



Australian
National
University

Centre for
European
Studies

ANU Centre for European Studies Briefing Paper Series

Jean Monnet Paper

**Australian Data Protection Law Post-Optus and Medibank:
Comparing the *Privacy Act 1988* (Cth) with European Best-Practice**

Joshua Woodyatt



Recent Briefing Papers

The ANU Centre for European Studies Briefing Paper Series

is an interdisciplinary series that aims to provide a concise overview of the latest research promoting greater understanding of issues relating to Europe, the European Union and the Europe–Australia relationship.

The Papers serve as a summary of these issues, and as a ready information source for the preparation of submissions, media releases or reports for use by university students, government departments, diplomats and other interested parties, as well as the general public.

The Briefing Papers also showcase the work of the Centre, providing an avenue of public outreach for the broad range of workshops, seminars, public lectures and conferences that form the Centre’s work program. They showcase, too, the research projects supported by the Centre through its appointment of highly qualified scholars as staff members, postdoctoral research fellows, adjuncts and associates, and by its competitive visiting fellowship program.

All ANUCES Briefing Papers can be viewed on our website:

<http://politicsir.cass.anu.edu.au/centres/ces/research/publications/briefing-paper>

The Centre of Excellence for EU-Australia Economic Cooperation: Roundtable with Mr Volkmar Klein | Ed. Joshua Woodyatt | October 2022 | Volume 13 Number 3

Liberal Democracy in Action – Background Paper | Rita Parker | May 2022 | Volume 13 Number 2

Russia’s Invasion of Ukraine | Various authors | March 2022 | Volume 13 Number 1

Climate Change Litigation in the EU | Nicolas de Sadeleer | September 2021 | Volume 12 Number 5

Climate Change Litigation in Australia | Murray Raff | September 2021 | Volume 12 Number 4

Belarus, Russia and NATO: bringing Russia to NATO’s eastern flank | Various authors | July 2021 | Volume 12 Number 3

The EU’s and Greece’s Approach to Unregulated Migration | Constantine Karouzos | May 2021 | Volume 12 Number 2

Perspectives on EU’s Post-COVID-19 Green Recovery | Ivana Damjanovic | January 2021 | Volume 12 Number 1

Migration to and from Germany: Both a Model and a Cautionary Tale | Bettina Biedermann and Heribert Dieter | July 2020 | Volume 11 Number 1

The Europa Policy Labs | Eds. Shelley Zhao and Dean Karouzos | December 2019 | Volume 10 Number 4

Identifying Opportunities in EU-Australia Trade in Services | Steve Nerlich and Sihui Ong | November 2019 | Volume 10 Number 3

Schuman Lecture Series – Europe at the crossroads: global power or also-ran? | Gareth Evans | October 2019 | Volume 10 Number 2

AUSTRALIAN DATA PROTECTION LAW POST-OPTUS AND MEDIBANK: COMPARING THE *Privacy Act 1988 (Cth)* WITH EUROPEAN BEST-PRACTICE

Joshua Woodyatt*

I INTRODUCTION

When the *Privacy Act 1988 (Cth)* was first introduced into Parliament in November 1988,¹ then-Attorney-General Lionel Bowen explained it in prescient terms:

enormous developments in technology for the processing of information are providing new and, in some respects, undesirable opportunities for the greater use of personal information...[and] have focused attention on the need for the regulation of the collection and use of personal information by government agencies[.]²

At that time, it was inconceivable that ‘data protection’ might span beyond the perceived overreach of government. Indeed, the internet was only in its infancy,³ and NASA’s Space Shuttle had a maximum transmission rate back to Earth of just 80Kb/s.⁴ Today, the lowest-speed NBN plan delivers average download speeds of 25.3Mb/s—316 times faster.⁵ Indeed, where personal data was once government’s near-exclusive preserve, the *Privacy Act* must now reckon with global data-harvesting of scarcely-believable proportions.⁶ In turn, the risk of ‘data breaches’, where huge volumes of data are stolen and exploited/sold-on, has exploded, posing a significant problem for regulators seeking to balance security, privacy, and legitimate data use.⁷ In light of these challenges, this paper critically examines the *Privacy Act* as it relates to data storage, transfer, penalties, and fundamental principles, and proposes reform options from a comparison with best-

* Research Associate, ANU Centre for European Studies — email: Joshua.Woodyatt@anu.edu.au. A previous version of this paper was presented to Peter Khalil MP, Chair of the Parliamentary Joint Committee on Intelligence and Security and Federal Member for Wills, through the Australian National Internships Program. All views expressed in this paper are those of the author — and those of the author alone — as are any errors or omissions.

¹ Privacy Bill 1988 (Cth).

² Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2118 (Lionel Bowen, Attorney-General).

³ Johnny Ryan, *A History of the Internet and the Digital Future* (Reaktion Books, 2010) 91-104.

⁴ Gerald Soffen et al. (eds), *Research and Technology 1988: Annual Report of the Goddard Space Flight Center* (NASA, 1988) 65.

⁵ SamKnows, *Measuring Broadband Australia* (ACCC, Report N° 18, August 2022) 4 <<https://www.accc.gov.au/system/files/MBA%2018%20report%209%20August%202022.pdf>>.

⁶ Diane Coyle et al., *The Value of Data: Summary Report* (Bennett Institute for Public Policy, 26 February 2020) 6 <https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2020/12/Value_of_data_summary_report_26_Feb.pdf>.

See also “‘The Great Hack’: Cambridge Analytica is just the tip of the iceberg”, *Amnesty International* (Web Page, 24 July 2019) <<https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>>.

⁷ See generally Bruce Middleton, *A History of Cyber Security Attacks: 1980 to Present* (CRC Press, 2017); Monique Mann et al., ‘The limits of (digital) constitutionalism: Exploring the privacy-security (im)balance in Australia’ (2018) 80(4) *International Communication Gazette* 369; Janne Hagen and Olav Lysne, ‘Protecting the digitized society — the challenge of balancing surveillance and privacy’ [2016, Spring] *The Cyber Defense Review* 75.

practice exemplars from the EU (the *General Data Protection Regulation*; *GDPR*)⁸ and Germany (the *Bundesdatenschutzgesetz*, or ‘Federal Data Protection Law’).⁹

II CONTEXT AND METHODOLOGY

A *Recent Events*

The current sense of urgency surrounding data protection and privacy is not new. Indeed, as early as 1998, then-High Court Justice Michael Kirby observed:

T[he] quantity of personal information about individuals is likely to increase rather than decrease. Access to this information is what occasions the contemporary frailty of privacy – a human attribute that has been steadily eroded over the past century. To the extent that the individual has no control over, and perhaps knowledge about, the mass of identifiable data which may be accumulated concerning [them], and to the extent that national law-makers, despite their best endeavours, enjoy only limited power effectively to protect individuals in the global web, privacy as a human right is steadily undermined.¹⁰

In the two decades since Justice Kirby’s remarks, the dawn of the so-called ‘data age’ has forced unprecedented expansions to the scale and scope of the *Privacy Act*.¹¹ The pressures of this change have forced regulators to constantly update storage and transfer rules to balance the demands of growth with the prevention and deterrence of data security threats.¹² Attention on these threats has only grown following highly-publicised recent attacks on Optus and Medibank.¹³ In Optus’ case, an ‘unsophisticated’ hacker was able to access the data of some two million customers, including details of sensitive personal identification documents.¹⁴ Barely two weeks later, Medibank had *all* four million current customers’ data (replete with medical information) compromised in a

⁸ *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* [2016] OJ L 119/1.

