisional accreditation for a service, for the duration of that provisional accreditation.

### **31 Renewal of accreditation**

- (1) A TF provider may apply to renew their accreditation or the accreditation of an accredited service they provide.
- (2) If a renewal application is made before the accreditation of the provider or service expires, the accreditation continues to have effect until the renewal application is decided by the TF authority.
- (3) If the accreditation of a provider or service expires before a renewal application is made, instead of a renewal application, the provider must make a fresh application for accreditation under section 23.
- (4) A renewal application must be in the form, and be made in the manner, approved by the authority.
- (5) Except to the extent that this Act or the regulations set different requirements for renewal applications, sections 23 to 25 apply to the making of a renewal application as if it were an original application for accreditation.

### **32 Provisional accreditation**

- (1) The TF authority may grant provisional accreditation to a digital identity service provider or to a digital identity service.
- (2) A digital identity service provider that is not a TF provider may apply to the authority—
  - (a) for provisional accreditation as a TF provider; and
  - (b) for provisional accreditation for a service they wish to develop.
- (3) An application under subsection (2) must be for provisional accreditation for both the provider and at least 1 service they wish to develop.
- (4) A TF provider may apply to the authority for provisional accreditation for a service they wish to develop in addition to the 1 or more accredited services they already provide.
- (5) An application under this section must be in the form, and be made in the manner, approved by the authority.

- (6) Except to the extent that this Act or the regulations set different requirements for applications for provisional accreditation, sections 23 to 29 apply to the making and deciding of an application under this section with any necessary modifications.
- (7) Provisional accreditation expires—
  - (a) at the end of the 12-month period that begins on the date the provisional accreditation is granted or a longer period agreed by the authority; or
  - (b) on the date that accreditation is granted for the provider or service under section 26.
- (8) A provider or service with provisional accreditation is not a TF provider or an accredited service for the purposes of this Act.

### **33 Obligation to tell TF authority of changes to key information or specified information**

- (1) If any of the key information referred to in section 24(1)(b)(i), or the specified information listed in section 25(1), changes, the applicant or TF provider must tell the TF authority of the change within 5 working days of the change.
- (2) *See* section 100, which makes it an offence to fail to tell the authority of a change to key information or specified information.
- (3) The obligations under subsection (1) apply,—
  - (a) for an applicant (whether already a TF provider or not), after an application for accreditation has been made and until it is decided by the authority:
  - (b) for a TF provider, following the accreditation of themselves or a service they provide, from the date of the authority's decision and for the period during which they or the service remains accredited.
- (4) The obligations under this section apply even if an applicant or a TF provider has previously failed to give key information or specified information to the authority as required by sections 24 and 25.
- (5) In this section, **application for accreditation** means—
  - (a) an application for accreditation under section 23:
  - (b) an application for reconsideration under section 29:
  - (c) an application for renewal of accreditation under section 31:
  - (d) an application for provisional accreditation under section 32:
  - (e) any communication with the authority relating to an application in paragraphs (a) to (d), whenever the communication is made.

*TF register***34 Register of TF providers and accredited services**

(1) The TF authority must establish and maintain a register of TF providers and accredited digital identity services.

(2) In this section and sections 35 to 38,—

**accredited digital identity service** and **accredited service** include a digital identity service for which accreditation is suspended

**TF provider** includes an individual or organisation whose accreditation as a TF provider is suspended.

**35 Purposes of register**

The purposes of the TF register are—

(a) to enable the public to—

(i) determine whether an individual or organisation has been accredited as a TF provider and, if so, the status and history of that accreditation (for example, whether it is current or suspended or has lapsed or been cancelled); and

(ii) determine which of a TF provider's digital identity services have been accredited under this Act and the status and history of those accreditations; and

(iii) choose a suitable TF provider from the list of TF providers; and

(b) to facilitate the administrative, disciplinary, and other functions of the TF authority under this Act.

**36 Form of register**

The TF register must be kept as an electronic register on a publicly accessible Internet site maintained by or on behalf of the TF authority or its responsible department.

**37 Information to be contained in register**

(1) The TF register must contain the following information for each TF provider:

(a) the TF provider's full name:

(b) a unique identifier issued by the TF authority (for example, a registration number):

(c) information about the status and history of the TF provider's accreditation as a TF provider, including—

(i) the date on which they became accredited; and

(ii) if the accreditation is for a fixed period, the date on which it will expire if not renewed; and

- (iii) whether the accreditation is currently suspended and, if it is, the period of the suspension.
- (2) For each TF provider, the register must also—
  - (a) identify the digital identity services provided by the TF provider that are accredited services; and
  - (b) include information about the status and history of the accreditation of each of those digital identity services, including—
    - (i) the date on which the service became accredited; and
    - (ii) if the accreditation is for a fixed period, the date on which it will expire if not renewed; and
    - (iii) whether the accreditation is currently suspended, and, if it is, the period of the suspension.
- (3) The register may also contain—
  - (a) information about former TF providers and former accredited digital identity services, including information about when their accreditation ended; and
  - (b) any other information that the TF authority considers necessary or desirable for the purposes of the register.

### **38 Amendments to register**

The TF authority may make amendments to the TF register at any time for the purposes set out in section 35, including amendments to—

- (a) keep the register up to date by reflecting any changes in the information contained in it;
- (b) correct an error or omission on the part of the authority or anyone establishing or maintaining the register on the authority's behalf.

