SECURITY REQUIREMENTS

What security obligations are imposed on data controllers and data processors?

Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, prevent alteration, corruption or access by unauthorized third parties.

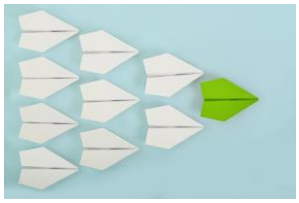
Appropriate technical and organizational measures should be implemented to ensure a level of security appropriate to the risk. In Australia, the data security obligations in the Privacy Principles (APP 11) apply to any entity that holds Personally Identifiable Information (PII). Employers should take reasonable steps to protect PII from: misuse; interference and loss; and from unauthorized access, modification or disclosure. Reasonable steps should be determined by the entity based on:

- the sensitivity of the information;
- the volume of the data; and,
- whether the entity is similar to a data controller or a vendor/subcontractor

The Taxation Administration Act 1953 and the Income Tax Assessment Act 1936 govern the collection, storage, use, disclosure, security and disposal of an employee's tax file numbers. Employers and any third party 'approved recipient' must take reasonable steps to protect employee tax file number (TFN) information from misuse and loss, and from unauthorized access, use, modification or disclosure.

Employers and approved recipients must also ensure that access to records containing TFN information is restricted to individuals who need to handle that information for taxation, personal assistance or superannuation law purposes. Employers and approved recipients must also ensure all staff are aware of the need to protect privacy when handling TFNs, and that staff who collect TFN are aware of:

- the circumstances when TFN information may be collected;
- the prohibitions on the use and disclosure of TFN information;
- the need to protect privacy (including under the TFN Rule and the Privacy Act); and,
- the penalties or other sanctions for breaches of TFN privacy laws.



HR Best Practices:

Take all appropriate security measures based on the sensitivity and confidentiality of the data. Educate employees and other individuals who have access to data on security standards, especially those who have access to TFN information. Take reasonable steps to ensure they comply with security procedures.

Last updated June 2020.