



## MEMO

To: Board of Directors  
From: Company Secretary  
Subject: **DATA PROTECTION LAWS**

---

As discussed at last board meeting, because our business provides a service to the public on-line, and 'the public' load up personal data to facilitate transactions, then we need to be very careful not to allow any 'hacker' to access that information (and maybe use it 'inappropriately').

This is important for all companies, particularly in light of the hacking of the accounts of 77 million Sony PlayStation Network users world-wide. Australians accounted for 1.6 million of those users affected.

It is incumbent on all organisations to notify individuals when their personal data has been compromised.

In fact, governments in various jurisdictions have introduced or are considering reforms to privacy laws and amended legislation in relation to mandatory data controls and breach notification laws.

### **Privacy Breach Register**

Also, companies should maintain a "Privacy Breach Register" and keep track of any formal complaints whether written or phoned-in specifically relating to any privacy breaches.

### **Applicable Legislation**

Australia has a very developed set of general data privacy principles at the federal (national) level which are broadly consistent with the principles in the EU Data Protection Directive. These principles apply to the federal government, the medical sector and the private sector generally (subject to a turnover threshold).

The principal Australian legislation is the Privacy Act, which is supported by various state legislation and guidelines, such as the Privacy and Personal Information Protection Act in New South Wales.

There are also industry specific rules and Codes of Practice for banking, medical services, e-commerce and telecommunications.



## **Protected Data**

Under this legislation information or opinions (“personal data”) about a living individual whose identity is apparent or can be reasonably ascertained (“identifiable person”) is protected. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or by one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

An even higher degree of regulation applies to “sensitive information” relating to a person’s race, political opinions or association, religious or philosophical belief, union membership, sexual preference, criminal record, health or genetic information.

---

### **DISCLAIMER**

*The comments in this memo reflect some commercial aspects and observations on the matter experienced or observed by the writer in practice as he understands them. The information is given as a guide only and does not represent a definitive or legal view of any of the issues raised, covered or referred to and the reader is urged to seek his own professional advice on all aspects of, or pertaining to, this and any related matter.*