15 May 2026

# Practice Note: The DISTF and s11 of the Privacy Act

## (Personal information treated as being held by another agency in certain circumstances)

This practice note sets out the Trust Framework Authority's interpretation of how section 11 of the Privacy Act 2020 applies in the context of digital identity services and, in particular, Part 4 of the Digital Identity Services Trust Framework (Trust Framework) Rules.

### Background

An important feature of defining privacy risks and responsibilities is clarifying who "holds" and is responsible for personal information. Understanding the role of a provider in relation to personal information is crucial in determining its obligations under the Privacy Act and the Trust Framework Rules.

### Definitions

The terms "controller" and "processor" are used in this document as a shorthand to provide clarity when referring to the various parties under section 11 of the Privacy Act. Note those are not statutory terms used in the Privacy Act or in the Trust Framework Rules.

**Controller**: An agency that engages another party to hold or process personal information on its behalf. The controller typically determines how personal information will be collected, used and shared. It is deemed to "hold" that information for the purposes of the Privacy Act and is responsible for complying with the Privacy Act.

**Processor**: An agent engaged by a controller solely for the purposes of holding or processing personal information for or on behalf of the controller. The processor cannot use or disclose the information for its own purposes. If it does, it will cease to be a processor in respect of the relevant personal information, which will be treated as being held by both the controller and the processor.

### Summary

Where a provider is solely a processor, the controller will be responsible for complying with the Privacy Act.

A provider could be processor for some functions (e.g. providing digital identity services) and a controller for others (e.g. in respect of the personal information of its staff). The provider and the independent privacy evaluator must consider the management of personal information for the service(s) in scope of the application for Trust Framework accreditation.

While controllers retain primary Privacy Act liability under s 11, processors still have privacy obligations under the Trust Framework Rules. The controller should impose contractual obligations on the processor to support the controller's compliance with the Privacy Act, including requirements for the processor to notify the controller of any privacy breach as soon as possible.

If the provider is not a processor because it uses or discloses personal information for its own purposes in addition to providing services to a controller, then both the provider and the controller will be deemed to "hold" and be responsible for that information under the Privacy Act. In those circumstances, the controller will need to assess whether sharing personal information with the provider is a "disclosure" under the Privacy Act that is permitted under IPP 11 and IPP 12 (where the provider is based overseas).

## How do you determine if a provider is a processor?

The key question in the context of the service(s) in scope of the accreditation application and the independent privacy evaluation is:

> Does the provider hold or process personal information **solely on behalf of another agency**, or does it use or disclose that information for its own purposes?

Note that the classification of a provider as a "processor" in a contract is not determinative for the purposes of section 11 of the Privacy Act.

Processor status depends on the substance of the arrangement and the actual processing activities undertaken in practice. Independent privacy evaluators must assess whether the provider **in fact** acts solely on behalf of the controller, rather than relying on contractual assertions.

## Examples where a provider **is** a processor

**1. Biometric comparison service**

A provider offers a white-labelled identity verification service that includes biometric matching. It is engaged by a bank to integrate the identity verification service into the bank's customer onboarding process.

- The bank engages the provider to provide the identity verification service, which the bank presents to its customers using its own branding. The bank determines when

identity verification is required and how the verification outcome is used within its onboarding process. The bank is the **controller**.

- The provider collects and processes the personal and biometric information of bank customers to verify customer identities on behalf of the bank, including confirming biometric matches. The provider does not retain, re-use or disclose the personal information beyond what is necessary to perform the biometric matching and identify verification and deletes the information on completion of the customer journey. The provider is a **processor**.

**2. Binding service**

A provider offers a binding service that securely links verified credentials and associated personal information to the correct individual. The provider is engaged by a telecommunications company dealing with high levels of SIM-swap fraud to provide the binding service in relation to the telco's online customer portal. This will enable telco customers to bind a verified digital identity credential to their customer account and help strengthen identity assurance for access to the portal.

- The telco wants to integrate the provider's binding service into its customer account management and authentication processes. The telco determines when binding is required (for example, during account recovery or high-risk transactions) and what personal information must be used to establish and confirm the link between the verified credential and the individual's customer account. The telco is the **controller**.
- The provider processes the personal information necessary to perform the binding service on behalf of the telco, including completing and recording the binding event that securely links the verified credential and associated personal information to the correct individual and their customer account. The provider does not retain, re-use, aggregate or disclose the personal information for its own purposes. The provider is a **processor**.

For further information on working with third party providers, see https://www.privacy.org.nz/resources-and-learning/a-z-topics/working-with-third-party-providers/.

## Examples of where a provider is **not** a processor

**1. Authentication service**

A provider offers a multi-factor authentication service that enables individuals to use authenticators such as passwords or device-based authenticators to access their online accounts and demonstrate that they are the same individual in subsequent interactions.

The provider is engaged by a national online retailer to integrate the provider's authentication service into the retailer's customer login and account security processes. The retailer wants to use the authentication service to help reduce online account fraud.

- The retailer determines when authentication is required (for example when customers change delivery details or access stored payment methods) and sets the access rules for its customers. The retailer is the **controller**.

- The provider processes the authenticators and related information necessary to perform the authentication services on behalf of the retailer, including verifying login attempts and returning authentication outcomes to the retailer.

- However, the provider also aggregates and analyses authentication logs and metadata across multiple customers/relying parties to develop its own commercial threat intelligence products and conduct its own analytics. In doing so, the provider is using the personal information for its own purposes so it is **not acting solely as a processor** and will be considered a controller with compliance obligations under the Privacy Act.