#### *Third party assessors*

### **39 Certification of third party assessors**

- (1) The TF authority may certify an individual or an organisation as a third party assessor to carry out 1 or more of its functions relating to accreditation of providers or services if permitted by, and in accordance with, the regulations.
- (2) A third party assessor does not have, and nor may the authority delegate to them, the authority's powers under sections 61 and 62 of this Act.
- (3) The regulations may prescribe circumstances under which the authority may suspend or cancel the certification of third party assessors.

### **40 Accountability and immunity**

- (1) This section applies to a third party assessor when intending to carry out or carrying out functions under this Act.

*Accountability*

- (2) The Ombudsmen Act 1975 and the Official Information Act 1982 apply to them as if the third party assessor were an organisation named in Schedule 1 of the Ombudsmen Act 1975.
- (3) Information they hold is to be treated as also being held by the TF authority for the purposes of the Official Information Act 1982.

*Immunity*

- (4) Section 104 of the Public Service Act 2020 applies to them as if they were a public service employee.

Compare: 1989 No 24 s 7G; 2020 No 40 Schedule 6 cl 3(2)

**41 Record-keeping and reporting by third party assessors**

The regulations may prescribe record-keeping and reporting requirements for third party assessors, including for the collection and keeping of certain information, and for providing information to the TF authority.

*Record-keeping and reporting by TF providers***42 Record-keeping and reporting by TF providers**

- (1) A TF provider must—
  - (a) collect the required information about its activities; and
  - (b) keep that information in the required manner and for the required period; and
  - (c) give that information to the TF authority—
    - (i) periodically as required;
    - (ii) at all reasonable times on request.
- (2) In this section,—

**give**, in relation to information, includes—

  - (a) give access to the information, including by permitting its inspection; and
  - (b) permit copies of the information to be made

**required** means required by the regulations.

## **Part 4**

### **TF board**

**43 TF board established**

The Trust Framework Board is established to carry out the board's functions set out in this Act.

**44 Responsible department**

- (1) The Prime Minister must nominate a department to be the responsible department for the TF board.
- (2) The board is a body within the responsible department and is accountable to its chief executive.
- (3) The responsible department must include in its annual report a description of the board's activities for the period covered by the report.

Compare: 2007 No 15 s 34(1)

*TF board's functions and powers***45 Functions of TF board**

- (1) The TF board's functions are to—
  - (a) recommend draft TF rules to the Minister, review the rules at reasonable intervals, and recommend updates to them:
  - (b) recommend regulations to the Minister:
  - (c) undertake education and publish guidance for TF providers and the public:
  - (d) monitor the effectiveness of the trust framework:
  - (e) carry out other functions conferred on the board by this Act or by the Minister to achieve the purposes of this Act:
  - (f) carry out any functions that are incidental and related to, or consequential on, the functions referred to in paragraphs (a) to (e).
- (2) If any functions are conferred on the board by the Minister, this must be done in writing.
- (3) When performing its functions, the board must engage with Māori in the manner provided for under section 53(5) to recognise and provide for Māori interests in the operation of the trust framework.

**46 General powers of TF board**

The TF board has all the powers that are reasonably necessary to carry out its functions under this Act to the extent consistent with section 44(2).

*TF board members***47 Appointment of TF board members**

- (1) The chief executive must appoint the members of the TF board. The members may include public service employees and individuals from outside the public service.
- (2) When selecting the board's members, the chief executive must ensure that—

- (a) members of the board include people who have expert knowledge of te ao Māori approaches to identity; and
- (b) members of the board include people who have—
  - (i) expert knowledge of the principles of te Tiriti o Waitangi/the Treaty of Waitangi; and
  - (ii) experience in engaging with Māori; and
- (c) the members of the board collectively possess sufficient knowledge and expertise in working with technology and identity data management, including with—
  - (i) the ethical use of digital information; and
  - (ii) protecting the privacy and confidentiality of digital information; and
  - (iii) the secure handling of digital information; and
- (d) the board has sufficient members to carry out its functions in a timely and efficient manner.

#### **48 Voting rights**

Only members of the TF board who are public service employees have voting rights on the board.

#### **49 Removal of TF board members**

The chief executive may give written notice to a TF board member removing them from the board if they become bankrupt or neglect their duty, or for misconduct.

#### **50 Remuneration of TF board members**

- (1) A TF board member who is a public service employee is entitled to be paid by their employer, as if they were undertaking their usual duties, for time reasonably taken by them away from their usual duties to undertake the work of the board.
- (2) Other board members are not public service employees as a result of their appointment to the board, and the responsible department must pay fees for their services, and expenses reasonably incurred by them in providing those services, in accordance with the fees framework.

#### *Māori Advisory Group*

#### **51 Māori Advisory Group established**

The Māori Advisory Group is established to advise the TF board.

Compare: 2020 No 52 s 14



**52 Appointment of members of Māori Advisory Group**

- (1) The Minister must appoint members to the Māori Advisory Group.
- (2) The Minister must consult the Ministers with portfolio responsibilities that relate to Māori development and Māori-Crown relations before making any appointments.
- (3) The Minister must appoint 1 of the members as chairperson of the Māori Advisory Group.
- (4) The Minister must appoint only people who, in the responsible Minister's opinion, have the appropriate knowledge, skills, and experience to assist the Māori Advisory Group to perform its role.

