DIGITAL.GOVT.NZ

Assess countries and service providers for data sovereignty

See which legal jurisdictions, often in the form of countries, are commonly used by NZ government organisations — understand the factors and best practice for assessing jurisdictions and service providers.

Jurisdictions commonly used by NZ government organisations

This is not an approved list and it can change to adapt to new legal and privacy conditions. Government organisations can use it as a helpful signpost in their case-by-case risk assessments of public cloud services.

> **Access to the CLASSIFIED report on jurisdictional risks**
>
> Join the Cloud Capabilities Network and request the CLASSIFIED report of jurisdictional risk assessments.
>
> Join the Cloud Capabilities Network

Geographically close — in terms of latency

NZ government organisations tend to use public cloud services that are hosted close to New Zealand:

- Australia
- Singapore
- the United States.

Delays to network availability and performance are part of the risk assessment tool for public cloud services.

Network availability and performance

Other jurisdictions

Latency is not the only factor when considering jurisdictions. NZ government organisations also tend to use public cloud services that are hosted in:

- the Netherlands
- Germany
- the United Kingdom
- Ireland
- Canada.

Government organisations can use public cloud services hosted in other jurisdictions.

Factors for assessing jurisdictions and service providers

For data sovereignty, there are different factors for assessing jurisdictions and service providers.

Factors — jurisdictions

When looking at jurisdictions, government organisations should consider the following factors.

- Lawful access — the laws that regulate a government's legal access to data.
- Legal institutions — the robustness of legal institutions that oversee a government's lawful requests for access to data.
- Privacy frameworks — the protections available for personally identifiable information.

Factors — service providers

When looking at the providers of public cloud services, government organisations should consider the following factors. They should make sure the provider:

- identifies where customer data is stored and backed up — location factor
- informs its customers when it gets unlawful requests to access customer data — informed factor
- only discloses customer data when required by a warrant — disclosure factor
- dedicates resources to reviewing lawful requests to access customer data — review factor
- deletes customer data after the contract is terminated — deletion factor.

Signs of best practice for data sovereignty

While it's rare to be able to negotiate contracts for public cloud services, the Government Chief Digital Officer's examples of terms and conditions can help you to understand what you should be looking for in contracts.

Terms and conditions for negotiating contracts for public cloud services

Pay attention to what is best practice for NZ government organisations — referred to here as customers. For data sovereignty, it's best practice when the service provider does the following.

Not disclosing customer data

It's best practice when the service provider, in its service terms, commits to never disclose customer data except when:

- directed by the customer
- required by the law
- defined exceptions happen, such as life-threatening situations — the provider should describe the processes that must be followed in these cases.

Processes for government requests

It's best practice when the service provider, in its service terms, defines its processes for responding to government requests. The service provider should:

- always redirect the requesting government to contact the customer — in this case, your government organisation
- if possible, narrow the scope of government demands
- always contact the user when information is released — unless legally stopped from doing so
- disclose only the information that is specified in the legal order.

Resources for reviewing government demands for user data

It's best practice for the service provider to have a dedicated team to review any government demands for user data.

Public reporting

It's best practice for the service provider to report publicly on the:

- frequency of data requests by country
- results of data requests — especially for commercial services.

Security options for data location

It's best practice for the service provider to allow its customers to:

- determine where their content will be stored
- specify the circumstances when it may be moved to another jurisdiction.

Last updated 10 October 2022

Date printed 25 November 2022

Te Kāwanatanga o Aotearoa
New Zealand Government