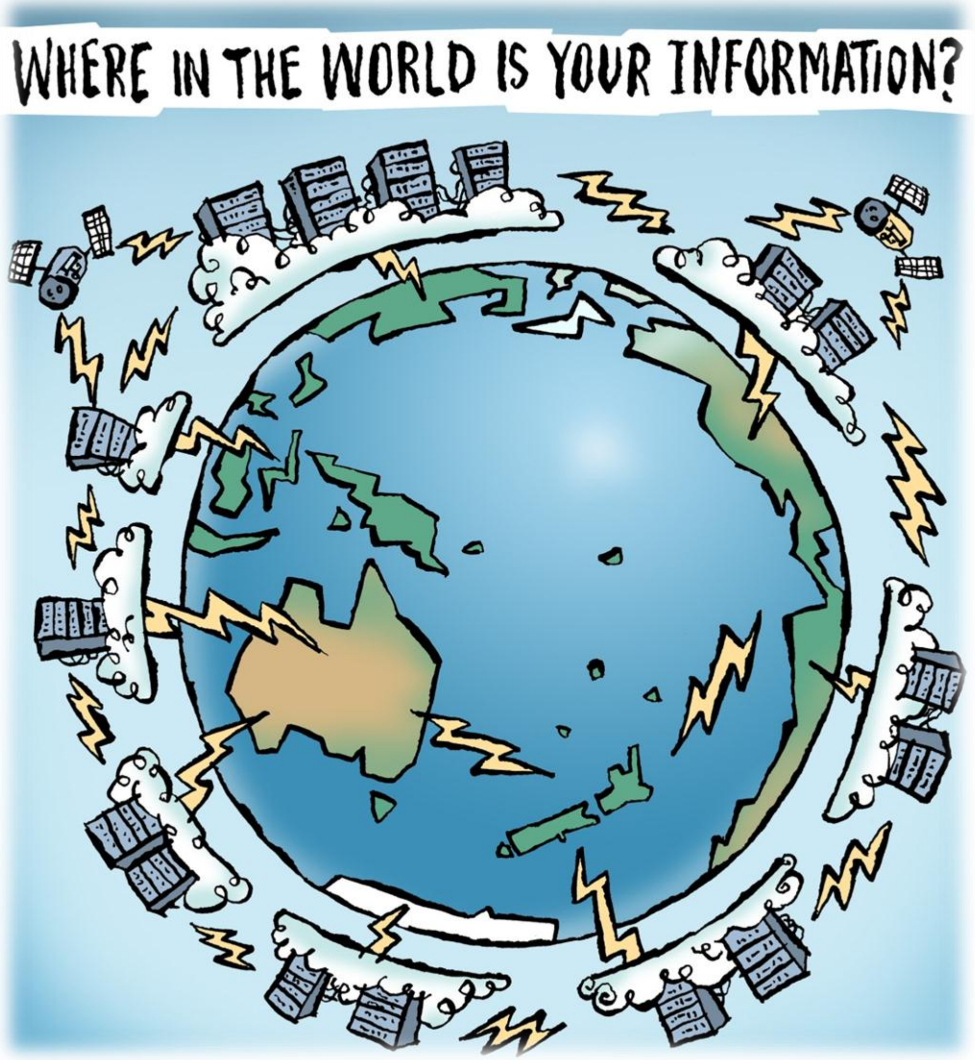
Privacy Commissioner
Te Mana Matapono Matatapu

20 YEARS
PRIVACY ACT
1993–2013
NEW ZEALAND



Cloud Computing

A guide to making the right choices

February 2013

Cloud Computing
A guide to making the right choices

Published by the Office of the Privacy Commissioner
PO Box 10094
Wellington
109-111 Featherston Street
Wellington 6143

ISBN 978-0-478-11737-0

Contents

If you're a business person thinking about using the cloud, read on...

Shifting to the cloud can make good business sense, but there's a lot to weigh up. One question that often worries businesses is whether their client and staff information will be safe if they switch to cloud services.

We've developed a privacy checklist to help you to answer that question. The checklist and its supporting material set out the most important privacy queries you should think about, and ask your cloud provider about.

Why does it matter? Because whether personal information is held on your own computers, in a shared datacentre in New Zealand, or offshore, you've got legal obligations to protect it. Also, your clients trust you to get it right – and loss of trust is loss of business. So it's worth spending some time to think things through.

Let us know if these resources are helpful, or if there is any other information that you need about managing privacy in the cloud.

Contact us:

enquiries@privacy.org.nz or 0800 803 909

http://www.facebook.com/PrivacyNZ and follow us on Twitter (@NZPrivacy).

