Boardroom Questions

Data Privacy

Why privacy is an important business consideration

OAIC Australian Community Attitudes to Privacy Survey 2017

60%

of people are either 'concerned' or 'extremely concerned' about the way companies handle and use their personal data..

79%

of people are uncomfortable with businesses sharing their personal information with other businesses.

58%

of people have decided to avoid dealing with a private company because of privacy concerns.).

Many organisations face challenges in protecting personal information from theft, intentional disclosure or mishandling. Proactively managing privacy risk and regulatory change helps ensure your customers, staff and other stakeholders trust you to treat their information appropriately.

Personal information is an important strategic asset for any organisation. Organisations must comply with local and global privacy legislation, but also compete to become market leaders through a responsible and innovative use of personal information.

Australian and global privacy laws require most organisations to make publically available their privacy policies, provide privacy collection statements, ensure internal privacy processes are compliant and manage their third party and software vendors.

Failing to manage personal information appropriately may result in harm to individuals. This can lead to significant reputational damage, loss of staff and customers. Classifying and mapping data and keeping data according to retention periods is key to ensure good data quality and minimising risk of data breaches.

Managing the consequences of a privacy breach can be devastating and costly, especially with GDPR enforcing fines of up to 4% of annual turnover. Putting in place a privacy framework helps to ensure you are doing your best to safeguard the privacy of information in your care.

Why business need to review their privacy strategies

New and emerging regulations such as the Notifiable Data Breach (NDB) scheme under the Privacy Act 1988 (Cth), the General Data Protection Regulation (GDPR), the Consumer Data Right (CDR) and Open Data regime, have increased the standard on privacy and data governance and management, data security and organisation-wide data awareness and culture.

Major privacy incidents and data breaches have increased community, regulator and government scrutiny on organisations' privacy practices. Globally, regulator actions and fines for non-compliance are increasing.

Potential impacts and risks

1. A strong privacy management framework helps organisations unlock the value of data, improving customer experience and securing competitive advantages while reducing the privacy risks associated with data usage.
2. As more products and services are delivered and managed by third party vendors, both locally and internationally, privacy management moves further away from organisation's control and becomes increasingly difficult.
3. Customers expect organisations to fulfil service and product obligations and remain competitive and profitable whilst protecting their privacy interests.
4. Regulatory changes including the introduction of the Notifiable Data Breach Scheme in Australia, as well as the General Data Protection Regulation (GDPR) in the EU, have resulted in increased scrutiny on privacy management for organisations around the world.
5. Poor privacy management and data breaches can do significant damage to an organisation's brand and reputation.
6. The costs associated with the fallout from non-compliance can frequently be far greater than the cost of investing in compliance activities.

Boardroom Questions

1. Do we understand our business's privacy obligations and risks?
2. Does our organisation have a fit-for-purpose privacy compliance strategy?
3. Are we making sound decisions and plans with regard to technology and business transformation initiatives involving personal information?
4. Do we have a clear view of what personal information the business collects, how it is being processed, by whom, and for what purpose?
5. Does the business have strong information management, security, retention and destruction processes and policies?

Actions for Boards to consider

1. Develop a privacy management framework incorporating appropriate governance mechanisms
2. Understand your organisation's privacy risks and risk appetite.
3. Know what personal information your organisation holds, including information held or processed by third party suppliers on your organisation's behalf.
4. Ensure that policies, processes and procedures are in place in your organisation to manage privacy risks.
5. Ensure staff at all levels understand their privacy obligations.
6. Establish monitoring systems for identifying and reporting privacy and information security incidents.

Contact us:

Kelly Henney
National Leader, Data Privacy Services
KPMG Australia
khenney@kpmg.com.au