Compare: 2020 No 52 s 15

**53 Role of Māori Advisory Group**

- (1) The role of the Māori Advisory Group is to advise the TF board on Māori interests and knowledge, as they relate to the operation of the trust framework, and to do so in accordance with the engagement policy and terms of reference referred to in subsection (4).
- (2) The board must seek advice from the Māori Advisory Group if a matter the board is dealing with raises matters of tikanga Māori or Māori cultural perspectives.
- (3) The board must give effect to the advice of the Māori Advisory Group to the extent that it considers is reasonable and practicable after taking account of other relevant considerations.
- (4) The board and the Māori Advisory Group, acting jointly, must—
  - (a) prepare an engagement policy, setting out how they will work together; and
  - (b) prepare and agree the terms of reference for the Māori Advisory Group.
- (5) The engagement policy must include details of how and when consultation with iwi and hapū will be undertaken by—
  - (a) the board;
  - (b) the board together with the Māori Advisory Group;
  - (c) the Māori Advisory Group to inform its advice to the board.
- (6) The board must publish on an Internet site maintained by or on behalf of the board's responsible department—
  - (a) the engagement policy and the terms of reference for the Māori Advisory Group; and
  - (b) all written advice from the Māori Advisory Group to the board, with redactions if needed, to—
    - (i) protect the privacy of individuals:

- (ii) maintain legal professional privilege:
  - (iii) protect commercially sensitive information.
- (7) The board and the Māori Advisory Group, acting jointly, must review both the engagement policy and the terms of reference at intervals of not more than 3 years.

Compare: 2020 No 52 s 17

#### **54 Further provisions relating to Māori Advisory Group**

- (1) The following provisions of the Crown Entities Act 2004 apply to members of the Māori Advisory Group as if they were members of the board of a Crown agent:
- (a) section 28 (method of appointment of members):
  - (b) section 30 (qualifications of members):
  - (c) section 31 (requirements before appointment):
  - (d) section 32 (term of office of members):
  - (e) section 35 (validity of appointments):
  - (f) section 43 (no compensation for loss of office):
  - (g) section 44 (resignation of members):
  - (h) section 45 (members ceasing to hold office).
- (2) The members are entitled to fees for their services, and expenses reasonably incurred by them in providing those services, in accordance with the fees framework.

Compare: 2020 No 52 s 16

#### **55 Removal of Māori Advisory Group members**

The Minister may give written notice to a member of the Māori Advisory Group removing them as a member if they become bankrupt or neglect their duty, or for misconduct.

#### *Committees of advisers*

#### **56 Appointment and remuneration of committees of advisers**

- (1) The TF board may establish committees of advisers of public service employees and individuals from outside the public service to give advice and make reports to the board.
- (2) An adviser who is a public service employee is entitled to be paid by their employer, as if they were undertaking their usual duties, for time reasonably taken by them away from their usual duties to undertake the work of a committee.
- (3) Other advisers are not public service employees as a result of their appointment to a committee, and the board's responsible department must pay fees for their

services, and expenses reasonably incurred by them in providing those services, in accordance with the fees framework.

**57 Removal of committee members**

The TF board may give written notice to a committee member removing them from a committee if they become bankrupt or neglect their duty, or for misconduct.

## **Part 5**

### **TF authority**

**58 TF authority established**

The Trust Framework Authority is established to carry out the authority's functions set out in this Act.

**59 Responsible department**

- (1) The Prime Minister must nominate a department to be the responsible department for the TF authority.
- (2) That department may be the same as the responsible department nominated for the TF board under section 44.
- (3) The authority is a body within the responsible department and is accountable to its chief executive. However, the authority must act independently in respect of its enforcement functions under Part 6.
- (4) The responsible department must include in its annual report a description of the authority's activities for the period covered by the report.

Compare: 2007 No 15 s 34(1)

#### *TF authority's functions and powers*

**60 Functions of TF authority**

The TF authority's functions are to—

- (a) establish, administer, and maintain an accreditation regime for digital identity service providers and digital identity services:
- (b) establish, administer, and maintain a register of TF providers and accredited services:
- (c) monitor the performance and effectiveness of the accreditation regime:
- (d) operate procedures and tests for TF providers to demonstrate their compliance with the TF rules and the regulations:
- (e) undertake compliance monitoring of TF providers:
- (f) receive and assess complaints:

- (g) investigate breaches of the TF rules, the regulations, the terms of use of accreditation marks, and this Act:
- (h) carry out other functions conferred on the authority by this Act:
- (i) carry out any functions that are incidental and related to, or consequential on, the functions referred to in paragraphs (a) to (h).

## **61 General powers of TF authority**

The TF authority has all the powers that are reasonably necessary to carry out its functions under this Act to the extent consistent with section 59(3).

## **62 Power to require information or documents**

- (1) The TF authority may, by written notice and without charge, require an individual or organisation to provide to it information or a document in their possession or control if satisfied that the information or document is necessary for, and relevant to, 1 or more of the purposes listed in subsection (3).
- (2) The notice may set a date by which the information or document must be provided to the authority. This must not be sooner than 5 working days after receipt of the notice by the individual or organisation.
- (3) The purposes for which the authority may issue a notice are—
  - (a) assessing or investigating a complaint under Part 6:
  - (b) investigating compliance with the TF rules, the regulations, the terms of use of accreditation marks, or this Act:
  - (c) assessing whether additional record-keeping or reporting requirements imposed under section 83 should be lifted:
  - (d) assessing compliance with a compliance order issued under section 83:
  - (e) assessing whether a suspension of accreditation should be lifted.
- (4) The individual or organisation that receives a notice must comply with it within the period stated in the notice.
- (5) However, an individual or organisation that receives a notice need not comply with it in relation to any information or document if—
  - (a) it would be privileged in a court:
  - (b) another Act deals specifically with access to the information or document:
  - (c) disclosure would breach an obligation of secrecy or non-disclosure imposed by an enactment (other than the Privacy Act 2020 or the Official Information Act 1982).
- (6) The authority must not release any information or document received by it under this section if the information or document is commercially sensitive, unless the release is required by an enactment.