Cloud computing checklist for small business

1. **Figure out which cloud services will work for you and what your current risk level is**

   Cloud computing comes in many shapes and forms. Know what you need, so you can evaluate your options.

   Different cloud services carry different risks and responsibilities. Think of what risks you currently have with handling personal information. Will using the cloud increase or decrease those risks? The cloud will not always be a riskier option – if you have personal information on a poorly secured server sitting in the back room of your office, it might be safer stored with a trustworthy cloud provider.

2. **Know what information you'll be sending to the cloud**

   Work out what information you'll be putting into the cloud, so you know what to focus on and what you can relax about.

   If none of the information is personal information, then privacy isn't an issue.

   If some of it is personal information, could it harm your clients if the information was lost, deleted, stolen or misused? The more harm it could cause, the more care you have to take to check it's protected.

3. **Recognise that the responsibility is ultimately yours**

   All cloud services involve trusting someone else with your clients' personal information to some extent. Your cloud provider might have some responsibility for handling the information safely – check the contract. But if you're putting client information in the cloud, you're still responsible for it. The buck stops with you. Period.

4. **Security - lock it down**

   Make sure the information is protected both while it travels and when it's at the provider's end. Encrypting your data is the easiest and most reliable way of doing this. If it's encrypted, it's unlikely to get misused, or to cause harm if it gets hacked or lost. So encrypting the information takes a bit of pressure off you.

5. **Check out your provider**

   Do an internet search on the cloud provider you're thinking of using – along with words like "breach" and "privacy". If the provider has had problems in the past, it might show up. Check how well they dealt with things. Are they regularly and independently audited?

New Zealand-based providers may be signed up to the Institute of IT Professionals (IITP) CloudCode, which requires them to provide information on a set list of important issues.

6. **Know exactly what you're signing up for**

You may not have much clout when it comes to negotiating contract terms, but you probably have a choice of providers – compare the protections they're able to offer.

Be clear about what the contract says. You don't want things to fall through the cracks. For instance, make sure you know what will happen if the provider goes under, or is bought out. Where will your information go? What if there's a data breach – will you get told?

7. **Be as up front with your clients as you can**

Wherever you can, tell the people concerned what you're doing with their personal information. Also, work out how you would respond to a customer's request to see information about themselves.

8. **Location - where will the information be?**

If possible, work out where your information is going and what privacy laws apply.

Not all providers will tell you where their data centres are. But at least make sure that they tell you how they deal with government requests, whether they demand a search warrant before giving access to information on their servers, and your rights to be notified if they pass the information on to somebody else. Also find out who you would complain to if something goes wrong.

9. **Use and disclosure – who sees the information and what will it be used for**

Make sure you know if your cloud provider will be passing the information to a third party. It's very common for cloud providers to contract out key parts of their services. The protections for the information should be equally strong whoever is providing the service. What come-back do you have if the third party contractor stuffs up?

Who will be able to see or use the information? Make sure you know what the provider will be doing with the information (if anything).

10. **Ability to exit, and deleting information**

Can you get the information out, in a form that you can use, if you decide to switch providers? Will the provider delete the information or will they try to keep it?

What do we mean by cloud computing?

If you're sending personal information outside your business to overseas servers or if you're storing it with a third party within New Zealand, this guidance is relevant to you.

Cloud computing comes in many different forms. It can involve storing your information with another company. It can involve a full replacement for desktop software, or just some space on a server.

What matters in terms of privacy is what is happening to the information – where it goes, where it's stored, who can see it and who can use it.

Formal definitions of cloud computing tend to be technically complex. The reason for this is that there are numerous computing solutions that can bear the name "Cloud".

In practice, you might not care whether you're using something that's technically "the cloud" or not. The services are just part of your business. But if you are after a formal definition, the National Institute of Science and Technology in the US has one that is broadly accepted by most cloud providers. That's available here: (NIST link). The IITP CloudCode also provides a simplified version of the NIST definition designed to be more easily understandable by a non-technical audience (IITP link).

What is “personal information”?

The Privacy Act covers “personal information”. If you’re using personal information in your business, whether in the cloud or not, you need to comply with the Privacy Act.

> Personal information is any piece of information that relates to a living, identifiable human being. People’s names, contact details, financial, health, purchase records: anything that you can look at and say “this is about an identifiable person”.

Even if their name doesn’t appear, it could be personal information. The question is whether there’s a reasonable chance that someone could be identified from the information. Also, it does not need to be “secret” or “sensitive” – it just needs to be about them.

