Regulatory & Compliance Advisory Services – Privacy

The Australian Privacy law has changed and organisations need to be compliant immediately.

The new law requires organisations who generate more than AUD 3 million annually with an Australian link to make changes to their privacy policies, privacy collection statements, internal privacy processes and reconsider their third party and software vendors. For serious non-compliance, penalties of up to AUD 1.7 million for organisations and AUD 340,000 for individuals apply.

Major changes

- Increased obligations on both Federal Government agencies and private businesses that collect or deal with personal information in Australia or from Australian residents.
- Privacy policies and privacy statements must contain certain new key provisions.
- An entirely new privacy regime for direct marketing.
- Transfer of personal information outside Australia needs to be done in accordance with the new regime and specific notifications given to individuals. This is particularly relevant in the use of cloud computing, IT outsourcing and managed services arrangements.
- There are new obligations for the treatment of unsolicited personal information. This has implications on the use and monitoring of social media.
- Part IIIA of the act enables more comprehensive credit reporting. This is accompanied by stricter requirements for credit-related personal information. That is information about individuals activities in relation to consumer credit. Stricter rules on data security have been introduced, including organisations having to provide evidence of external security audits to credit reporting agencies.

Our approach

To find practical and commercially realistic solutions to privacy and data issues, with a focus on helping organisations to strategically enhance data value and use, while minimising legal and reputational risks. For example, this could include streamlining business processes and simultaneously reducing possible points of private data exposure.

Well established methodologies

Dedicated resources working with clients to effectively manage compliance risks

Compliance, risk & operational professionals, auditors, lawyers and regulators

Broad industry experience with variety of approaches to compliance

Extensive working knowledge of the legislation and regulatory requirements

Global networks with access to the latest information and industry developments
Why select us?

- **Privacy framework and strategy** – Australian Standard for Compliance Programs AS3806 and industry benchmarking, design and implementation of effective privacy compliance arrangements and extensive Regulator and External body networks
- **Privacy and data security** – data matching, offshore outsourcing, international data transfers, regulatory investigations, identity verification, compliance reviews, surveillance and monitoring, communications interception, health privacy, credit reporting, tax file numbers, employment privacy
- **Marketing privacy** – spam, telemarketing, direct mail, market research, call recording, do not contact
- **Online privacy** – cloud computing, cookie compliance, online behavioural advertising, mobile device and application compliance, social media
- **Data security** – preventative security, data breach incidents investigation
- **Information access requests** – subject access requests, freedom of information
- **Complementary professional experience** – technology, banking, superannuation, employment, health, energy, telecommunications, education, consumer protection, document management, confidentiality, contract compliance, impact assessments, process simplification

How we can help

We have experience assisting clients in the following activities:

- privacy risk and compliance framework assessments
- gap analysis of the privacy landscapes, systems and processes against the new principles and broader privacy laws
- process mapping the flow of data, overlaying processes with privacy law obligations
- reviewing and updating privacy policies and collection statements
- preparing obligation registers and compliance plans
- updating compliance manuals and privacy training
- data flow/storage analysis, including preparing information security strategy, assessment and cloud computing vendor selection
- assisting with third party and software vendor selection against privacy law requirements
- preparing data security audits to satisfy credit provider requirements
- software application assessments and penetration testing, including identifying and assessing the privacy and risk implications of mobile applications.

Contact us

**Mike Ritchie**  
Partner  
+61 2 9335 8251  
+61 0410 606 417  
mikenitchie@kpmg.com.au

**Angela Jaric**  
Associate Director  
+61 3 8626 0929  
+61 0419 157 843  
ajaric@kpmg.com.au

**Mark Tims**  
Partner  
+61 2 9335 7619  
+61 0412 254 142  
mtims@kpmg.com.au

**Tim Miller**  
Associate Director  
+61 2 9455 9182  
+61 0429 057 434  
tjillator@kpmg.com.au

kpmg.com.au