



Privacy Commissioner
Te Mana Mātāpono Matatapu

Disclosing personal information outside New Zealand

– the new information privacy
principle 12

Disclosing personal information outside New Zealand – the new information privacy principle 12

This guidance provides a practical, step-by-step introduction to the requirements of principle 12 of the Privacy Act for organisations considering disclosing personal information outside New Zealand. You may need to get more detailed advice on how the requirements apply to your organisation's specific situation.

Principle 12 is a new privacy principle introduced in the Privacy Act 2020. You can read more about the purpose of the principle [here](#).

What does principle 12 do?

Principle 12 enables a business or organisation to disclose personal information to a foreign person or entity who is subject to comparable privacy safeguards, or when the disclosure is authorised by the person to whom the information relates.

When does principle 12 apply?

Principle 12 only applies if you are disclosing information from your organisation to a foreign person or entity.

When does principle 12 not apply?

Principle 12 does not apply if the personal information:

- Is sent to a person or entity that is subject to the New Zealand Privacy Act
- is sent to an agent for storage or processing (see below), or
- is sent to the person concerned (including the person's authorised representative), or
- is publicly available.

What do I need to do?

You must have reasonable grounds to believe that at least one of the criteria in principle 12 applies before disclosing personal information to a foreign person or entity. As discussed below, the best and most practical way to comply with principle 12 might be through the terms of your contract with the foreign person or entity. The Office of the Privacy Commissioner has developed model contract clauses for this purpose.

If your organisation regularly discloses personal information overseas, you must be satisfied that you continue to have reasonable grounds to believe that the disclosure is permitted under principle 12. That is, you must be satisfied that comparable safeguards or authorisation by the person concerned still apply to ongoing disclosures to foreign persons or entities.

What about sending information to a cloud provider or other agent?

Using offshore cloud providers or other agents to store or process your data is not treated as a disclosure under principle 12, so long as the agent or cloud provider is not using that information for their own purposes.

If the receiving organisation uses or shares that personal information for their own purposes, then the transfer of personal information to them *will* be covered by principle 12.

The Office of the Privacy Commissioner is preparing more detailed guidance about how the Privacy Act applies to information transferred to a cloud provider, software as a service provider or other agent, and this will be available on our website.

Example: Cloud service providers based outside New Zealand

New Zealand Company 'NZC' contracts with 'Overseas Cloud Storage' to store its customer information. The information will be stored in data centres outside New Zealand.

Overseas Cloud Storage is acting as the agent for NZC. NZC is treated as holding the customer information. Principle 12 does not apply in this situation as NZC has not disclosed personal information.

Step-by-step guide

Is the disclosure to a foreign person or entity?

If your organisation is not making a disclosure to a 'foreign person or entity', principle 12 does not apply.

A foreign person or entity is:

- an individual who is not present in New Zealand nor ordinarily resident in New Zealand (for example, a US citizen who does not live in New Zealand)
- an entity that is not established under New Zealand law and does not have its central control and management in New Zealand (for example, a foreign company)
- the Government of an overseas country.

Is the foreign person or entity 'carrying on business' in New Zealand?

Overseas persons or entities are responsible for complying with the New Zealand Privacy Act when they are 'carrying on business' in New Zealand. If you believe on reasonable grounds that the foreign person or entity is subject to the New Zealand Privacy Act, you will meet your obligations under principle 12.

An organisation could seek confirmation from the foreign person or entity that they are carrying on business in New Zealand and are subject to the Privacy Act. This could be by written confirmation or a contractual term.

'Carrying on business' in New Zealand:

Relevant factors include whether:

- the organisation is undertaking activities that involve the collection, use and disclosure of personal information on a repetitive, systematic or continuing basis
- the organisation has a website offering goods or services to countries including New Zealand, or specifically targeted at New Zealanders
- the activities take place or are acted upon in New Zealand, or
- the organisation is the holder of trademarks or has registered web domains in New Zealand.

An organisation can be treated as carrying on business in New Zealand without necessarily:

- (a) being a commercial operation
- (b) having a place of business in New Zealand
- (c) receiving any monetary payment for the supply of goods or services, or
- (d) intending to make a profit from its business in New Zealand.

Organisations such as churches and non-profits groups can be considered as carrying on business in New Zealand if they have regular activities in New Zealand or other relevant links to New Zealand.

Example

A New Zealand bank has a partnership with an overseas-based charity called SpendWell. This involves sharing some banking information about customers so that SpendWell can intervene where necessary to provide financial and wellbeing advice. The bank is very open with its customers about this disclosure. While SpendWell is based overseas, it offers online services to New Zealanders (via a New Zealand website), and uses the information provided by the bank for the purposes of helping New Zealanders. SpendWell is therefore 'carrying on business' in New Zealand and is subject to the New Zealand Privacy Act.

Is there an agreement that provides for comparable safeguards, such as the Office of the Privacy Commissioner model contract clauses?

You may disclose personal information to a foreign person or entity where that entity is required to protect the information in a way that provides comparable safeguards to those in the New Zealand Privacy Act. The best and most practical way to ensure comparable safeguards is through an agreement you have with the foreign person or entity.

If you have reasonable grounds to believe the foreign person or entity is required, under a contractual agreement you have with them, to protect the information in a way that provides comparable safeguards, this will comply with principle 12. If the foreign person or entity is subject to privacy laws that do not provide comparable safeguards (see below), contractual agreements should refer to the applicable legislation and provide additional protections so that the agreement provides comparable safeguards.

We recommend that you consider using the model contract clauses developed by the Office of the Privacy Commissioner. The model contract clauses are designed to assist agencies to comply with principle 12 and to reduce the compliance burden for agencies.

