ARTICLE

Australia Is Getting Serious About Penalties for Privacy Enforcement

Boardooms, Take Notice

In the wake of a flurry of high profile data breaches in the local telecoms and healthcare sectors, the Australian Government announced on 22 October 2022 that it was moving quickly to increase financial penalties under the *Privacy Act 1988* (Cth). Attorney General, the Hon. Mark Dreyfus MP, tabled the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 ("Bill") four days later. [1] It was passed a month later, on 28 November 2022, and came into force on 13 December 2022 ("Amendment Act").

The Amendment Act radically reshapes the privacy compliance landscape in Australia and places the penalties for the mishandling of personal data amongst the most stringent in the world. It is an opportune time for Australian companies, and companies with Australian exposure, to reassess how they handle personal information and ensure their processes are mature, robust and defensible.

SIGNIFICANT INCREASE IN FINANCIAL PENALTIES

The Privacy Act 1988 (Cth) (**"Privacy Act"**) applies to the handling of personal information by most Australian Government agencies and by private companies, excluding "small" businesses with an annual turnover of less than AUD$3 million. Currently, the maximum civil penalty for "serious or repeated interferences with privacy" is AUD$2.22 million.[2]

Under the Amendment Act, the maximum penalty for incorporated entities has been increased to the greater of:

- AUD$50 million
- Three times the value of any benefit obtained through the misuse of information; or
- 30% of a company's adjusted turnover in the relevant period (i.e., the period of non-compliance with the Privacy Act).[3]

For unincorporated entities (including individuals, sole traders and partnerships), the penalty will increase from the previous maximum of AUD$440,000 to AUD$2.5 million.[4]

[1] Parliament of Australia, Bills and Legislation – *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*
[2] Privacy Act 1998 (Cth) S13G where "penalty unit" is defined by the Crimes Act 1914 (Cth) S4AA.
[3] Parliament of Australia, Bills and Legislation – Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, Schedule 1 - Amendments, part 14
[4] Ibid.

These penalties apply to any breach of the Privacy Act (including the Australian Privacy Principles) that constitute a "serious or repeated interference with privacy", per s13G of the Privacy Act. This maximum penalty could apply to scenarios involving security incidents or data breaches and breach notification, but also to any other non-compliance with the APPs — for example, issues relating to transparency, uses and disclosures of personal information, or over-retention of personal information without a lawful business purpose.

The penalties are similar in approach to those under GDPR in Europe, which is widely considered the strongest global privacy regime. GDPR includes fines of €20 million, or up to 4% of global revenue, whichever is the greater.[5] To date, European regulators have issued fines in the tens and hundreds of millions of euros.[6]

The passing of this bill means that Australia now has some of the most severe financial penalties for data privacy violations in the world, with fines for large businesses potentially reaching hundreds of millions of dollars. This proposal is an evolution of an ongoing trend within the recently elected Australian Government of focusing on cybersecurity, data risk and the importance of building resilience against these risks to protect the Australian economy and the public.

ENHANCED ENFORCEMENT POWERS

The Amendment Act has also amended the *Australian Information Commissioner Act 2010 (Cth)* ("AIC Act") to provide the Office of the Australian Information Commissioner ("OAIC") enhanced enforcement powers. These include:

a. expanding the types of declarations that the Commissioner can make in a determination at the conclusion of an investigation

b. amending the extraterritorial jurisdiction of the Privacy Act to ensure foreign organisations that carry on a business in Australia must meet the obligations under the Act (even if they do not collect or hold Australians' information directly from a source in Australia)

c. providing the Commissioner with new powers to conduct assessments

d. providing the Commissioner new infringement notice powers to penalise entities for failing to provide information without the need to go to court to seek a civil penalty order; and

e. strengthening the Notifiable Data Breaches scheme to ensure the Commissioner has comprehensive knowledge of the information compromised in an eligible data breach, to enable them to better assess the risk of harm to individuals.[7]

ENHANCED INFORMATION SHARING POWERS

The Amendment Act also expands and clarifies information gathering and information sharing powers. This is seemingly in response to some recent high profile Australian data breaches in which the Information Commissioner and the Attorney General have had to actively seek out or demand information about the extent and severity of data breaches from breached entities. It is intended to ensure the Government and the Information Commissioner are better equipped to provide information about data breaches to affected individuals.

Specifically, the Bill will enhance the Information Commissioner's ability to share information by:

a. clarifying the Commissioner can share information gathered through the Commissioner's Information Commissioner functions, Freedom of Information functions and Privacy functions

b. providing the Commissioner with the power to disclose information or documents to an enforcement body, an alternative complaint body, and a State, Territory, or foreign privacy regulator for the purpose of the Commissioner or the receiving body exercising their powers, or performing their functions or duties; and

c. providing the Commissioner with the power to publish a determination or information relating to an assessment on the Commissioner's website; and disclose all other information acquired while exercising powers or performing functions or duties if it is in the public interest.[8]

[5] What are the GDPR fines? https://gdpr.eu/fines/
[6] GDPR Fines & Data Breach Penalties, https://www.gdpreu.org/gdpr-compliance/fines-and-penalties/
[7] Parliament of Australia, Bills and Legislation – *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, Schedule 1 - Amendments, part 18*
[8] Parliament of Australia, Bills and Legislation – *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, Schedule 1 - Amendments, part 20*

The Amendment Act will also amend the *Australian Communications and Media Authority Act 2005* (Cth) ("ACMA") to expand the ACMA's ability to share information with other Australian Government agencies to assist in the enforcement of Commonwealth laws.[9]

Noting the ACMA and the OAIC have recently launched coordinated investigations into a significant data breach in the telecoms sector, it appears the Government is laying the groundwork for greater interagency cooperation on privacy regulation.

WHAT'S NEXT?

The Australian Government is also continuing its review of the Privacy Act, which has been in progress since December 2019. A report on the consultation on the Review of the Privacy Act 1988 – Discussion paper is due before the end of the year. The amendments are expected to be far-reaching — proposals currently under consideration include the elimination of existing exemptions, broader powers to issue penalty notices, expansion of the definition of personal information and the introduction of a statutory tort of privacy. Draft legislation will likely be introduced next year.

FTI Consulting Technology's global Information Governance, Privacy & Security experts recommend that businesses that handle personal information and operate in Australia, or that collect personal information from Australia, are proactive in reviewing and mitigating their privacy risks. In the changing privacy risk landscape, developing defensible approaches to personal information management, and designing toward privacy best practice, will continue to be critical issues for the boardroom.

To discuss these issues further, please reach out to Tim.deSousa@fticonsulting.com or contact our Sales team.

[9] Parliament of Australia, Bills and Legislation – *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, Schedule 1 - Amendments, part 40*

TIM DE SOUSA
Senior Director
Technology
+61 2 9235 9305
tim.desousa@fticonsulting.com

DEVINA POTTER
Senior Consultant
Technology
+61 03 9604 0672
devina.potter@fticonsulting.com