## Practical Questions for Evaluators

In the context of section 11 of the Privacy Act 2020, a provider uses or discloses personal information for its own purposes when it uses or shares that information for any purpose other than delivering the services it has been engaged to provide.

That will often involve deriving independent value from the personal information beyond what is necessary to deliver the service on behalf of the engaging agency.

When assessing whether a provider is a processor under section 11, independent privacy evaluators should consider whether the provider:

- uses the personal information for independent analytics, model training or service improvement beyond what is strictly necessary to deliver the contracted service
- develops its own commercial products or services based on the personal information
- aggregates personal information across multiple clients/controllers or relying parties
- discloses personal information beyond what is required for the contracted service
- retains personal information for purposes unrelated to providing, evidencing or securing the contracted service.

If the answer to such questions is "yes", the provider is unlikely to be acting solely as a processor under section 11 of the Privacy Act. This will make it a controller, with responsibility for demonstrating compliance with both the DIST Rules and the Privacy Act.

A provider does not use information for its own purposes if it:

- processes personal information solely to perform the contracted credential, binding, authentication or facilitation service
- retains information only for evidential, security or compliance purposes required to deliver that service for the controller
- does not reuse or disclose the information beyond what is necessary to fulfil the provision of services to the controller.

## Application of Trust Framework Rules to processors

Controllers are responsible for complying with the Privacy Act. Both controllers and processors are responsible for complying with the Trust Framework Rules.

Part 4, rule 12 of the Trust Framework Rules requires all accredited providers to:

- Complete an independent **privacy impact assessment** (**PIA**) for the digital identity service they provide (rule 12(2)) and review the PIA at the earlier of two years from the previous review or when there is a change to the service (rule 12(4))
- Appoint a **designated individual** who is responsible for privacy (rule 12(5))
- Provide regular **training** to staff on their privacy policies (rule 12(6))
- **Communicate** changes to privacy policies and processes to staff (rule 12(7))
- Maintain a documented **privacy incident response plan** (rule 12(8))
- Establish an **incident register** (rule 12(9)) and review it regularly to ensure applicable processes and policies are updated accordingly (rule 12 (10))
- Publish a **Privacy Statement** (rule 12(11))
- **Only use** personal information collected for **digital identity service purposes** for other purposes with the explicit authorisation of the user (rule 12(12)).

It is important to recognise that **not all processors are alike**. Depending on how they process personal information, they will have **different privacy risk profiles.**

For example, a provider processing encrypted credential data with only very limited retention presents a different privacy risk profile from one that retains authentication logs or binding records for months.

Each privacy evaluation must take account of the **specific privacy risk profile** of the provider in question.

## Application of Trust Framework Rules to processors

The independent evaluator must complete the independent privacy evaluation template for **all** accreditation applications, irrespective of whether the provider is a processor or a controller. However, the following should be specifically considered for providers that are **processors**.

| Rule requirement | Baseline expectation |
|---|---|
| **Rule 12(1)**<br>**Privacy Impact Assessment (PIA)**<br>All Trust Framework providers must complete a PIA for the accredited digital identity service they provide, featuring the content listed in rule 12(3). | Every processor must:<br>• conduct a PIA covering the digital identity service it provides<br>• clearly document its section 11 status and identify its core processing functions undertaken solely on behalf of a controller<br>• identify if and where it is ever a controller (i.e. if it uses or discloses personal information for its own purposes in certain areas). |
| **Rule 12(6) and (7)**<br>**Training and Internal Communications**<br>All Trust Framework providers must ensure personnel receive regular training on privacy policies and ongoing communications about any changes to its privacy policies and processes. | Every processor will provide regular privacy training to all relevant personnel covering the following.<br>• The processor's role under section 11 and a clearly explained prohibition on using or disclosing the relevant personal information for any purpose other than delivering the services it has been engaged to provide.<br>• Secure information handling requirements, including access controls and storage and disposal processes.<br>• Identification and escalation of privacy incidents.<br>• Recognition and referral of privacy complaints and access or correction requests to the relevant controller. |

| Rule requirement | Baseline expectation |
|---|---|
| **Rule 12(8)**<br>**Privacy Incident Response Plan**<br>All Trust Framework providers must maintain a documented privacy incident response plan which:<br>(a) clearly assigns roles and responsibilities;<br>(b) sets out escalation and notification processes; and<br>(c) includes processes to contain and assess the incident. | In addition to the elements required by rule 12(8), every processor's privacy incident plan should include a requirement for prompt notification to affected controllers.<br>Also consider whether it is necessary to specify what information must be provided to controllers to support breach assessment and potential notification under the Privacy Act. |
| **Rule 12(9) and (10)**<br>**Incident Register and Review**<br>All Trust Framework providers must:<br>• maintain an incident register;<br>• provide instructions for personnel to record incidents;<br>• review the register regularly. | In addition to the rule 12(9) and (10) obligations, processors must also record which controller(s) it has notified in relation to any incident. |
| **Rule 12(11)**<br>**Privacy Statement**<br>All Trust Framework providers must have a Privacy Statement. | A processor's privacy statement, or equivalent, should:<br>• clearly describe its role as a provider, including that it processes personal information on behalf of controllers<br>• identify categories of personal information handled<br>• clarify that it does not use or disclose personal information for its own purposes<br>• explain how individuals may exercise access or correction rights, including referral to the controller where appropriate.<br>The privacy statement must clearly distinguish between:<br>• processing carried out solely on behalf of controllers under section 11; and<br>• processing carried out by the provider in its own right. |