



Implementing Privacy Data Security

Evado's Privacy Data Security Implementation service assists companies to implement the management practices needed to ensure that they meet the new regulatory requirements.

KEY FEATURES

Gap analysis to identify policy and privacy risks.

Development of a plan to address the identified issues and risks.

Implementation of the remediation plan.

KEY BENEFITS

- Understand your data breach risks.
- Reduce the risk of a data breach.
- Have appropriate plans and processes place to handle a breach should it occurs.
- Improve your company's IT security management practices.
- Reduces the risk of unauthorised IP disclosure.

Are you ready for the Privacy Act changes on 22 February 2018?

The new Australian privacy data security and mandatory breach requirements come into force on 22nd February 2018. These changes affect all companies with a turnover of more than 3 Million or companies of any size that handle sensitive personal data (e.g. health records). These companies must comply with data breach requirements or risk heavy penalties and potential reputational damage.

Evado offers a comprehensive affordable consultative approach to implementing a privacy policy, beginning with a gap analysis through to implementation of privacy policies & procedures.

All affected companies must as soon as possible notify the Office of the Australian Information Commissioner (OAIC) and all of the affected individuals if a "reasonable person" believes that any of those individuals affected are likely to suffer "serious harm" because of the data breach.



All affected companies remain liable and responsible (i.e. they must notify) data breaches that occur in respect of personal information that has been disclosed to third parties (including group companies) overseas.

An affected company's privacy management and compliance needs to be mature and best practice. Any data breach involving sensitive information or large amounts of personal information should be considered a data breach requiring notification.

The OAIC expects affected companies to have:

- Defined privacy policies
- An appropriate privacy management plan (PMP) in place
- Data breach response plan (DBRP) to handle a data breach should it occur
- Have taken appropriate steps to secure all privacy related data to minimise the risk of a privacy data breach.

Evado Pty. Ltd.

Level 7, 171 Collins Street Melbourne VIC 3000
T: +61 3 9600 3616 e: info@evado.com w: www.evado.com
ACN: 138 226 927

A U S T R A L I A

U N I T E D S T A T E S

S I N G A P O R E



Australia's privacy law

The main privacy law in Australia is the Privacy Act 1988 (Cth) which includes the Australian Privacy Principles (APPs).

The Privacy Act and Australian Privacy Principles (APPs):

- Regulate the collection, use and disclosure of "personal information" (including "sensitive information", Tax File Numbers and credit information) by all APP entities being:
 - Federal public sector agencies
 - Private sector organisations.
- Companies with a revenue greater than \$3 million or who handles sensitive personal data (e.g. health records) are required to comply with a set of privacy principles (the APPs), a breach of which constitutes an interference with privacy.
- All relevant companies (APP entities) must implement relevant monitoring and business processes to handle data breaches and report significant breaches to OAIC by February 22, 2018.

What the regulator expects to see

A privacy management plan or framework including a cyber-risk management plan (PMP) is a cost effective way of creating a good privacy/information security governance that:

- Embeds a culture of compliance
- Establishes robust processes
- Is evaluated regularly
- Enhances responses to issues.

Evado's consulting approach

The Evado consulting approach has been designed to assist companies to implement management practices that will meet the new data breach management and reporting requirements.

- Gap analysis:
 - Privacy and data security policies
 - Privacy management plans and procedures
 - Corporate data security plans and procedures
 - IT data risk management
 - Monitoring of IT security
 - Plans and procedures for managing data security breaches.
- Assists companies to develop an action plan to address the issues and risks identified in the gap analysis.
- Assists in the implementation of appropriate management policies, plans and procedures to meet the new mandatory breach requirements, which could include:
 - Updating corporate policies and procedures
 - Developing specific cyber and data breach management processes
 - Implementing staff IT and cyber awareness training
 - Updating IT security policies
 - Updating IT security procedures and processes
 - Implementing pro-active cyber security monitoring.

Evado Pty. Ltd.

Level 7, 171 Collins Street Melbourne VIC 3000
T: +61 3 9600 3616 e: info@evado.com w: www.evado.com
ACN: 138 226 927