

## **Will Cloud Computing Bring Stormy Weather When Protecting Personal Information?**

In our digital world, individuals and businesses are increasingly reliant on technology to efficiently conduct business. Cloud computing is one such technology. It offers businesses an alternative, low cost means for storing and processing information.

### **What Is Cloud Computing?**

Cloud computing is a technology that uses the internet and remote servers to store information and applications. It allows businesses to use applications without the need for installing their own business software on their own hardware or heavy investment in IT infrastructure.

### **Privacy Act 1993**

Under the Privacy Act 1993, businesses have significant obligations about how they collect, store and use personal information. 'Personal Information' is information that relates to any living identifiable human being.

Using a cloud computing system does not remove obligations in respect of protecting personal information. In fact, it can make compliance with their obligations more difficult, in circumstances where personal information will be controlled by a third party, which may be located offshore, and subject to different privacy rules (if any).

The Law Commission, which has addressed the issue at Chapter 10 of a recently released a final report of its review of New Zealand's privacy laws, has recommended that the Privacy Act 1993 be amended, making it clear that New Zealand agencies will remain fully responsible for personal information that is sent to a third party that is offshore. Consequently, businesses can expect further development of the law in this area.

### **Practical Considerations to Minimise Risk**

In the meantime, things to ask about when considering a cloud computing solution as they relate to personal information include:

1. **Location.** One challenge with information processed in the cloud is that it's not always possible to identify where the information is to be stored. Ascertain as best as possible the location of the cloud computing service provider and the server where the information is to be held.
2. **Security.** Ask the cloud computing service provider about what controls are built into its system for security and privacy of the information it holds.
3. **Internal compliance.** Create rules about own staff access to the information, and how access security will be maintained.
4. **Use and disclosure.** Find out what information can be seen by the cloud computing service provider, who can see that information, and how that is controlled.
5. **Information access and availability.** Ask about the cloud computing service provider's policies about transfer and access of information, and its disaster recovery procedures.

6. Termination. Understand the cloud computing service provider's contract provisions about how personal information will be returned when the service contract terminates.

Cloud computing has the potential to offer businesses a number of benefits in managing computing and information needs. However, cloud computing is still a relatively new concept. Continual development of technologies will be necessary to improve the reliability and security of cloud computing services.

Businesses that choose to store personal information on an off-site server will remain responsible under the Privacy Act to ensure the security of that information. This is a challenge associated with cloud computing, and businesses intending to use a cloud computing service will need to make full enquiries of the service provider to ensure that the service agreement adequately addresses information privacy obligations.