⁹ *Bundesdatenschutzgesetz* [Federal Data Protection Law] (Germany) 30 June 2017, BGBl I, 2017, 2097.

¹⁰ Justice Michael Kirby, ‘Privacy in Cyberspace’ (1998) 21 *University of New South Wales Law Journal* 323, 325-326. See also Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (Federation Press, 2005) 1-12.

¹¹ *Privacy Act 1988* (Cth); cf *Privacy Act 1988* (Cth), as enacted. See, eg, *The Data Age Is Here. Are You Ready?* (Splunk Inc, 2020).

¹² Mann et al. (n 7).

¹³ Ariel Bogle, ‘Data breach fine proposals in wake of Optus, Medibank hacks not enough, say privacy advocates’, *ABC* (Web Page, 27 October 2022) <<https://www.abc.net.au/news/science/2022-10-27/data-breach-penalties-privacy-laws-not-enough-critics-say/101578160>>.

¹⁴ ‘Optus reveals more than 2 million customers had personal ID numbers compromised in cyber attack’, *ABC* (Web Page, 3 October 2022) <<https://www.abc.net.au/news/2022-10-03/optus-data-breach-cyber-attack-deloitte-review-audit/101496190>>.

similar hack.¹⁵ Unsurprisingly, reforming the *Privacy Act* is now firmly on the Albanese government's agenda,¹⁶ with media pressure for reform widespread.¹⁷

B Data Protection as a National Priority

From the *Privacy Act's* (relatively) humble origins as a safeguard against government overreach,¹⁸ data protection has since emerged as a core national priority. It now features in defence and foreign policy white papers alongside 'traditional' concerns like trade routes and economic security,¹⁹ and has spurred complementary State and Territory-level legislation.²⁰ Given the potential uses of personal data – especially of the sensitive kind captured in the Optus/Medibank breaches – for identity theft, scams, and even sophisticated state-backed operations, the *Privacy Act* must necessarily be amended regularly.²¹ The consequences of failure can be severe. Figures from IBM's annual *Cost of a Data Breach* reporting have shown a continuing rise in the average cost of breaches in Australia since 2018,²² even as the number of 'notifiable' breaches (that is, breaches by certain data-holding bodies, defined under the *Privacy Act*)²³ published by the Office of

¹⁵ Emilia Terzon and Samuel Yang, 'Medibank says all customers' personal data compromised by cyber attack', *ABC* (Web Page, 26 October 2022) <<https://www.abc.net.au/news/2022-10-26/medibank-hack-criminals-access-hack-data/101578438>>.

¹⁶ Matthew Knott and Nick Bonyhady, 'Privacy laws to be overhauled as Dreyfus questions why Optus kept customers' details', *Sydney Morning Herald* (Web Page, 29 September 2022) <<https://www.smh.com.au/politics/federal/privacy-laws-to-be-overhauled-as-dreyfus-questions-why-optus-kept-customers-details-20220929-p5blve.html>>.

¹⁷ Michael Slezak and Marty Smiley, 'Medibank, Optus, Woolworths data hacks show how a 'decade of anti-security policy' is putting Australia at risk, experts say', *ABC* (Web Page, 21 October 2022) <<https://www.abc.net.au/news/2022-10-21/medibank-optus-data-hack/101558932>>; Alison Xiao and Dan Conifer, 'Hackers could see Australia as weak target after Optus, Medibank data breaches, insider says', *ABC* (Web Page, 2 November 2022) <<https://www.abc.net.au/news/2022-11-02/hackers-could-see-australia-as-weak-target-after-optus-medibank/101599524>>; Miriah Davis, 'Government increases fines for companies involved in data breaches following Optus and Medibank cyber attacks', *Sky News* (Web Page, 22 October 2022) <<https://www.skynews.com.au/australia-news/government-increases-fines-for-companies-involved-in-data-breaches-following-optus-and-medibank-cyber-attacks/news-story/63bb6ded022539f379cc92a33449295d>>; John Davidson, 'Privacy fallout from Medibank hack 'will be widespread', *Australian Financial Review* (Web Page, 24 October 2022) <<https://www.afr.com/technology/privacy-fallout-from-medibank-hack-will-be-widespread-20221023-p5bs75>>. See also, beyond the *Privacy Act* context, Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (Cth).

¹⁸ See also, on Australian privacy rights before the *Privacy Act 1988* (Cth), *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479; cf *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. But see *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948) art 12; cf *Commonwealth v Tasmania* (1983) 158 CLR 1; *Coe v Commonwealth of Australia*; *Government of the United Kingdom of Great Britain and Northern Ireland* (1978) 52 ALJR 334. See also, generally, Doyle and Bagaric (n 10) 59-94; Raymond Wacks, *The Protection of Privacy* (Sweet & Maxwell, 1980) 1-12.

¹⁹ See, eg, *2017 Foreign Policy White Paper: Opportunity Security Strength* (Australian Government, 2017) 31; *2016 Defence White Paper* (Australian Government, 2016) 51-53.

²⁰ See, eg, *Information Privacy Act 2009* (Qld); *Privacy and Data Protection Act 2014* (Vic).