Information about your business practices or policies, your trade secrets, and aggregated statistical information that cannot identify individual people will not usually be personal information. It may be confidential or commercially sensitive, so you may still want to protect it. Some aspects of this guide may give you an idea about how to get there. But the Privacy Act isn’t relevant.

The bottom line – you’re responsible for the information you put in the cloud

If you use a cloud service, you’re still responsible for what happens to the information. If there’s a privacy breach, you’re going to be the one answering the questions about what went wrong.

Specifically, it’s your responsibility to make sure that personal information:

- is stored safely
- is transferred safely
- can be provided if the subject of the information asks to see it
- can be corrected if the subject of the information thinks it’s wrong
- is destroyed when it is no longer needed
- isn’t misused
- isn’t improperly disclosed to someone else.

These guidelines focus on helping you manage these responsibilities in the context of cloud computing and other information technology outsourcing.

For most businesses, the staff are the key to handling personal information properly. Figure out what your staff need to know. Talk to them about your move to the cloud, and what’s involved. Give them any training or advice they need so they can help you keep personal information safe. If you need help from us, check our website or contact our enquiries line (0800 803 909) or email enquiries@privacy.org.nz.

For example, you might have a policy that information needs to be encrypted when you send it to an outsourcer or cloud service provider for processing or storage. But if that’s not done automatically, or your staff aren’t trained to make sure the information is encrypted, mistakes are inevitable.

What do you have to do to keep information secure?

Because IT outsourcing, including cloud computing, involves dealing with a third party – and therefore sending personal information outside your organisation – you need to make sure that the information is secure both while it's in transit and when it's stored.

Be clear on which aspects of security are your responsibility and which are the provider's.

<u>What the provider should tell you</u>

- Whether the data is automatically encrypted when it is being transferred between your organisation and the cloud provider. All personal information should be encrypted in transit – even supposedly "non-sensitive" information like name and date of birth is valuable for identity theft. If the provider does not include encryption for data in transit, you need to find a way to encrypt it. Most providers at least give the option of a secure socket layer (SSL) connection.
- What commitments the provider makes about the security of its datacentre , for example:
    - the measures that it takes to ensure physical and digital security (the Cloud Security Alliance Cloud Controls Matrix provides a comprehensive list that you can ask providers to respond to)
    - the independent audit or certification process that the provider undertakes and the results of those tests (there are internationally recognised standards in place, such as ISO/IEC 27001).
    - are these certifications current and do they require independent verification? Some certifications do not require any independent assurance, and therefore may be of limited value
    - what other technical protections they have in place (for example EAL4+ certified firewalls and "hypervisors" are common features)
    - what physical security measures they have – for example do they have surveillance, guards or restricted access?

What if it all goes wrong?

If things go wrong for some reason, you need to know how to deal with it. Have a clear understanding of what your rights and responsibilities are and how any problems will be addressed.

Check the contract. Make sure your key concerns are covered in the contract (if you have the ability to negotiate) or in the standard terms and conditions.

In particular, check that you know:

- whether the provider has to tell you if something goes wrong (for instance if there is a security breach)
- how you would notify your customers if their data is lost or stolen
- how you're going to know whether the provider is living up to the terms of the agreement (for example does it get regular independent audits done that you'll be able to check?)
- who is liable and what the penalties are if something goes wrong
- what country's law applies if there is a legal dispute and who the appropriate regulator might be?
- whether mediation or arbitration is available. This might be cheaper and more practical than going to court
- whether your provider is insured against privacy breaches
- what the provider's disaster recovery plan covers.

Tell people what’s happening if you can

It’s vital to maintain your relationship with the people whose information you hold. They have entrusted you with their personal information. You need to be able to assure them that it's being looked after. If you let them down, you’ll lose their trust – and quite probably their business.

So keep them in the loop. If possible, tell them up front if their information will be held offshore and where their information is going. That’s an opportunity to tell them that you’ve checked it’s secure, that it won’t be misused, and that you can get it back whenever you need it.

If it’s not practicable to tell people – for example because it’s too confusing – at least have a privacy policy that sets out what you’re using cloud computing services for. You can put that policy on your website and also have it ready to show people when they ask.

How to handle customer requests

People are entitled to see and correct the information you have about them. So you need to make sure that if someone asks to access their information or correct it, that you can do this easily. It doesn't matter where in the world that information happens to be stored. You have to respond to a request as soon as you can – and at most within 20 working days.

This shouldn't normally be a problem, but there are some cloud products that are designed to make some personal information difficult to access. In these situations you'll need to work out how to deal with a request to access or correct information.

Some services may enable customers to access their own information securely.

If you aren't sure that you can access the information when you need to, you may need to rethink your choice of provider.

