Privacy and data security factsheet: ISO/IEC 27001:2013(E) certification

In today's rapidly evolving digital landscape, privacy and data security have become paramount concerns for individuals and organisations across all industries. The Australian legal sector, with its vast repository of sensitive client information and confidential case data, faces unique challenges in safeguarding privacy and maintaining robust data security practices.

Gadens is committed to following best practice procedures and protecting our firm and our clients against cyber threats and ransomware attacks, safeguarding our data. The firm has recently attained its ISO/IEC 27001:2013(E) certification (**ISO 27001**).

Read on for more on how Gadens is working to ensure we continue to review and improve our information technology and data security practices – to ensure that we protect our own as well as our clients' information and data.

ISO/IEC 27001:2013(E)

ISO 27001 is an International Standard that sets out a framework for establishing an information security management system that preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

1. What is ISO 27001 certification?

ISO 27001 is a globally recognised standard that sets out a framework for managing risks and protecting sensitive information, ensuring confidentiality, integrity, and availability of data. It encompasses 114 security controls and measures across 14 control domains that organisations can adopt to safeguard their information assets. Accreditation demonstrates an organisation's commitment to maintaining robust information security management, through security controls, risk assessments, and established processes to identify, manage, and mitigate information security risks.

2. How does an organisation obtain and retain the certification?

Obtaining ISO 27001 certification involves establishing an Information Security Management System (**ISMS**), conducting a gap analysis and implementing necessary measures, documenting policies and procedures, and performing internal audits and management reviews.

The certification is valid for three years and is independently audited and re-appraised annually. In conforming to the standard, Gadens will continually review and assess policies and procedures, regularly engaging with an independent external accreditation body to ensure the firm keeps pace with the evolving digital landscape.

3. Why ISO 27001?

Gadens realises the significance of the client data it holds and processes. To give confidence to our clients we take this obligation seriously, Gadens sought to certify against the leading global standard for information security management. Gadens is one of only a small number of law firms in Australia that has obtained the ISO 27001 certification. Achieving this accreditation demonstrates our commitment to market-leading data security practices.

4. What does this mean for Gadens and our clients?

The certification requires a full-firm approach, with managerial support key to driving adherence to policies. Achieving ISO 27001 accreditation is a real top-down, bottom-up process that requires buy-in from all of our staff. It demonstrates our commitment to maintaining confidentiality, integrity, and availability of firm and client data.

5. What other measures does Gadens take to ensure robust privacy and data security practice?

Gadens works with multiple security partners to ensure we have a best-in-class approach to managing data security. The firm takes a defence in depth approach, and has aligned its information security practices to the recommendations of the Australian Cyber Security Centre, including full adoption of the Essential Eight. Gadens runs regular security awareness campaigns and phishing campaigns; we reinforce multifactor authentication; and engage accredited consultants to regularly test the integrity of our network perimeter and web-based applications.

*Should you wish to have a more in-depth understanding of the work we are doing or want to understand the ISO 27001 certification better, please reach out to your Gadens contact person who can arrange time for you / your security team to meet with our Chief Information Officer (**CIO**).*