New Zealand model contract clauses to establish comparable safeguards

The Office of the Privacy Commissioner has commissioned law firm Chapman Tripp to develop model contract clauses for agencies to use. These clauses are available [on our website here](#).

The model contract clauses are tailored to the requirements of the New Zealand Privacy Act. They are designed to make it easier to comply with principle 12, particularly for small and medium-sized businesses. Agencies can modify the clauses to suit their needs or use their own contract clauses, so long as comparable privacy safeguards are included.

You will still need to assess whether the model contract clauses are fit for purpose for the particular type of personal information disclosure you are engaged in.

Is the foreign person or entity subject to a comparable privacy law?

You may disclose personal information to a foreign person or entity that is subject to privacy laws that provide comparable safeguards to New Zealand's Privacy Act.

To rely on this ground, you must have reasonable grounds to believe that the personal information will be subject to comparable safeguards. You would need to undertake careful checks or due diligence to be satisfied you can rely on this ground. See below for a summary of some factors to consider when assessing whether overseas privacy laws provide comparable safeguards.

'Comparable safeguards' does not mean that the foreign person or entity must be subject to requirements that are exactly the same as New Zealand requirements. You would need to carefully investigate whether any key differences from New Zealand privacy law are significant. For example, some laws only cover specific sectors, such as health. A privacy law that is limited to the health sector could provide comparable safeguards if the recipient agency is in that sector and is subject to that law.

Some factors to consider when assessing whether a foreign person or entity is subject to a comparable privacy law

1) Scope of the privacy law

Does the privacy law:

- cover the foreign person or entity (i.e. they do not fall within an exemption or carve-out under that law)?
- extend to the personal information that you provided?
- take account of the sensitivity of the information that you provided?
- cover the people whose personal information you have disclosed, who may not be citizens or resident in that country?

2) Protections

Will the foreign person or entity:

- have security safeguards that are reasonable in the circumstances?
- dispose of the personal information securely if they no longer need it?
- be constrained in how they can use the personal information? (see principle 10 of the New Zealand Privacy Act)
- be constrained in how they can disclose the personal information? (see principles 11 and 12 of the Privacy Act)
- be required to notify people about any privacy breach that may cause serious harm?

3) Right to access and seek correction of personal information

Will people:

- have meaningful access to their own information? (including if they are not a citizen or resident of the country the foreign person or entity is in)
- be able to request a correction of their personal information if they consider that it is incorrect?

4) Accessible and meaningful complaint processes

- If something goes wrong, can the affected person access complaint mechanisms with a data protection authority?
- Will that person need legal representation or face other legal costs in accessing justice or remedies?

5) Independent oversight and enforcement

- Is there an independent data protection authority in the country that holds oversight, compliance, and enforcement functions broadly comparable to the New Zealand Privacy Commissioner?

Is the foreign person or entity in a country or a binding scheme that the New Zealand Government has prescribed in regulation?

The Privacy Act allows the New Zealand Government to prescribe in regulation countries or binding schemes that have privacy safeguards that are comparable to New Zealand's.

No such regulations have been made at this time.

Has the individual authorised the disclosure?

You can disclose the personal information to a foreign person or entity if the person concerned has authorised that disclosure.

In those cases, you need to make sure the person understands what they are authorising. You must expressly inform them that the organisation you are disclosing their information to may not protect their information in a way that provides comparable safeguards to the New Zealand Privacy Act. Explain why, in language that is easy to understand.

You will need to provide people with enough information to make an informed decision. Outline where the information will go and explain that you do not believe the recipient will be required to look after the personal information in a way that is comparable to the Privacy Act.

What does it mean to expressly inform people?

When assessing how well an organisation has expressly informed someone, the Office of the Privacy Commissioner will consider:

- Did the organisation take reasonable steps to ensure people were made aware that the foreign person or entity receiving their personal information might not protect the information in a way that provides comparable safeguards?
- Were people informed in a way that was clear to them? (*for example, on the front page of a document or on a separate screen*).
- Was the relevant information buried within a long legal document?

These standards are related but additional to existing principle 3 requirements to adequately inform people about the way their information will be used, for what purpose, and by whom. In addition to meeting the requirements of principle 3, you will need to take steps to inform the person about foreign disclosures and obtain their authorisation.

Is the disclosure necessary to avoid prejudice to the maintenance of the law or to prevent or lessen a serious threat?

You do not need to comply with principle 12 if you believe on reasonable grounds that:

- the disclosure is necessary to avoid prejudice to the maintenance of the law or to prevent or lessen a serious threat, **and**
- it is not reasonably practicable in the circumstances to comply with principle 12 requirements.

It may not be reasonably practicable to comply with principle 12 if the circumstances require the information to be disclosed urgently. Maintenance of the law relates to activities carried out by Police and other key public sector agencies. 'Serious threat' relates to public health or safety, or the life or health of an individual. Further guidance about disclosure under maintenance of the law and serious threat exceptions is available [here](#)¹.

What if none of the options apply to my situation?

If none of the situations discussed above appear to apply to you, you should stop and review the basis for the disclosure to meet one of the available criteria, seek advice or you may decide not to disclose the personal information to the foreign person or entity.

Other statutes may override the privacy principles, including principle 12 (see sections 23 and 24). If your disclosure is authorised by another statute you may not have to comply with principle 12.

¹ <https://www.privacy.org.nz/assets/Files/Reports/October-2017-Final-Guidance-on-releasing-personal-information-to-Police-and-law-enforcement-agencies-Principle-11f-and-ei.pdf>

Appendix: Principle 12 flow chart