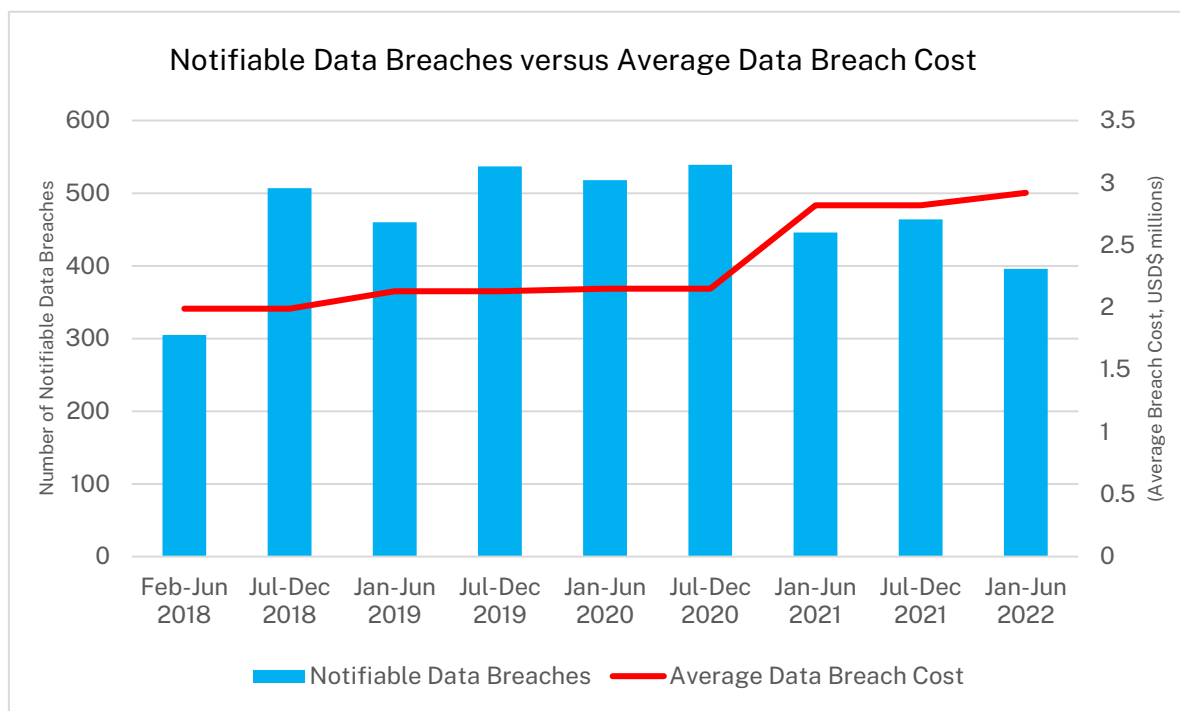
²¹ The *Privacy Act 1988* (Cth) has been amended eight times by five Acts since January 2021, see *National Emergency Declaration (Consequential Amendments) Act 2020* (Cth); *National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Act 2021* (Cth); *Federal Circuit and Family Court of Australia (Consequential Amendments and Transitional Provisions) Act 2021* (Cth); *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth); *Data Availability and Transparency (Consequential Amendments) Act 2022* (Cth).

²² Ponemon Institute, *2018 Cost of a Data Breach Study: Global Overview* (13th Annual Report, IBM Security, July 2018) 15; Ponemon Institute, *Cost of a Data Breach Report 2019* (14th Annual Report, IBM Security, 2019) 21; Ponemon Institute, *Cost of a Data Breach Report 2020* (15th Annual Report, IBM Security, 2020) 23; Ponemon Institute, *Cost of a Data Breach Report 2021* (16th Annual Report, IBM Security, 2021) 14; Ponemon Institute, *Cost of a Data Breach Report 2022* (17th Annual Report, IBM Security, 2022) 10.

²³ *Privacy Act 1988* (Cth) s 26WE.

the Australian Information Commissioner has begun trending downward since a peak in 2019-20 (per figure one).²⁴

Figure One



Easily the most significant data protection challenge is that posed by malicious or criminal actors, consistently comprising over 55% of breaches (versus the 35% attributed to human error).²⁵ Given this threat environment, minimising unnecessary data storage and transfer through regulatory reform, and increasing penalties for the kinds of data security and handling practices which lead to breaches, is crucial. Comparative law is a proven learning tool to this end.²⁶

²⁴ *Notifiable Data Breaches Quarterly Statistics Report: 1 April – 30 June 2018* (OAIC, 31 July 2018) 4; *Notifiable Data Breaches Quarterly Statistics: 1 July – 30 September 2018* (OAIC, 30 October 2018) 4; *Notifiable Data Breaches Quarterly Statistics Report: 1 October to 31 December 2018* (OAIC, 7 February 2019) 4; *Notifiable Data Breaches Quarterly Statistics Report: 1 January to 31 March 2019* (OAIC, 13 May 2019) 4; *Notifiable Data Breaches Quarterly Statistics Report: 1 April to 30 June 2019* (OAIC, 27 August 2019) 4; *Notifiable Data Breaches Report: July–December 2019* (OAIC, 28 February 2020) 5; *Notifiable Data Breaches Report: January–June 2020* (OAIC, 31 July 2020) 5; *Notifiable Data Breaches Report: July to December 2020* (OAIC, 28 January 2021) 5; *Notifiable Data Breaches Report: January to June 2021* (OAIC, 23 August 2021) 5; *Notifiable Data Breaches Report: July to December 2021* (OAIC, 22 February 2022) 5; *Notifiable data breaches report: January to June 2022* (OAIC, 10 November 2022) 6.

²⁵ *Ibid.*

²⁶ The potential of comparative law, or ‘borrowing’ from other jurisdictions, is well-documented. See, eg, John A Makdisi, ‘The Islamic Origins of the Common Law’ (1999) 77 *North Carolina Law Review* 1635; David J Gerber, ‘Comparative law and global regulatory convergence: the example of competition law’ in Maurice Adams and Jacco Bomhoff, *Practice and Theory in Comparative Law* (Cambridge University Press, 2012) 120-142. See also, generally, Uwe Kischel, *Rechtsvergleichung* (CH Beck, 2015).

C Why Compare the Privacy Act with EU and German Models?

Australia is not alone in its rapidly changing data protection environment. Major breaches like the Optus/Medibank incidents—including against Dutch firm RDC,²⁷ German telecommunications giant T-Mobile,²⁸ and US payment platform CashApp²⁹—have redoubled international attention on data protection. This is especially so for the EU, with its task of safeguarding some 450 million citizens and the world’s second-largest economy necessitating robust legislative safeguards.³⁰ Compared with the US (and its piecemeal data protection framework),³¹ however, the EU has a history of consolidated and targeted reform. Pioneering instruments like the *Consumer Rights Directive*,³² the *European Climate Law*,³³ and the *GDPR* establish strong minimum standards, with Member States then extending this to create a coherent and robust regulatory network.³⁴ In turn, these standards swell the so-called ‘Brussels effect’, where European regulatory momentum is carried by factors like trade and commerce to influence laws across the world.³⁵ The reach of EU law is readily apparent even in Australia, with the Attorney-General’s Department issuing guidelines in 2018 on the implications of the then-new *GDPR* for Australian companies.³⁶

The value of comparison with Europe goes beyond the Brussels effect, however. Taken together, the EU is Australia’s second-largest two-way goods and services trading

²⁷ Joost Schellevis, ‘Datalek bij autobedrijven treft mogelijk miljoenen Nederlanders’, *Nederlandse Omroep Stichting* (Web Page, 25 March 2021) <<https://nos.nl/artikel/2374024-datalek-bij-autobedrijven-treft-mogelijk-miljoenen-nederlanders>>.

