Making privacy core business

Privacy and cyber at the forefront of corporate social responsibility

28 June 2022

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000, Australia

Privacy and cyber at the forefront of corporate responsibility

Increasingly, privacy no longer sits solely within the realm of the Office of the Australian Information Commissioner. We have seen other regulators including the Australian Competition and Consumer Commission, Australian Communications and Media Authority and eSafety Commissioner play their part in relation to the regulation of personal information as it impacts their regulatory spheres of consumer protection, communications and online safety respectively.

Now, there is another regulator that oversees how the regulation of personal information or lack thereof impacts corporate responsibility, namely the Australian Securities and Investments Commission (ASIC).

In writing this piece, Privcore has partnered with Antcliffe:Scott, a law firm that fuses the best of blue-chip experience with a flexible approach and personalised service. The firm provides a comprehensive range of legal services including corporate & commercial, intellectual property, commercial property, dispute resolution, mining & resources and more.

Together we will explore the implications for corporations under the Corporations Act, and what can be learnt from the Australian Privacy Principles (APPs). The APPs regulate the management and security of personal information under the Privacy Act.

Adequate risk management systems

What are adequate risk management systems under section 912A(h) of the corporations law was recently tested in Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496. The decision was handed down on 5 May 2022. Whilst the decision also looked at other provisions of the corporations law, our focus is on the issues most relevant to privacy and cyber security.

This decision puts financial services, and more broadly, the corporate sector, on notice that ASIC will consider a lack of understanding and management of cyber security to be unacceptable. In a recent article, ASIC stated it: “is not seeking to prescribe technical standards or to provide expert guidance on cyber security. Where we consider a firm has not met its cyber risk management obligations, we may consider enforcement action to drive changes in behaviour. This is illustrated by ASIC’s proceedings against RI Advice Group. We argued it failed to have adequate policies, systems and resources in place to appropriately manage risk relating to cyber resilience.”

The case

Between 2014-2020, a number of authorised representatives of RI Advice Group Pty Ltd (RI Advice) were subject to nine cyber security breaches. During several of these attacks cyber criminals obtained access to sensitive and confidential client information.

ASIC claimed by failing to promptly implement recommended advice, plans, procedures, guidelines, frameworks and systems to manage cyber security risk, and to manage the effectiveness of cyber security controls, RI Advice contravened the Corporations Act. In particular, the Federal Court found:

"RI Advice contravened ss.912A(1)(a) and (h) of the Corporations Act from 15 May 2018 to 5 August 2021 as a result of its failure to have documentation and controls in respect of cyber security and cyber resilience in place that were adequate to manage risk in respect of cyber security and cyber resilience across its AR network, and as a result of this conduct, it:

1. failed to do all things necessary to ensure the financial services covered by the Licence were provided efficiently and fairly, in contravention of s.912A(1)(a) of the Corporations Act; and
2. failed to have adequate risk management systems, in contravention of s.912A(1)(h) of the Corporations Act."

What are the implications?

Pursuant to s.912A(1), a holder of an Australian Financial Service Licence (AFSL) or a director of a financial services provider has responsibilities to ensure it and its authorised representatives have implemented effective cyber security systems. Such systems should be a part of standard risk and compliance procedures and, if relevant, reporting to the Board.

All directors today should have an understanding and ongoing awareness of their company's privacy and cyber resilience and cyber security standards and protections. This may include ensuring appropriate experts are retained to assist the company to design and implement adequate controls. All directors must ensure the company implements the controls, measures and procedures necessary to ensure systems have adequate security measures in place commensurate with the level of risk.

When considering the obligation of an AFSL holder to do all things necessary to ensure the financial services covered by the licence are provided 'efficiently, honestly and fairly' (s.912A(1)(a)), the AFSL holder is required to identify and document risks. Appropriate risk management systems must be in place to manage those risks.

Tools to identify privacy and security risks include the conduct of privacy impact assessments (PIA). A PIA is a risk assessment of new or existing processes, technology, laws or regulations, systems or programs involving personal information. PIAs are designed to identify the privacy risks of handling personal information and then provide ways to mitigate, prevent or eliminate those risks.

The question inevitably arises, what is cyber security best practice and what is expected of a reasonable cyber security risk management and resilience system?

The court considered the relevant test is what the reasonable person qualified in the area of cyber security and cyber resilience would expect, not the expectations of the general public. On this basis, it is necessary for business to engage with privacy and cyber security experts and to maintain ongoing system reviews to maintain cyber resilience.

What can be learnt from the Australian Privacy Principles?

Not dissimilar to s912A(1)(h) of the Corporations Act requiring adequate risk management systems, APP 1 requires regulated entities to "take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity…"

APP 11.1 also requires regulated entities holding personal information to "take steps as are reasonable in the circumstances to protect the information:
(a) from misuse, interference and loss; and
(b) from unauthorised access, modification or disclosure

In this case, RI Advice possessed personal information including names, addresses, birth dates, health data, contact details and copies of official ID documents such as licences, passports and more. It is clear from this case adequate risk management systems under the Corporations Act, include those designed to protect personal information.

As the privacy regulator, the OAIC has a significant amount of guidance on what are appropriate steps to take under APPs 1 and 11. This includes:

- Data minimisation and deleting or de-identifying personal information no longer required (for example, old customer personal information)
- Ensuring multi-factor authentication
- Procedures for identifying and responding to privacy incidents, handling access and correction requests and receiving and responding to complaints and inquiries
- A program of proactive review and audit of the adequacy and currency of the privacy policy, practices, procedures and systems implemented

The Australian Cyber Security Centre has also published the Essential Eight mitigation strategies to mitigate cyber security incidents.

It is likely further strengthened accountability and security requirements will be incorporated

under the Privacy Act as part of the reform process the Attorney-General's Department is currently undertaking. A recent summary of that reform is available.

Whilst cyber security has been a growing concern for corporations, this case reflects just how truly critical the management of cyber security will be moving forward.
Businesses must ensure effective and appropriate privacy and security risk management processes are in place, to protect their customers (and business) and to avoid any potential future regulatory action.

About Privcore

Privcore's team with 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a Superstar of STEM in 2021-2022 and a privacy professional practising since 2001 founded Privcore. She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.