- (7) In this section, **information** means any information, whether contained in a document or not.

Compare: 2020 No 31 ss 87–89

### **63 Extension of time to provide information**

- (1) An individual or organisation that receives a notice under section 62 may apply to the TF authority for an extension of time to provide the information or document, and the authority may extend the time for a period it considers to be reasonable in the circumstances.
- (2) The application must set out the reasons for requesting the extension of time.

#### *TF authority members*

### **64 Appointment of TF authority members**

- (1) The chief executive must appoint the members of the TF authority. The members may include public service employees and individuals from outside the public service.
- (2) When selecting the authority's members, the chief executive must ensure that the authority has—
- (a) members who collectively possess the appropriate skills and experience to carry out its functions; and
  - (b) sufficient members to carry out its functions in a timely and efficient manner.

### **65 Removal of TF authority members**

The chief executive may give written notice to a member of the TF authority removing them from the authority if they become bankrupt or neglect their duty, or for misconduct.

### **66 Remuneration of TF authority members**

- (1) A member of the TF authority who is a public service employee is entitled to be paid by their employer, as if they were undertaking their usual duties, for time reasonably taken by them away from their usual duties to undertake the work of the authority.
- (2) Other members of the authority are not public service employees as a result of their appointment to the authority, and the responsible department must pay fees for their services, and expenses reasonably incurred by them in providing those services, in accordance with the fees framework.

## Part 6

### Complaints and offences

#### 67 Purpose of Part

The purpose of this Part is to promote confidence in the trust framework by establishing processes for dealing with complaints.

#### 68 Principles

In carrying out its functions under this Part (except when granting remedies or prosecuting offences), the TF authority must be guided by the following principles:

- (a) processes for complaints should be fair and accessible and have particular regard to tikanga Māori;
- (b) complaints should be resolved in a timely and efficient manner;
- (c) complaints should be resolved at a level appropriate to the seriousness and nature of the complaint.

#### *Complaints*

#### 69 Who may make complaint

- (1) Any person may complain to the TF authority if they believe there has been a breach by a TF provider.
- (2) **Breach** means a breach of the TF rules, the regulations, terms of use of accreditation marks, or provisions of this Act.

#### 70 How to make complaint

- (1) A complaint must—
  - (a) identify the complainant and the TF provider to which the complaint relates; and
  - (b) describe the alleged breach; and
  - (c) state why the complainant believes that a breach has occurred; and
  - (d) comply with other requirements set out in the regulations.
- (2) A complainant is entitled to reasonable assistance from the TF authority to meet the requirements of subsection (1).

#### 71 How complaints must be dealt with

- (1) As soon as practicable after receiving a complaint, the TF authority must—
  - (a) tell the complainant in writing that their complaint has been received; and
  - (b) tell the TF provider in writing about the substance of the complaint; and
  - (c) give the TF provider a reasonable opportunity to comment; and

- (d) consider the complaint and make a preliminary assessment of whether a breach appears to have occurred unless it decides—
  - (i) to refer the complaint to an office holder under section 72; or
  - (ii) not to consider the complaint further under section 73.
- (2) If part of a complaint is referred to an office holder, the authority must make a preliminary assessment of the remaining part of the complaint unless it decides not to consider that part of the complaint further under section 73.

## **72 Referral of complaints to office holders**

- (1) This section applies if the TF authority considers that a complaint (in full or in part) may be more appropriately dealt with by:
  - (a) the Ombudsman;
  - (b) the Privacy Commissioner;
  - (c) the Inspector-General of Intelligence and Security;
  - (d) another office holder.
- (2) The authority must consult the relevant office holder about whether the complaint—
  - (a) is within their jurisdiction; and
  - (b) would be more appropriately dealt with by them.
- (3) The decision about whether a complaint is within the jurisdiction of an office holder is a matter solely for the relevant office holder.
- (4) If the complaint is within the jurisdiction of the office holder and the authority decides that it would be more appropriately dealt with by that office holder, the authority must as soon as practicable—
  - (a) refer the complaint or the relevant part of it to the relevant office holder; and
  - (b) tell the complainant and TF provider in writing it has done so.

## **73 TF authority may decide not to consider complaint further**

- (1) The TF authority may decide not to consider a complaint or part of a complaint further if it considers—
  - (a) the complaint does not meet the requirements of section 70; or
  - (b) the complaint involves any of the matters set out in section 76(2); or
  - (c) the complainant has not made reasonable efforts to first resolve the complaint directly with the TF provider concerned; or
  - (d) there is a dispute resolution scheme or process available to resolve the complaint because of the TF provider's membership of a particular industry and the complainant has not made use of it; or

- (e) the complaint appears to largely involve a commercial dispute between 2 or more trust framework participants; or
  - (f) the complainant knew about the breach or potential breach for 12 months or more before they made the complaint; or
  - (g) the length of time that has elapsed between the date on which the subject of the complaint arose and the date on which the complaint was made means that consideration of the complaint is no longer practicable or desirable; or
  - (h) the complainant does not have a sufficient personal interest in the subject of the complaint; or
  - (i) the complaint is frivolous, vexatious, or not made in good faith.
- (2) The authority may also decide not to consider a complaint further if, after having regard to all of the circumstances of the case, the authority is of the opinion that considering the complaint further is unnecessary or inappropriate.
- (3) If the authority decides not to consider a complaint further, it must tell the complainant and TF provider in writing of the decision and give its reasons.