²⁸ Bree Fowler, ‘T-Mobile hack: Here’s what we know about the massive data breach’, *CNET* (Web Page, 28 August 2021) <<https://www.cnet.com/tech/t-mobile-hack-heres-what-we-know-about-the-massive-data-breach/>>.

²⁹ Irina Ivanova, ‘Cash App says data breach could affect millions of users’, *CBS News* (Web Page, 6 April 2022) <<https://www.cbsnews.com/news/cash-app-hack-data-breach-potentially-affecting-millions-of-users/>>.

³⁰ If the EU27 are taken together, see ‘Australia’, *CIA World Factbook* (Web Page, accessed 9 November 2022) <<https://www.cia.gov/the-world-factbook/countries/australia/>>; ‘European Union’, *CIA World Factbook* (Web Page, accessed 9 November 2022) <<https://www.cia.gov/the-world-factbook/countries/european-union/>>; if the EU27 are taken together, see ‘GDP (current US\$) – United States, European Union, China’, *World Bank* (Web Page, accessed 9 November 2022) <<https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US-EU-CN>>.

³¹ See, inter alia, *Federal Trade Commission Act*, Pub L N° 63-203, § 5, 132 Stat 3314 (1914); *Privacy Act*, Pub L N° 93-579, 88 Stat 1896 (1974); *Financial Services Modernization Act*, Pub L N° 106-102, 113 Stat 1338 (1999); *Fair Credit Reporting Act* 15 USC § 1681 (1970). See also *Data Protection Act of 2021*, S 2134, 117th Congress (2021); *American Data Privacy and Protection Act*, HR 8152, 117th Congress (2022).

³² *Directive 2011/83/EU of the European Parliament and of the Council of 25 October on consumer rights, amending Council Directive 91/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council* [2011] OJ L 304/64.

³³ *Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999* [2021] OJ L 243/1.

³⁴ See, eg, in the consumer protection context, *Projet de Loi modifiant les livres I^{er}, VI et XV du Code de droit économique* [‘Bill amending Books I, VI, and XV of the Code of Economic Law’] (Belgium), *Chambre des représentants de Belgique*, 4th sess, 55th Legislature, Doc 55 2473/007 (25 April 2022).

³⁵ Lee A Bygrave, ‘The “Strasbourg Effect” on data protection in light of the “Brussels Effect”: Logic, mechanics and prospects’ (2021) 40 *Computer Law and Security Review* 105460, 2. See also Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020) 25-65.

³⁶ ‘Australian entities and the EU General Data Protection Regulation (GDPR)’, *OAIC* (Web Page, 8 June 2018) <<https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation>>.

partner,³⁷ and Germany the ninth largest.³⁸ With an EU-Australia FTA looming,³⁹ closer *GDPR* alignment would carry tangible economic benefits by facilitating wider Australian business engagement with the single market. The EU's pioneering legislative tendencies — as a historically early mover on issues like antitrust law,⁴⁰ climate change,⁴¹ and 'big tech'⁴² — also mean that both successes and failures can be weighed when drawing comparisons. For example, Australia's abortive 2011 ETS legislation benefitted significantly from the lessons of the EU ETS,⁴³ introduced in 2005.⁴⁴ Comparisons with Europe cannot be appreciated by reference to EU law alone, however. It is equally important to consider how Member State law, which is not limited by the treaty-specified competencies that constrain EU lawmaking,⁴⁵ builds upon EU minimum standards.⁴⁶ In the data protection-space, Germany offers a useful analogue. Beyond fundamental similarities — both are highly-developed federal states⁴⁷ — Germany's *Bundesdatenschutzgesetz* extends the *GDPR* in several respects.⁴⁸ Germany is also well regarded for its regulatory thoroughness, even if Germany's civil law system differs from

³⁷ DFAT, *Australia's Trade in Goods and Services (a)(b) by Top 15 Partners* (Trade and Investment Data and Publications, Financial Year 2020/2021) 1. <<https://www.dfat.gov.au/sites/default/files/australias-goods-services-by-top-15-partners-2020-21.pdf>>.

³⁸ *Ibid.*

³⁹ Tory Shepherd, 'Australia-EU free trade agreement back on track with Albanese government, ambassador says', *The Guardian* (Web Page, 5 August 2022) <<https://www.theguardian.com/australia-news/2022/aug/05/australia-eu-free-trade-agreement-back-on-track-with-albanese-government-ambassador-says>>.

⁴⁰ *Treaty on the Functioning of the European Union*, opened for signature 7 February 1992, [2009] OJ C 115/199 (entered into force 1 November 1993) arts 101, 102, and 107(1) [cited as amended] ('*TFEU*'). See also Meinrad Dreher and Michael Kulka, *Wettbewerbs- und Kartellrecht: Eine systematische Darstellung des deutschen und europäischen Rechts* (CF Müller, 10th ed, 2018) 11-16.

⁴¹ See, eg, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Green Deal*, COM(2019) 640 final (11 December 2019).

⁴² See, eg, *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)* [2022] OJ L 265/1; European Commission, *Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, COM(2022) 68 final.

⁴³ *Clean Energy Act 2011* (Cth) (repealed). See also, inter alia, Carbon Pollution Reduction Scheme Bill 2009 (Cth); Carbon Pollution Reduction Scheme Bill 2009 (N° 2) (Cth); Carbon Pollution Reduction Scheme Bill 2010 (Cth); Carbon Credits (Carbon Farming Initiative) Bill 2011 (Cth).

⁴⁴ *Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a scheme for greenhouse gas emission allowance trading within the Community and amending Council Directive 96/61/EC* [2003] OJ L 275/32.

⁴⁵ *TFEU* (n 40) arts 2-6; *Treaty on European Union*, opened for signature 7 February 1992, [2009] OJ C 115/13 (entered into force 1 November 1993) art 5 [cited as amended] ('*TEU*'). See also Takis Tridimas, 'Competence after Lisbon: The elusive search for bright lines', in Diamond Ashiagbor, Nicola Countouris and Ioannis Lianos (eds), *The European Union after the Treaty of Lisbon* (Cambridge University Press, 2012) 47-77; Jacob Öberg, 'National Parliaments and Political Control of EU Competences: A Sufficient Safeguard of Federalism?' (2018) 24(4) *European Public Law* 695; Christiaan Timmermans, 'The Competence Divide of the Lisbon Treaty Six Years After', in Sacha Garben and Inge Govaere (eds), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future* (Hart Publishing, 2017) 19-32; Robert Schütze, 'Classifying EU Competences: German Constitutional Lessons?', in Sacha Garben and Inge Govaere (eds), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future* (Hart Publishing, 2017) 33-56; Paul Craig and Gráinne de Búrca, *EU Law: Text, Cases, and Materials* (Oxford University Press, 6th ed, 2015) 73-103.

⁴⁶ See, eg, Pablo Ibáñez Colomo, 'The EU's Exclusive Competence in Competition Law', in Sacha Garben and Inge Govaere (eds), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future* (Hart Publishing, 2017) 112-132.

⁴⁷ *Grundgesetz der Bundesrepublik Deutschland* ['Basic Law of the Republic of Germany'] ('*Grundgesetz*'). See also, generally, Christoph Möllers, *Das Grundgesetz* (CH Beck, 3rd ed, 2019); Pedro Conceição et al., *Human Development Report 2021/2022 — Uncertain Times, Unsettled Lives: Shaping our Future in a Transforming World* (United Nations Development Program, 2022) 281.

⁴⁸ See below at sections IV(B)-IV(D).

Australia's more evolutionary common law approach.⁴⁹ Further, Germany's status as Europe's largest economy and predominant political force means that laws like the *Bundesdatenschutzgesetz* can hint at future EU-level legislative development.⁵⁰ These legislative, economic, and political factors together make the *GDPR* and *Bundesdatenschutzgesetz* especially useful comparators.

D Comparative Methodology

Each of the *Privacy Act*, *GDPR*, and *Bundesdatenschutzgesetz* number into the multiple hundreds of pages, spanning a diversity of topics. Considering their breadth, this paper will focus on three main features of each enactment—fundamental principles, data storage and transfer, and penalties. Beyond brevity, these focuses are common to all three, with fundamental principles informing each law's operation, and provisions on data storage, transfer, and penalties together comprising the central architecture of data protection in each jurisdiction.

III THE PRIVACY ACT 1988 (CTH)

A Fundamentals: The Australian Privacy Principles

Although 'privacy principles' have long featured in the *Privacy Act*, these were amended significantly in 2012.⁵¹ The so-called 'Australian Privacy Principles' introduced following those reforms sought to simplify both compliance and enforcement.⁵² Indeed, the term

⁴⁹ See generally Ernst A Kramer, 'Der Einfluß des BGB auf das schweizerische und österreichische Privatrecht' (2000) 200(3/4) *Archiv für die civilistische Praxis* 365; Apostolos Georgiades, 'Der Einfluß des deutschen BGB auf das griechische Zivilrecht' (2000) 200(3/4) *Archiv für die civilistische Praxis* 493; Ulf Göranson, 'Der Einfluß des BGB auf die Entwicklung des skandinavischen Privatrechts' (2000) 200(3/4) *Archiv für die civilistische Praxis* 503; Arthur Hartkamp, 'Deutsche Einflüsse auf das niederländische Privatrecht' (2000) 200(3/4) *Archiv für die civilistische Praxis* 507; Hyung-Bae Kim, 'Das deutsche BGB und das koreanische Zivilrecht' (2000) 200(3/4) *Archiv für die civilistische Praxis* 511; Toshiyuki Kono, 'Eine Skizze der Entwicklung des Bereicherungsrechts in Japan – anlässlich des hundertjährigen Bestehens des BGB' (2000) 200(3/4) *Archiv für die civilistische Praxis* 519; Ferenc Mádl, 'Der Einfluß des BGB auf die Entwicklung des ungarischen Privatrechts' (2000) 200(3/4) *Archiv für die civilistische Praxis* 526.

⁵⁰ See, eg, 'Capital subscription', *European Central Bank* (Web Page, 29 December 2021) <<https://www.ecb.europa.eu/ecb/orga/capital/html/index.en.html>>; 'GDP (current US\$) – Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden', *World Bank* (Web Page, accessed 20 November 2022) <<https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=AT-BE-BG-HR-CY-CZ-DK-EE-FI-FR-DE-GR-HU-IE-IT-LV-LT-LU-MT-NL-PL-PT-RO-SK-SI-ES-SE>>; 'Germany is doomed to lead Europe', *The Economist* (Web Page, 25 June 2020) <<https://www.economist.com/europe/2020/06/25/germany-is-doomed-to-lead-europe>>; Hans von der Burchard, 'The EU's most powerful Germans', *Politico* (Web Page, 30 June 2020) <<https://www.politico.eu/article/eu-most-powerful-germans-rotating-council-presidency/>>.

⁵¹ *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

⁵² Commonwealth, *Parliamentary Debates*, House of Representatives, 23 May 2012, 5210 (Nicola Roxon, Attorney-General). See generally Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report N° 108, May 2008). See *Privacy Act 1988* (Cth) s 6(1), as at 10 December 2012. See also, for an overview of the previous Information Privacy Principles and National Privacy Principles, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report N° 108, May 2008) vol I, 638-642 [18.8]-[18.23]; Jeremy Douglas-Stewart, *Annotated National Privacy Principles* (Presidian, 2nd ed, 2005) 37-142.

‘principles’ is somewhat misleading, with the thirteen overarching APPs functioning as the framework for a detailed subset of rules. Set against the more public-focused *Australian Consumer Law*,⁵³ the APPs are mainly written for the benefit of organisational understanding and compliance, by spelling out the obligations owed by so-called ‘APP entities’ to the individuals whose data they hold.⁵⁴ If these obligations are breached, they trigger the *Privacy Act*’s penalty regime.

Table One

The APPs		
Purpose	APP N°	Principle
Requiring APP entities to consider personal information privacy and manage it openly and transparently ⁵⁵	1	Open and transparent management of personal information ⁵⁶
	2	Anonymity and pseudonymity ⁵⁷
Requirements regarding data storage and unsolicited personal information ⁵⁸	3	Collection of solicited personal information ⁵⁹
	4	Dealing with unsolicited personal information ⁶⁰
	5	Notification of the collection of personal information ⁶¹
Requirements regarding storage of sensitive personal data like government identifiers, and the transfer of such data ⁶²	6	Use or disclosure of personal information ⁶³
	7	Direct marketing ⁶⁴
	8	Cross-border disclosure of personal information ⁶⁵
	9	Adoption, use or disclosure of government related identifiers ⁶⁶
Requirements of data security	10	Quality of personal information ⁶⁷
	11	Security of personal information ⁶⁸
Requests for access to/correction of data	12	Access to personal information ⁶⁹
	13	Correction of personal information ⁷⁰

⁵³ *Competition and Consumer Act 2010* (Cth) sch 2.

⁵⁴ *Privacy Act 1988* (Cth) s 15.

⁵⁵ *Ibid* sch 1 pt 1.

⁵⁶ *Ibid* s 1.

⁵⁷ *Ibid* s 2.

⁵⁸ *Ibid* sch 1 pt 2.

⁵⁹ *Ibid* s 3.

⁶⁰ *Ibid* s 4.

⁶¹ *Ibid* s 5.

⁶² *Ibid* sch 1 pt 3.

⁶³ *Ibid* s 6.

⁶⁴ *Ibid* s 7.

⁶⁵ *Ibid* s 8.

⁶⁶ *Ibid* s 9.

⁶⁷ *Ibid* s 10.

⁶⁸ *Ibid* s 11.

⁶⁹ *Ibid* s 12.

⁷⁰ *Ibid* s 13.

Table Two

Who is bound by the APPs?	
The APPs apply to so-called 'APP entities', ⁷¹ which are defined to mean either 'an agency or organisation': ⁷²	
'Organisations' ⁷³	Individuals ⁷⁴
	Bodies corporate ⁷⁵
	Partnerships ⁷⁶
	'[A]ny other unincorporated association' ⁷⁷
	Trusts ⁷⁸
'Agencies' ⁷⁹	Ministers ⁸⁰
	Departments ⁸¹
	Certain bodies (whether incorporated or not) or tribunals established or appointed for a public purpose or under a Commonwealth law ⁸²
	Bodies or tribunals established by or under State/Territory law in force in an external Territory, ⁸³ or persons holding offices so established ⁸⁴
	Bodies established/appointed by the Governor-General or by a Minister ⁸⁵
	Persons holding or performing the duties of an office established by or under Commonwealth/State/Territory law ⁸⁶
	Persons holding or performing the duties of a role appointed by the Governor-General or a Minister ⁸⁷
	Federal/Norfolk Island courts ⁸⁸
	The AFP ⁸⁹
	'eligible hearing service provider[s]' ⁹⁰
	service operators under the <i>Healthcare Identifiers Act 2010</i> (Cth) ⁹¹

Table Three

Who is exempt from the APPs?	
Certain agencies (bodies and tribunals 'established or appointed for a public purpose by or	Incorporated companies/societies/associations ⁹³
	Organisations/branches registered under the <i>Fair Work (Registered Organisations) Act 2009</i> (Cth) ⁹⁴
	Certain bodies established by or under State/Territory law and exempted by the Minister under sub-s (5A). ⁹⁵
	Departmental Secretaries ⁹⁶

⁷¹ Ibid s 15.

⁷² Ibid s 6 (definition of 'APP entity').

⁷³ Ibid s 6C.

⁷⁴ Ibid (definition of 'organisation para (1)(a)).

⁷⁵ Ibid (para (1)(b)).

⁷⁶ Ibid (para (1)(c)).

⁷⁷ Ibid (para (1)(d)).

⁷⁸ Ibid (para (1)(e)).

⁷⁹ Ibid s 6 (definition of 'agency').

⁸⁰ Ibid (para (a)).

⁸¹ Ibid (para (b)).

⁸² Ibid (para (c)).

⁸³ Ibid (para (ca)).

⁸⁴ Ibid (para (ea)).

⁸⁵ Ibid (para (d)), except by or under Commonwealth law.

⁸⁶ Ibid (para (e)).

⁸⁷ Ibid (para (f)), except under Commonwealth law.

⁸⁸ Ibid (paras (g), (ha)).

⁸⁹ Ibid (para (h)).

⁹⁰ Ibid (para (k)).

⁹¹ Ibid (para (l)).

⁹³ Ibid (para (c)(i)).

⁹⁴ Ibid (para (c)(ii)).

⁹⁵ Ibid (para (ca)).

⁹⁶ Ibid (para (e)).

under...Commonwealth law') ⁹²	Certain State/Territory officeholders exempted by the Minister under sub-s (5A). ⁹⁷
Certain organisations ⁹⁸	Small business operators ⁹⁹ (annual turnover <AUD\$3m) ¹⁰⁰
	Registered political parties ¹⁰¹

B *Data Storage and Transfer Rules*

1 *Storage*

The rules on data storage are spread across multiple APPs. APP 1 provides for privacy policies, requiring any data-storing APP entity to make available a 'clearly expressed and up-to-date policy'¹⁰² which details the kind of data stored/held,¹⁰³ how it is collected/held,¹⁰⁴ and the purposes for which this is done.¹⁰⁵ It must also explain how individuals can access their data,¹⁰⁶ how they can complain about an APP violation, and what the data-holder will do about that complaint.¹⁰⁷ APP 3 obliges APP entities not to collect personal information not 'reasonably necessary for, or directly related to, one or more of the entity's [functions/activities].'¹⁰⁸ When data is stored, APP entities must disclose the following to the person whose data has been collected:¹⁰⁹

- The entity's identity and contact details;¹¹⁰
- If data collection is required/authorised under Australian law or court ordered, the details of that requirement/authorisation;¹¹¹
- The purposes for which data is being collected;¹¹² and
- The main consequences if some/all of the data is *not* collected (i.e. if the person opts-out).¹¹³

⁹² Ibid (para (c)).

⁹⁷ Ibid (para (ea)).

⁹⁸ Ibid s 6C.

⁹⁹ Ibid.

¹⁰⁰ Ibid s 6D.

¹⁰¹ Ibid s 6C. See also *Commonwealth Electoral Act 1918* (Cth) pt XI.

¹⁰² *Privacy Act 1988* (Cth) sch 1 s 1.3, s 5.1.

¹⁰³ Ibid s 1.4(a).

¹⁰⁴ Ibid sub-s (b).

¹⁰⁵ Ibid sub-s (c).

¹⁰⁶ Ibid sub-s (d).

¹⁰⁷ Ibid sub-s (e).

¹⁰⁸ Ibid ss 3.2-3.3.

¹⁰⁹ Ibid s 5.1.

¹¹⁰ Ibid s 5.2(a).

¹¹¹ Ibid sub-s (c).

¹¹² Ibid sub-s (d).

¹¹³ Ibid sub-s (e).

Further, stored data cannot be put to ulterior purposes or used for direct marketing (with limited exceptions).¹¹⁴ The requirements governing ‘sensitive’ data like government identification numbers are stricter still. If it is collected – which is only permissible in certain circumstances¹¹⁵ – not only must such collection be ‘reasonably necessary’,¹¹⁶ but consent *must* be obtained.¹¹⁷ Further, government identification numbers cannot be used to identify individuals in APP entity databases, to guard against data breach risks.¹¹⁸ Lastly, data must be protected ‘from misuse, interference...loss...unauthorised access, modification or disclosure’,¹¹⁹ and must as reasonably possible be destroyed or de-identified once ‘the entity no longer needs the information for any purpose for which [it] may be [validly] used or disclosed’.¹²⁰ Data-holders must make individuals’ data available to them, or correct it, on request.¹²¹

2 Transfer

The *Privacy Act* provides for both domestic and ‘cross-border’ data transfers. In addition to privacy policy rules, which provide for notice about potential/actual transfers,¹²² ‘disclosures’ for purposes other than that for which the data was collected (‘secondary disclosures’) generally require consent,¹²³ with some exceptions.¹²⁴ Similarly, cross-border transfers must be detailed in privacy policies, along with where such data might be transferred.¹²⁵ APP entities must also take reasonable steps to ensure that cross-border recipients do not breach the APPs,¹²⁶ either by being satisfied with that country’s data laws or by obtaining the recipient’s consent to abide by the APPs.¹²⁷

C Penalties

Australia’s data protection penalty regime is presently being overhauled with the government’s *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*

¹¹⁴ Ibid s 7.1; but see ss 7.2-7.5.

¹¹⁵ Ibid ss 3.3(b), 3.4.

¹¹⁶ Ibid s 3.3(a)(i)-(ii).

¹¹⁷ Ibid s 3.3(a).

¹¹⁸ Ibid s 9.1. But see exceptions at sub-ss (a)-(b), and s 9.3.

¹¹⁹ Ibid s 11.1.

¹²⁰ Ibid ss 11.2. But see exceptions at sub-ss (c)-(d). See also s 6.4.

¹²¹ On access, see ibid s 12.1, 12.4-12.10. But see exceptions at ss 12.2-12.3; On correction, see ibid s 13.

¹²² Ibid sub-ss 5.2(f), (i), and (j).

¹²³ Ibid s 6.1.

¹²⁴ Ibid ss 6.2-6.3, 6.5.

¹²⁵ Ibid s 1.4(f)-(g).

¹²⁶ Ibid s 8.1.

¹²⁷ Ibid s 8.2.

(Cth) recently passing into law.¹²⁸ Previously, the *Privacy Act* penalised both ‘serious’ and ‘repeated’ APP breaches with a fine up to AUD\$2.22m.¹²⁹ The government’s recent amendments increased this to a maximum of AUD\$2.5m for individuals,¹³⁰ or the greater of AUD\$50m,¹³¹ three times the benefit gained by the breach,¹³² or 30% of ‘adjusted turnover’ during the breach period for corporations.¹³³

IV THE EU GENERAL DATA PROTECTION REGULATION AND GERMAN BUNDESDATENSCHUTZGESETZ

A Constitutional Protection and Division of Competencies

Europe and Germany had established constitutional data protection rights well before either the *GDPR* or *Bundesdatenschutzgesetz*. The EU makes this explicit, with ‘protection of personal data’ guaranteed by both the *Charter of Fundamental Rights of the EU* and the *Treaty on the Functioning of the EU*.¹³⁴ German constitutional protection is less direct, safeguarding ‘privacy of correspondence, post and telecommunications’.¹³⁵ The relationship between these two constitutional orders is complex.¹³⁶ As a supranational treaty organisation, the EU only has competences to the extent provided by such treaties,¹³⁷ including competence to ‘coordinate the actions of the Member States’ in ‘civil protection’ (covering data protection).¹³⁸ Conversely, Germany’s EU membership means that it cannot legislate in conflict with EU law, having voluntarily recognised European

¹²⁸ Mark Dreyfus, Attorney-General, ‘Privacy penalty bill passes house’ (Media Release, Attorney-General’s Department, 9 November 2022) <<https://ministers.ag.gov.au/media-centre/privacy-penalty-bill-passes-house-09-11-2022>>. See also the previous government’s proposed Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth).

¹²⁹ See also *Privacy Act 1988* (Cth) s 13.

¹³⁰ *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) s 14, inserting s 13G(2).

¹³¹ *Ibid*, inserting s 13G(3)(a).

¹³² *Ibid*, inserting s 13G(3)(b).

¹³³ *Ibid*, inserting s 13G(3)(c). See also *ibid*, inserting s 13G(5); s 13G(7).

¹³⁴ *Charter of Fundamental Rights of the European Union*, opened for signature 7 December 2000, [2012] OJ C 326/391 (entered into force 1 December 2009) art 8(1); *TFEU* (n 40) art 16(1). But see *TEU* (n 45) art 6(1).

¹³⁵ *Grundgesetz* (n 47) art 10.

¹³⁶ See, eg, in the ECJ-Bundesverfassungsgericht dialogue, *Costa v ENEL* (C-6/64) [1964] ECR 585; *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (C-11/70) [1970] ECR 1126; *Solange I*, Bundesverfassungsgericht, 2 BvL 52/71, 29 May 1974, reported in (1974) 37 BVerfGE 271; *Re Wünsche Handelsgesellschaft*, Bundesverfassungsgericht, 2 BvR 197/83, 22 October 1986, reported in (1986) 73 BVerfGE 339 (‘*Solange II*’); *Amministrazione delle Finanze dello Stato v Simmenthal SpA* (C-106/77) [1978] ECR 630; *Maastricht-Urteil*, Bundesverfassungsgericht, 2 BvR 2134, 12 October 1993, reported in (1993) 89 BVerfGE 155; *Ministero delle Finanze v IN.CO. GE.90 Srl* (joined cases C-10/97 to C-22/97) [1998] ECR I-6324; *Lissabon-Urteil*, Bundesverfassungsgericht, 2 BvE 2/08, 30 July 2009, reported in (2009) 123 BVerfGE 267; *Gauweiler I*, Bundesverfassungsgericht, 2 BvR 2728/13, 14 January 2014, reported in (2014) 134 BVerfGE 366; *Gauweiler and Others v Deutscher Bundestag* (CJEU, C-62/14, ECLI:EU:C:2015:400, 16 June 2015); *Gauweiler II*, Bundesverfassungsgericht, 2 BvR 2728/13, 21 June 2016, reported in (2016) 142 BVerfGE 123; *Weiss I*, Bundesverfassungsgericht, 2 BvR 859, 18 July 2017, reported in (2017) 146 BVerfGE 216; *Weiss and Others v Deutscher Bundestag* (CJEU, C-493/17, ECLI:EU:C:2018:1000, 11 December 2018); *Weiss II*, Bundesverfassungsgericht, 2 BvR 859/15, 5 May 2020, reported in (2020) 154 BVerfGE 17.

¹³⁷ *TEU* (n 45) art 5; *TFEU* (n 40) title I.

¹³⁸ *TFEU* (n 40) art 6(f).

legal primacy.¹³⁹ The *GDPR* thus provides the bulk of data protection regulation in Germany, with the *Bundesdatenschutzgesetz* implementing and extending its protections.

B Fundamental Principles

The *GDPR* provides both general ‘principles relating to processing of personal data’ and specific ‘rights of the data subject’. These ‘rights’ go to specific matters of storage and transfer, whereas ‘principles’ apply to all data collection equally. The *Bundesdatenschutzgesetz* extends only the former.

Table Four

<i>GDPR</i> Principles	Corresponding APPs
Lawful, fair, and transparent processing ¹⁴⁰	APP 1-2
Data collection for limited purposes only ¹⁴¹	APP 3, 6, 7
Minimal necessary data collection ¹⁴²	No
Accuracy ¹⁴³	APP 10
Stored ‘no longer than is necessary’ ¹⁴⁴	APP 11 ¹⁴⁵
Stored securely and confidentially ¹⁴⁶	APP 11
Data-holding entities are accountable ¹⁴⁷	APP 1

C Data Storage and Transfer Rules

1 Storage

Data storage and transfer is provided for extensively in both the *GDPR* and *Bundesdatenschutzgesetz*. The majority of storage and transfer rules are couched as ‘rights of the data subject’, although the *Bundesdatenschutzgesetz* provides for additional protections alongside several national security exceptions.¹⁴⁸ Importantly, the ‘right to be forgotten’ has been recognised by both European and German courts, with the CJEU establishing the right pre-*GDPR* in *Google Spain v AEDC* in 2014,¹⁴⁹ and the

¹³⁹ Möllers, *Das Grundgesetz* (n 47) 115-120.

¹⁴⁰ *GDPR* (n 8) art 5(1)(a); *Bundesdatenschutzgesetz* (n 9) s 47(1).

¹⁴¹ *GDPR* (n 8) art 5(1)(b); *Bundesdatenschutzgesetz* (n 9) s 47(2).

¹⁴² *GDPR* (n 8) art 5(1)(c); *Bundesdatenschutzgesetz* (n 9) s 47(3).

¹⁴³ *GDPR* (n 8) art 5(1)(d); *Bundesdatenschutzgesetz* (n 9) s 47(4).

¹⁴⁴ *GDPR* (n 8) art 5(1)(e); *Bundesdatenschutzgesetz* (n 9) s 47(5).

¹⁴⁵ APP 11 is much broader than its *GDPR* equivalent, see below at section V(B).

¹⁴⁶ *GDPR* (n 8) art 5(1)(f); *Bundesdatenschutzgesetz* (n 9) s 47(6).

¹⁴⁷ *GDPR* (n 8) art 5(2).

¹⁴⁸ See especially *Bundesdatenschutzgesetz* (n 9) art 10(2).

¹⁴⁹ *Google Spain SL and Google Inc v Agencia Española de Protección de Datos and Mario Costeja González* (Court of Justice of the European Union, C-131/12, ECLI:EU:C:2014:317, 13 May 2014).

Bundesverfassungsgericht confirming its existence in several post-Bundesdatenschutzgesetz decisions.¹⁵⁰

Table Five

Rights of the data subject		Corresponding APP
GDPR	For information about data collection to be made available ‘in a concise, transparent, intelligible and easily accessible form, using clear and plain language’ ¹⁵¹	APP 1 ¹⁵²
	Data-holding entities must ‘facilitate the exercise of data subject rights’ ¹⁵³	No ¹⁵⁴
	Data-holding entities must give: <ul style="list-style-type: none"> • their identity;¹⁵⁵ • their contact details;¹⁵⁶ • the purposes of data collection and the legal basis for that collection;¹⁵⁷ • any entities to which data may be transferred;¹⁵⁸ and • the period of storage.¹⁵⁹ For both personal and non-personal data ¹⁶⁰	APP 1 (partly) ¹⁶¹
	Data-holding entities must explain: <ul style="list-style-type: none"> • The individual’s right to request access and rectify/erase data;¹⁶² • The individual’s right to withdraw consent;¹⁶³ • Avenues of complaint;¹⁶⁴ and • Any obligation they are under to collect/transfer data (such as by law)¹⁶⁵ For both personal and non-personal data ¹⁶⁶	Only partly (APP 1) Avenues of complaint ¹⁶⁷ and ‘whether the entity is likely’ to transfer data overseas ¹⁶⁸
	To access data, and receive a copy of it ¹⁶⁹	APP 1, ¹⁷⁰ APP 12 ¹⁷¹

¹⁵⁰ *Recht auf Vergessen I*, Bundesverfassungsgericht [German Constitutional Court] 1 BvR 16/13, 6 November 2019 reported in (2019) 152 BVerfGE 152; *Recht auf Vergessen II*, Bundesverfassungsgericht [German Constitutional Court] 1 BvR 276/17, 6 November 2019 reported in (2019) 216 BVerfGE 152. See also David Kravets, ‘Convicted Murderer Sues Wikipedia, Demands Removal of His Name’, *Wired* (Web Page, 11 November 2011) <<https://www.wired.com/2009/11/wikipedia-murder/>>.

¹⁵¹ GDPR (n 8) art 12(1)

¹⁵² *Privacy Act 1988* (Cth) sch 1 s 1.1.

¹⁵³ GDPR (n 8) art 12(2).

¹⁵⁴ Cf *Privacy Act 1988* (Cth) sch 1 s 1.5-1.6.

¹⁵⁵ GDPR (n 8) art 13(1)(a).

¹⁵⁶ *Ibid*.

¹⁵⁷ *Ibid* art 13(1)(c).

¹⁵⁸ *Ibid* arts 13(1)(e)-(f).

¹⁵⁹ *Ibid* art 13(2)(a).

¹⁶⁰ See *ibid* art 14.

¹⁶¹ *Privacy Act 1988* (Cth) sch 1 s 1.4.

¹⁶² GDPR (n 8) art 13(2)(b).

¹⁶³ *Ibid* art 13(2)(c); Cf *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* (C-311/18) [2020] ECLI:EU:C:2020:559.

¹⁶⁴ GDPR (n 8) art 13(2)(d).

¹⁶⁵ *Ibid* art 13(2)(e).

¹⁶⁶ See *ibid* art 14.

¹⁶⁷ *Privacy Act 1988* (Cth) sch 1 s 1.4(e).

¹⁶⁸ *Ibid* s 1.4(f)-(g).

¹⁶⁹ GDPR (n 8) arts 15, 20.

¹⁷⁰ *Privacy Act 1988* (Cth) sch 1 s 1.4(d).

¹⁷¹ *Ibid* s 12.1.

	To data rectification ¹⁷²	APP 1, ¹⁷³ APP 13 ¹⁷⁴
	To data erasure ('right to be forgotten') ¹⁷⁵	No
	To restrict processing in certain circumstances ¹⁷⁶	No
	To object to data processing ¹⁷⁷	No
	To opt-out of 'automated individual decision-making' ¹⁷⁸	No
	To be notified of data breaches 'likely to result in a high risk to the rights and freedoms of natural persons' ¹⁷⁹	Provided elsewhere ