Australian Government

Office of the Australian Information Commissioner

Relying parties: privacy obligations when handling personal information

November 2026



OAIC

Contents

What is a relying party? 2

What privacy obligations apply to relying parties? 2

Key steps for relying parties to protect personal information 3

Further information 6

What is a relying party?

Please refer to this page for further information on whether your entity will be acting as a relying party.

What privacy obligations apply to relying parties?

When using digital ID services, a relying party's handling of personal information will be regulated by any existing privacy legislation that applies to it. The additional privacy safeguards in the Act do not apply to relying parties.

For example:

- A relying party that is an APP entity covered by the Privacy Act[1]: their handling of personal information when using digital ID services will be regulated by the Australian Privacy Principles (APPs).
- A relying party that is a private sector entity that does not fall within the definition of 'APP entity': no specific privacy framework applies, but the entity should adopt best practice privacy practices.
- A relying party that is a state or territory agency: their handling of personal information when using digital ID services will be regulated by their relevant state or territory privacy legislation.

The legislation contains privacy-enhancing features to minimise the collection of 'attributes' by relying parties, so that a relying party only collects the attributes that are necessary for the service that an individual is accessing. These features include:

- an accredited entity needing an individual's express consent before it can disclose certain attributes to a relying party.[2]
- a 'data minimisation principle' obligation on an accredited entity to ensure that a relying party can only select the attributes of an individual that are necessary to provide its services.[3]

[1] The Privacy Act applies to Australian Government agencies and organisations with an annual turnover of more than $3 million. The Privacy Act also covers some small business operators (refer to guidance on OAIC website: organisations with an annual turnover of $3 million or less).

[2] s 45 of the Digital ID Act.

[3] See rule 4.42 of the Digital ID (Accreditation) Rules.

- participating relying parties do not have access to, or the ability to obtain and disclose, restricted attributes within the AGDIS by default[4]. Furthermore, restricted attributes must not be disclosed to relying parties who do not participate in AGDIS if the accredited entity's conditions do not include the correct authorisation.[5]

Key steps for relying parties to protect personal information

Example:

Rachel wishes to use XYZ bank's online services. XYZ bank (as the relying party) offers a Digital ID log in page which Rachel selects.

The identity exchange provider (IXP) must obtain Rachel's express consent for her identity service provider (ISP) to share certain attributes with the relying party. To do this, Rachel logs into her Digital ID and authenticates her identity. She provides express consent for the sharing of her attributes from the ISP to the relying party through the IXP.

To ensure data minimisation and only required personal information is shared, the Digital ID Regulator has imposed accreditation conditions on the ISP which determine which restricted attributes can be provided through the IXP for the relying party's purposes. XYZ bank does not require Rachel to provide any restricted attributes as part of delivering its service to Rachel. XYZ bank has selected from the ISP only the attributes it requires, in order to provide Rachel with use of their online banking services.

The relying party collects and uses the attributes required and provides Rachel with use of their online banking services.

Topic	APP(s)	Description	Further OAIC website guidance
Develop policies, procedures and systems	APP 1.2	APP 1.2 requires APP entities to take reasonable steps to implement practices, procedures and systems relating to their functions and activities that ensure compliance with the APPs, and that enable the entity to deal with inquiries or complaints from individuals about the entity's	Australian Privacy Principles Guidelines: Chapter 1 (APP 1).

[4] s 75 of the Digital ID Act and [31] of the Statement of Compatibility with Human Rights in the Revised Explanatory Memorandum to the Digital ID Act.

[5] s 46(2) of the Digital ID Act.

Topic	APP(s)	Description	Further OAIC website guidance
		compliance with the APPs. As a foundational principle, compliance with this APP assists compliance with all other APPs.	
Data minimisation	APP 3, APP 11	Data minimisation is the principle of limiting the collection, use and disclosure of personal information. Under APP 3, an APP entity must not collect personal information unless the information is reasonably necessary for one or more of their functions or activities and, in the case of sensitive information, the individual consents. APP 11.2 outlines the circumstances when an entity should take reasonable steps to destroy or de-identify the personal information of individuals. Relying parties who seek to rely on digital ID services should consider what kind of information is reasonably necessary to provide their services to an individual. A digital ID provided by an accredited provider means the individual has been through rigorous identity proofing processes. The higher the identity proofing level, the higher the assurance and trust that an individual is who they say they are. A relying party should consider what kind of personal information, if any, is required beyond the confidence that an individual's identity has been verified to a certain level.	Australian Privacy Principles Guidelines: Chapter 3 (APP 3) Australian Privacy Principles Guidelines: Chapter 11 (APP 11)

Topic	APP(s)	Description	Further OAIC website guidance
Data breach planning	APP 11	Compliance with the requirement to secure personal information in APP 11 is key to minimising the risk of a data breach. APP 11 requires APP entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. The type of steps that are reasonable to protect information will depend on the circumstances of the entity and the risks associated with personal information handled by the entity. The OAIC recommends that all APP entities, including relying parties, have a data breach response plan. This plan will assist in meeting privacy obligations, limiting the consequences of a data breach and preserving and building public trust. A data breach response plan should set out the roles and responsibilities involved in managing a data breach and what steps an entity will take if a data breach occurs. For participating relying parties, it is important to note that the Digital ID Rules[6] contain requirements in relation to cyber security, fraud management and disaster recovery plans which may be relevant to an entity's data breach response planning.	Part 2: Preparing a data breach response plan | OAIC

[6] See rule 3.3 of the Digital ID Rules.

Topic	APP(s)	Description	Further OAIC website guidance
Privacy complaints mechanisms	APP 1	Relying parties, as APP entities, must implement procedures for receiving and responding to privacy complaints and inquiries. If complainants are unhappy with how the entity has handled the matter and are dissatisfied with the response, they are able to lodge a complaint with the OAIC.	Handling privacy complaints | OAIC.

Further information

For more information on privacy obligations, please refer to the following pages on the OAIC website:

- Privacy guidance for organisations and government agencies | OAIC
- Privacy Foundations self-assessment tool
- State and territory privacy legislation | OAIC