Compare: 2020 No 31 s 74

### *Preliminary assessment of complaints*

#### **74 Procedure for preliminary assessment of complaints**

- (1) When making a preliminary assessment of a complaint, the TF authority must take into account—
- (a) any relevant information and comments received from the complainant; and
  - (b) any relevant information and comments received from the TF provider; and
  - (c) any other relevant information that is readily accessible to it.
- (2) The authority may, for the purpose of making a preliminary assessment, in its absolute discretion, decide—
- (a) to provide information received from the TF provider to the complainant and seek their response;
  - (b) to obtain information or documents from an individual or organisation under section 62.
- (3) *See* section 62(6), which limits the release of any information or document that is commercially sensitive. The authority must also not provide any information or document to a complainant that is confidential.
- (4) If the authority obtains information or documents under section 62 from an individual or organisation that is not the TF provider, it must give the TF provider copies and a reasonable opportunity to comment on them.



- (5) The authority may, when making a preliminary assessment, regulate its procedure as it considers appropriate and in a way that is consistent with this Act and the regulations (if any).

#### **75 Notice of preliminary assessment**

The TF authority must give the complainant and the TF provider—

- (a) written notice of its preliminary assessment including its reasons for the assessment; and
- (b) if its assessment is that it appears a breach has occurred,—
  - (i) information about the dispute resolution scheme run by the authority; and
  - (ii) information about the authority’s powers of investigation and the remedies it may grant.

#### *Dispute resolution scheme*

#### **76 Dispute resolution scheme**

- (1) The TF authority may, in accordance with any requirements and criteria prescribed in the regulations, recommend a dispute resolution scheme for the Minister’s approval.
- (2) The dispute resolution scheme must not deal with the following:
  - (a) a matter that may be dealt with under the Privacy Act 2020;
  - (b) an employment dispute that may be dealt with under the Employment Relations Act 2000;
  - (c) a dispute relating to acts that may be prosecuted as an offence under this Act;
  - (d) a dispute relating to the carrying out of a Minister’s function;
  - (e) a dispute of a kind prescribed by the regulations.
- (3) The chief executive may employ or engage persons or organisations to provide dispute resolution services to support the resolution of complaints under this Part.

#### **77 Ministerial approval of dispute resolution scheme**

The Minister may approve a dispute resolution scheme if satisfied that—

- (a) it provides a means of resolving complaints that is consistent with the principles listed in section 68; and
- (b) it meets any requirements set out in the regulations.

*Investigations by TF authority***78 Investigation of breach**

The TF authority may commence an investigation—

- (a) following a preliminary assessment that a breach that was the subject of a complaint appears to have occurred;
- (b) on its own initiative, into any matter that could be the subject of a complaint under this Part.

Compare: 2020 No 31 s 79

**79 Commencing investigation**

- (1) As the first step of an investigation, the TF authority must notify the TF provider that it is commencing an investigation.
- (2) A notice given under subsection (1) must—
  - (a) set out the details of—
    - (i) the alleged breach that was the subject of a complaint; or
    - (ii) if the investigation is commenced under section 78(b), the subject of and reasons for the investigation; and
  - (b) advise the TF provider of their right to provide, within a reasonable time, a written response to the authority.

Compare: 2020 No 31 s 80

**80 Conducting investigation**

- (1) The TF authority must conduct an investigation in a timely manner.
- (2) During an investigation, the authority may—
  - (a) hear and obtain information or documents from any person (*see* section 62); and
  - (b) make any inquiries.
- (3) At any time during an investigation, the authority may decide to take no further action on a complaint or matter if it—
  - (a) is satisfied that any of the matters set out in section 73(1) apply; or
  - (b) after having regard to all of the circumstances of the case, considers that any further action is unnecessary or inappropriate.
- (4) As soon as practicable after making a decision under subsection (3), the authority must notify the complainant (if any) and the TF provider of—
  - (a) that decision; and
  - (b) the reasons for that decision.
- (5) It is not necessary for the authority to hold a hearing, and no person is entitled as of right to be heard by the authority.

- (6) Any investigation conducted by the authority must be conducted in private.

Compare: 2020 No 31 s 81

### **81 TF authority may regulate own procedure**

When conducting an investigation, the TF authority may regulate its procedure as it considers appropriate and in a way that is consistent with this Act and the regulations (if any).

Compare: 2020 No 31 s 82

### **82 Finding by TF authority**

- (1) If the TF authority is satisfied, on the balance of probabilities, that a breach has occurred, it must give the complainant (if any) and the TF provider written notice of its decision, including its reasons.
- (2) The authority may also grant 1 or more of the remedies listed in section 83 but must first give the TF provider a reasonable opportunity to make submissions on the issue of remedies.
- (3) The authority may find that a breach has occurred even if it is of the view that the breach was unintentional or without negligence on the part of the TF provider. However, the authority must take the conduct of the TF provider into account when deciding what, if any, remedy or remedies to grant.

