Do you know where your data is stored?

Why data residency for cloud systems is vital to your compliance with data privacy laws.

Compliance with Australian data privacy regulations is a non-negotiable requirement for Australian schools. This is why it is important for your school to ensure that your cloud based systems comply with Australian Data Privacy Laws. Breaching your data privacy obligations may not only leave your school open to significant financial penalties, it also exposes your school to serious reputational damage.

The specific Australian privacy laws which your schools must ensure compliance to are:

1. **Commonwealth of Australia Privacy Act 1988**

   This Act regulates the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information, plus access to and correction of that information.

2. **The Privacy Amendment Act**

   This Act came into effect in March 2014 and it introduced many changes to the original Privacy Act. It included a set of new principles that cover the processing of personal information by government agencies and private business. The new principles are jointly called the Australian Privacy Principles (APPs).

Why Cloud data residency is important.

In the context of cloud data storage, Australian Government Agencies and private businesses dealing with personal information are subject to APP8 (Cross-border disclosure of personal information). This regulates the disclosure and transfer of personal information offshore (to non-Australian Territories).

Before permitting the movement of personal data offshore, an Australian Government Agency or private business **must** take reasonable steps to ensure that the overseas recipient will comply with/not breach the APPs.

Your liability cannot be transferred. Your school remains liable for any breach.

It is important to understand that the liability for any breach of The Privacy Amendment Act for any data that is stored offshore remains at all times with the school, even if reasonable steps have been taken to ensure compliance with the Act. Permitting the overseas storage of private data means that your school is exposed to risk and liability regardless of any steps taken to ensure data security by your provider. In particular:

- The Australian Sender of personal data to offshore locations will remain liable for the overseas recipient's acts associated with any transferred personal information and, where relevant, be in breach of the APPs due to any of the overseas recipient's acts or omissions.
- In addition, APP11 (Security of personal information) requires that an organization must "take reasonable steps to protect information it holds from misuse". Where data is stored with providers in jurisdictions which are not governed by Australian Privacy Regulations then protecting data from misuse can be more complicated.

REACH guarantees that all cloud data storage for Australian schools is stored only in Australia. In addition, all backup data for Australian schools is stored only in Australia. This is recognised best practice which eliminates the risk and exposure to unforeseen liability which is associated with APP8 when personal private data is not stored in Australia. REACH also offers schools the option to self host your REACH database on your own campus.

www.reachboarding.com