Complying with Australian data sovereignty rules in the age of the cloud

Introduction

Where in the world is your cloud data?

That is a key question many companies and organisations are struggling to answer. When we use a service like Dropbox, Google Drive or iCloud we all know that the data is stored ‘in the cloud’, but what or where does that mean?

It is becoming more important to clearly know where your cloud data is stored.

The data you save to the cloud may not be physically stored in an Australian data centre. This could create legal or regulatory challenges for your business, in particular under the laws and regulations set out in the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APP). What does privacy law have to do with storing data in the cloud? Privacy law is highly relevant due to the legal concept of ‘data sovereignty’.

‘Data sovereignty’ is a term and a concept that is becoming more important for your business to understand.

Where in the world is your cloud data?

Laws around privacy and data sovereignty mean it's becoming more important to know and manage where your data is stored.

Developed in Melbourne, Australia by
network2share
Deploy. Empower. Sell.

What is data sovereignty?

Data sovereignty is:
The concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located.

In practical terms this means that even if you conduct business in Australia, the information that you are uploading to the cloud could be subject to the laws of a different country, if the data is physically stored on a server in that country.

What are data sovereignty rules in Australia?

Data sovereignty rules in Australia are largely reflected in Section 5B of the Privacy Act 1988 (Cth). Under this section of the Act, it states that the Australian law and approved privacy codes or guidelines apply to an action done outside of Australia by an organisation if that action relates to personal information about an Australian citizen.

The volume of data covered by the definition of 'personal information' is vast. Under the Act, this covers:
• …information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable

This definition is extremely broad, so the Act further breaks the concept of 'personal information' down to include any information about an individual that is specific to their legal existence, including, but not limited to, a person's:

• Name • Signature • Address • Date of birth • Telephone number • Driver's licence • Tax return • Medical history • Bank account • And more

Further to the definition of personal information under the Act, Chapter 8 of the APP covers the cross border disclosure of personal information. Key points of Chapter 8 state:

• Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1).
• An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (s16C).

Could our cloud storage breach the Privacy Act?

If your company is using a cloud storage service like Dropbox, Google Drive or OneDrive it is possible that your data covering the personal information of Australian citizens is stored outside of Australia.

This is clearly outside of the definition of data sovereignty and in breach of the Privacy Act 1988 (Cth) and the Australian Privacy Principles. This is because you do not know if the organisation you have shared the data with has breached the APPs and because you can't always control what another organisation does with data you have provided to it, particularly when that organisation takes a step that breaches the APPs.

Additionally, if you are using these services in your business, your company could be liable for any act taken by an overseas provider that you use to store and manage your client data. This includes any 'misconduct' which the Privacy Act defines as "… fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty".

So, if you are using these cloud storage services, you need to ask yourself these questions:
• Are we in breach of Australian data sovereignty laws and regulations?
• Have we disclosed personal information to an overseas recipient?
• Has this recipient breached, or could this recipient breach, the Privacy Act or the Australian Privacy Principles?

What are the legal and financial implications of breaching data sovereignty rules in Australia?

Any breach of the rules discussed in this document opens an organisation up to the possibility of civil law and other punitive compensation penalties (civil penalties of up to $AU 1.7 million apply for serious or repeated breached of the Privacy Act).

This is compounded by the likely impact from loss of business should your company be found to have compromised its own data or the sensitive data of its clients.

The reputation and standing of your business would also be impacted if you are in breach of the Privacy Act or the Australian Privacy Principles. Breaking these laws and principles means you have broken a commitment to your clients around safely managing and storing their sensitive data.

Would you do business with a company that had breached its clients' trust in this way?

Other considerations around data sovereignty

This Whitepaper provides a brief overview of data sovereignty considerations in Australia. The laws around data sovereignty are complex and cannot be easily broken down and summarized, so it is best that you familiarise yourself with the Privacy Act and the Australian Privacy Principles.

It is also advisable that you discuss any questions or concerns around data sovereignty laws with your organisation's legal advisor.

Other considerations about data sovereignty and how these laws and regulations apply to your organisation include:
• Do you have the resources to manage a data-related incident, such as a breach, if something happened to a client's data in an overseas jurisdiction?
• Do you have business processes in place to manage client complaints relating to a data breach?
• Do you have legal resources in place to manage complaints relating to a data breach where that data was held in overseas storage?

Compliance with data sovereignty laws in the age of the cloud

Network2Share's mission is to give companies and organisations a secure way to access and share their data across a number of devices and platforms. As a part of this, our CloudFileSync tool provides full visibility over who accesses and shares files and over who the files are shared with. We are providing businesses with a tool that helps them to regain control over their own data.

Regaining control of your data also means knowing where your data is stored. Companies can deploy our CloudFileSync secure file sync and share solution on top of in-house private cloud, meaning the data is physically stored on a server in the company's own building.

As an alternative, companies can purchase hosted storage from the CloudFileSync Marketplace, always knowing where this storage is physically located.
We are clearing the fog from the cloud, helping users to know exactly where their data is stored, and helping them to purchase cloud storage in their own country so that they comply with data sovereignty laws.

If you have any questions about data sovereignty, the cloud and where your organisation's data is stored, please contact regan@network2share.com