Compare: 2020 No 31 s 102(3)

## *Remedies*

### **83 Remedies following finding of breach**

- (1) If the TF authority finds a breach by a TF provider, it may do 1 or more of the following:
- (a) issue a private or public warning;
  - (b) require the provider to comply with additional record-keeping or reporting requirements either for a specified period or indefinitely;
  - (c) issue a compliance order;
  - (d) suspend the provider's accreditation or the accreditation of the relevant service they provide until they take specified steps;
  - (e) cancel the provider's accreditation or the accreditation of the relevant service they provide.
- (2) If the authority is satisfied that a TF provider has failed to comply with a compliance order or give the notice required by section 89, it may suspend or cancel the accreditation of the provider or the relevant service.

*Public warnings***84 Public warnings**

- (1) The TF authority may issue a public warning under section 83(1)(a) only if it is satisfied on reasonable grounds that—
  - (a) a public warning is necessary to give users notice that use of a service provided by the TF provider carries a material risk of identity fraud, economic loss, or physical or emotional harm; and
  - (b) that risk is attributable to the breach by the TF provider; and
  - (c) the imposition of 1 or more of the other remedies under section 83 is insufficient to mitigate that risk; and
  - (d) issuing a public warning will not result in disclosure of a security-related vulnerability of the relevant service that could be exploited by others.
- (2) Before making a decision under this section, the authority must—
  - (a) take reasonable steps to give notice to the TF provider that it is considering issuing a public warning and give them a reasonable opportunity to comment; and
  - (b) take into account any comments they make.

*Additional record-keeping or reporting requirements***85 Additional record-keeping or reporting requirements**

The authority may require additional record-keeping or reporting requirements under section 83(1)(b) for any period that the authority considers appropriate, but it may lift those additional requirements earlier if satisfied that they are no longer needed.

*Compliance orders***86 Issuing compliance order**

- (1) Before issuing a compliance order under section 83(1)(c), the TF authority must consider all of the following:
  - (a) whether there is another means under this Act of dealing with the breach that would be more effective than a compliance order;
  - (b) the seriousness of the breach;
  - (c) the likelihood of the breach continuing or being repeated;
  - (d) the number of people who may be or are affected by the breach;
  - (e) whether the TF provider has been co-operative in all dealings with the authority;
  - (f) the likely costs to the TF provider of complying with the order.
- (2) However, each of those factors need be considered only to the extent that—

- (a) it is relevant in the authority's view; and
  - (b) information about the factor is readily available to the authority.
- (3) Before issuing a compliance order, the authority must also—
- (a) take reasonable steps to give notice to the TF provider that it is considering issuing a compliance order and give them a reasonable opportunity to comment on—
    - (i) a draft of the order; and
    - (ii) a summary of the conclusions reached about the factors in subsection (1) that the authority considered; and
  - (b) take into account any comments they make.

Compare: 2020 No 31 s 124

### **87 Form of compliance order**

- (1) A compliance order must—
- (a) state the name of the TF provider and describe the relevant accredited service; and
  - (b) describe the breach, citing the relevant TF rule, regulation, term of use, or provision of this Act; and
  - (c) require the TF provider to remedy the breach within a specified time that is reasonable in the circumstances; and
  - (d) require the TF provider to report to the TF authority, within a specified time or times, about—
    - (i) the steps they have taken to remedy the breach;
    - (ii) whether the breach has been remedied; and
  - (e) inform the TF provider that the order may be varied or cancelled under section 91; and
  - (f) contain other information required by the regulations (if any).
- (2) A compliance order may also—
- (a) require the TF provider to take particular steps to remedy the breach;
  - (b) contain any other information the authority considers would be useful.

Compare: 2020 No 31 s 125

### **88 TF provider response to compliance order**

- (1) A TF provider that is issued with a compliance order must comply with it, including by taking any particular steps to remedy the breach specified in the order.
- (2) The TF provider must remedy the breach,—
- (a) if no time is stated in the order, as soon as is reasonably practicable;
  - (b) within the time stated in the order:

(c) at a later time if varied by the TF authority.

Compare: 2020 No 31 s 126

**89 TF provider must tell TF authority when compliance order complied with**

A TF provider must tell the TF authority when it has complied with a compliance order and must do so within 5 working days of doing so.

**90 TF provider may elect to forfeit accreditation**

- (1) A TF provider that receives a draft compliance order or a compliance order may elect to forfeit their accreditation or the accreditation of the relevant service, whichever is the subject of the draft order or order.
- (2) The TF provider must tell the TF authority that it wishes to do so within 5 working days of receiving the draft order or order.
- (3) If the authority receives the advice referred to in subsection (2) for a draft compliance order, it must cancel the accreditation in place of issuing a compliance order.
- (4) If the authority receives the advice after issuing a compliance order, it must cancel both the accreditation and the compliance order.

**91 TF authority may vary or cancel compliance order**

- (1) A TF provider may apply to the TF authority to vary or cancel a compliance order on the ground that there has been an error of fact or law.
- (2) The authority may do so on terms it considers appropriate.

Compare: 2020 No 31 s 127

*Suspension or cancellation of accreditation following finding of breach*

**92 Suspension of accreditation**

- (1) This section applies if the TF authority has suspended the accreditation of a TF provider or a service they provide—
  - (a) by suspending them or it under section 83(1)(d):
  - (b) by suspending them or it under section 83(2) because the authority is satisfied that a TF provider has failed to comply with a compliance order or it has not received notice required by section 89.
- (2) The suspension may be for any period the authority considers appropriate, but it may reinstate the accreditation earlier if it is satisfied that—
  - (a) any steps specified under section 83(1)(d) have been taken by the TF provider; and
  - (b) the TF provider has complied with the compliance order.
- (3) However, before making a decision under this section, the authority must—

- (a) take reasonable steps to give notice to the TF provider that it is considering suspending the accreditation and give them a reasonable opportunity to comment; and
- (b) take into account any comments they make.

### **93 Cancellation of accreditation**

- (1) This section applies if the TF authority has cancelled the accreditation of a TF provider or a service they provide—
  - (a) by cancelling it under section 83(1)(e);
  - (b) by cancelling it under section 83(2) because the authority is satisfied that a TF provider has failed to comply with a compliance order or it has not received notice required by section 89.
- (2) However, before making a decision under this section, the authority must—
  - (a) take reasonable steps to give notice to the TF provider that it is considering cancelling the accreditation and give them a reasonable opportunity to comment; and
  - (b) take into account any comments they make.

### **94 Suspension or cancellation if breach on 3 or more occasions**

- (1) If a TF provider is found to have breached any of the following on at least 3 separate occasions in a 12-month period, the TF authority may suspend or cancel their accreditation or the accreditation of the relevant service they provide:
  - (a) a TF rule;
  - (b) a regulation;
  - (c) a term of use of an accreditation mark;
  - (d) a provision of this Act.
- (2) The suspension may be for any period the authority considers appropriate, but it may reinstate the accreditation earlier if it is satisfied the suspension is no longer needed.
- (3) The authority must take reasonable steps to give notice to the TF provider of the suspension or cancellation, but need not give them an opportunity to comment before suspending or cancelling the accreditation.

#### *Suspension or cancellation of accreditation for other reasons*

### **95 Suspension or cancellation of accreditation**

- (1) The accreditation of a TF provider or of a service they provide may be suspended or cancelled by the TF authority if the TF provider—
  - (a) is convicted of an offence under this Act;
  - (b) has ceased to operate all or a substantial proportion of their accredited digital identity services;

- (c) is declared bankrupt or insolvent, or is unable to pay their debts as they fall due, or enters into an arrangement with creditors as a consequence of defaulting on a payment relating to a debt:
- (d) is a director of a company that has been put into receivership or liquidation:
- (e) has a receiver appointed for a business through which accredited services are provided:
- (f) does something or omits to do something that, in the view of the authority, may pose a risk to—
  - (i) the security, privacy, confidentiality, or safety of the information of any trust framework participants:
  - (ii) the integrity or reputation of the trust framework.
- (2) This section applies whether or not the authority has found a breach by a TF provider.
- (3) The suspension may be for any period the authority considers appropriate, but it may reinstate the accreditation earlier if it is satisfied the suspension is no longer needed.
- (4) However, before making a decision under this section, the authority must—
  - (a) take reasonable steps to give notice to the TF provider that it is considering suspending or cancelling the accreditation and give them a reasonable opportunity to comment; and
  - (b) take into account any comments they make.
- (5) For the purposes of subsection (1), the authority may take into account information that it reasonably believes is likely to be accurate.
- (6) In this section, **TF provider** means the TF provider and (as relevant) their officers and those involved in the management of, employed by, or contracted by, the TF provider.

### *Offences*

#### **96 Offence to knowingly or recklessly misrepresent provider to be TF provider or service to be accredited service**

- (1) A person who knowingly or recklessly represents themselves to be a TF provider when they are not commits an offence and is liable on conviction to,—
  - (a) in the case of an individual, a maximum fine of \$50,000;
  - (b) in the case of a body corporate, a maximum fine of \$100,000.
- (2) A person who knowingly or recklessly represents a digital identity service to be an accredited service when it is not (including using an accreditation mark when not entitled to do so) commits an offence and is liable on conviction to,—
  - (a) in the case of an individual, a maximum fine of \$50,000;



- (b) in the case of a body corporate, a maximum fine of \$100,000.

**97 Offence to misuse accreditation mark**

A person who knowingly or recklessly uses an accreditation mark in a manner that is contrary to the terms of use set by the TF authority commits an offence and is liable on conviction to,—

- (a) in the case of an individual, a maximum fine of \$50,000;
- (b) in the case of a body corporate, a maximum fine of \$100,000.

**98 Offence to knowingly or recklessly give false information to TF authority in application for accreditation**

- (1) A person who knowingly or recklessly gives false information to the TF authority in an application for accreditation commits an offence and is liable on conviction to,—

- (a) in the case of an individual, a maximum fine of \$50,000;
- (b) in the case of a body corporate, a maximum fine of \$100,000.

- (2) In this section, **application for accreditation** means—

- (a) an application for accreditation under section 23;
- (b) an application for reconsideration under section 29;
- (c) an application for renewal of accreditation under section 31;
- (d) an application for provisional accreditation under section 32;
- (e) any communication with the authority relating to an application in paragraphs (a) to (d), whenever the communication is made.

**99 Offence to fail to give key information or specified information in application for accreditation**

- (1) A person who makes an application for accreditation and who fails without reasonable excuse to give the TF authority key information or specified information in the application commits an offence and is liable on conviction to,—

- (a) in the case of an individual, a maximum fine of \$10,000;
- (b) in the case of a body corporate, a maximum fine of \$20,000.

- (2) In this section and section 100,—

**application for accreditation** means—

- (a) an application for accreditation under section 23;
- (b) an application for reconsideration under section 29;
- (c) an application for renewal of accreditation under section 31;
- (d) an application for provisional accreditation under section 32;
- (e) any communication with the authority relating to an application in paragraphs (a) to (d), whenever the communication is made

**key information** means the information referred to in section 24(1)(b)(i)

**specified information** means the information listed in section 25(1).

**100 Offence to fail to tell TF authority of change to key information or specified information**

- (1) A person who makes an application for accreditation and who fails without reasonable excuse to tell the TF authority of a change to key information or specified information, as required by section 33, commits an offence and is liable on conviction to,—
  - (a) in the case of an individual, a maximum fine of \$10,000;
  - (b) in the case of a body corporate, a maximum fine of \$20,000.
- (2) A TF provider that fails without reasonable excuse to tell the TF authority of any change to key information or specified information, as required by section 33, commits an offence and is liable on conviction to,—
  - (a) in the case of an individual, a maximum fine of \$10,000;
  - (b) in the case of a body corporate, a maximum fine of \$20,000.

**101 Offence to obstruct TF authority**

A person who, without reasonable excuse, obstructs the TF authority when it is carrying out its functions or exercising its powers commits an offence and is liable on conviction to,—

- (a) in the case of an individual, a maximum fine of \$10,000;
- (b) in the case of a body corporate, a maximum fine of \$20,000.

## **Part 7**

### **Regulations, immunity from civil liability, and reviews**

#### *Regulations*

**102 Regulations**

- (1) The Governor-General may, on the recommendation of the Minister, by Order in Council, make regulations for 1 or both of the following purposes:
  - (a) providing for anything this Act says may or must be provided for by regulations;
  - (b) providing for anything incidental that is necessary for carrying out, or giving full effect to, this Act.
- (2) The TF board may recommend draft regulations to the Minister.
- (3) Before regulations are made under this section, the Minister must consult the Office of the Privacy Commissioner.

- (4) Regulations made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

---

**Legislation Act 2019 requirements for secondary legislation made under this section**

<b>Publication</b>	PCO must publish it on the legislation website and notify it in the <i>Gazette</i>	LA19 s 69(1)(c)
<b>Presentation</b>	The Minister must present it to the House of Representatives	LA19 s 114
<b>Disallowance</b>	It may be disallowed by the House of Representatives	LA19 ss 115, 116

*This note is not part of the Act.*

---

*Immunity from civil liability*

**103 Immunity for members and staff of TF board and TF authority, members of Māori Advisory Group, and members of advisory committees who are not public service employees**

- (1) This section applies to a member of the TF board, the TF authority, the Māori Advisory Group, and any advisory committee, and a staff member of the board or the authority, who is not a public service employee.
- (2) Section 104 of the Public Service Act 2020 applies to a person listed in subsection (1) as if they were a public service employee.

**104 Immunity for TF providers for actions of users**

- (1) A TF provider is immune from liability in civil proceedings for a claim that a user, when using an accredited digital identity service provided by the TF provider, has caused harm or damage to an individual or organisation or has themselves suffered harm or damage.
- (2) However, subsection (1) does not apply—
- if an act or omission by a TF provider relating to the alleged harm or damage constitutes bad faith or gross negligence:
  - to proceedings arising from a complaint under the Privacy Act 2020.
- (3) In this section,—

**TF provider** means the TF provider and (as relevant) their officers and those involved in the management of, employed by, or contracted by, the TF provider  
**using an accredited digital identity service** means—

- using an accredited service for a transaction with a relying party; or
- communicating or interacting with a TF provider in relation to the provision of that service to the user.

Compare: 2012 No 123 s 65(5); 2012 No 124 s 20(3)

*Reviews***105 Review of TF board's operation**

- (1) A review of the TF board's operation must be commenced by its responsible department as soon as practicable after the second anniversary of the commencement of section 43.
- (2) As soon as practicable after that date, the Minister must set a date for completion of the review.
- (3) The review must include—
  - (a) an assessment of the effectiveness of the board in carrying out its functions; and
  - (b) an assessment of the viability of other models for carrying out the board's functions; and
  - (c) an assessment of how other models might better—
    - (i) ensure the privacy and security of user information (including Crown-held data) and protect it from unauthorised use; and
    - (ii) provide opportunities for Māori engagement in the trust framework; and
  - (d) consideration of whether, taking into account the matters in paragraphs (a) to (c) and any other relevant matters, the board should be established as a Crown entity.
- (4) The review may include other matters as the department considers appropriate.
- (5) The Minister must present a copy of the review to the House of Representatives as soon as practicable after receiving it from the department.

**106 Review of complaints process and dispute resolution scheme**

- (1) A first review of the complaints process and dispute resolution scheme operated by the TF authority under this Act (including if this is done by persons or organisations under section 76(3)) must be undertaken by the TF board as soon as practicable after the second anniversary of,—
  - (a) in the case of the complaints process, the commencement of section 69;
  - (b) in the case of the dispute resolution scheme, the commencement of section 76.
- (2) Subsequent reviews of that process and scheme must be undertaken by the authority at 5-yearly intervals from the date on which the first review (in each case) is commenced.

---

**Schedule**  
**Transitional, savings, and related provisions**

s 6

**Part 1**  
**Provisions relating to this Act as enacted**

There are no transitional, savings, or related provisions relating to this Act as enacted.

**Legislative history**

29 September 2021	Introduction (Bill 78–1)
19 October 2021	First reading and referral to Economic Development, Science and Innovation Committee
19 April 2022	Reported from Economic Development, Science and Innovation Committee (Bill 78–2)
26 July 2022	Second reading
28 March 2023	Committee of the whole House, third reading
5 April 2023	Royal assent

This Act is administered by the Department of Internal Affairs.