<u>What you will need to work out</u>

- where the information can be accessed from so you know how to retrieve it easily without incurring any retrieval charge
- how to retrieve information if you need it
- how long it will take to retrieve information
- how to alter the information if you have to make changes
- whether you can add notes to the records and where the note will sit. (If you disagree with a customer's view of what's correct, you don't have to change the information. But you do have to note their view alongside the information so it can all be read together).

Does location matter?

One of the benefits of cloud computing is that information can be mobile. It no longer has to be restricted by your current computer hardware. But sending personal information to another business for processing or storage can change which laws apply, as well as raising the possibility that others might be able to legally access the information.

For example, if a cloud provider does a significant amount of business overseas, the provider could be subject to overseas laws as well as New Zealand laws, even if the information is kept within New Zealand. Alternatively, if the provider doesn't have a significant presence in New Zealand it could be more difficult to enforce New Zealand laws. Different legal rules may apply depending on which country the information is in and your responsibilities may differ as a result. Location can sometimes affect the kind of relationship you can have with your cloud provider, and your options for sorting out any problems. Some countries may also raise different kinds of risks that affect the security of your data, such as the country's levels of corruption.

Of course, location could be a non-issue. The cloud provider might have the same procedures no matter where the information is located. It might only disclose information under a search warrant or court order. But it's worth asking. You're the one who needs to make the judgment about whether the location of the information will create risks that are unacceptable for you and your customers.

So try to find out where your information is going to be held and what laws apply, in case there are any fish-hooks. Have a look at the terms and conditions and ask any further questions that you need to.

Your cloud provider should be able to tell you where its data centres are. They might not be able to tell you exactly which data centre your data will be in though, because they may want to move it around in order to optimise their service.

What the provider should tell you

- whether there is a privacy law that applies in the country or countries where your data is stored or processed
- whether that privacy law is similar to New Zealand's privacy law
- whether the law applies to the cloud provider and to your information (some privacy laws exempt some types of businesses, or do not apply to the personal information of foreigners)
- how the cloud provider will deal with any requests for information that it receives from government agencies, courts etc. For example will the provider only disclose information in response to a court order? Will the provider let you know if it has to disclose information in response to a request?
- will the cloud provider notify you if data is lost or stolen, for instance if the provider is hacked?
- who can you or your clients complain to if there's a breach of privacy?

It's useful to have your information located in countries with similar privacy laws to New Zealand's because it's more likely that if there is a problem, there will be an effective means of sorting it out. In some jurisdictions you or your customers will be able to lay a privacy complaint directly with the local privacy commissioner. This makes it harder for your cloud provider to shirk its responsibilities.

If there isn't a local privacy law, you may need to make sure that equivalent privacy protections are specifically built into your contract with the cloud provider.

The Privacy Act says that you won't breach New Zealand law if local laws require disclosure of personal information. But you won't know if this is relevant to you unless you've checked it out. Your customers may see any disclosure of information as a breach of trust, particularly if a foreign government is involved. So, once you understand how your provider would handle any requests for information, it's a good idea to tell your customers too.

How much information does your provider see?

Your cloud services solution might not involve the provider accessing your information at all.

Some access to information will be relatively innocuous – such as automatically shifting files around to optimise performance.

But you need to ask. You’re not on the spot, so you can’t control things directly – you’re reliant on the provider to get it right. Your customers trust you to make sure their information is properly protected.

Any use of personal information should be directly related to the purpose for which you’ve got the information in the first place. If it’s being used for a new purpose, that should almost always be authorised by the person the information is about.

What the provider should tell you

- what purposes the provider may need access for, if any?
- are optimisation or other analytical processes carried out by the provider’s staff, or are they automated?
- which staff have access to the information?
- how is that access controlled and monitored?
- does the provider maintain an audit trail for who accesses the information and what for?
- can the provider use your information to develop its own products or for its own commercial gain - such as collecting statistics from your data to sell as a product to others?

Where are the exits?

At some point, you may decide that you no longer want to use a particular cloud provider. Whatever the reasons for this, you need to be able to get your information out and make sure that it’s no longer retained on the provider’s servers once you’re gone.

What the provider should tell you

- whether you can take the information with you if you choose not to use the service any longer
- whether you will get the information in a format that you can use elsewhere - and how quickly the provider will get you the information
- who will bear the cost for the process of switching to a new supplier
- whether your information will be kept on the provider’s systems after you move on, or whether it will be securely deleted. For instance, many providers will hold backups, which will keep records for a certain period even once an account is deleted
- how the provider will verify for you that the information has been deleted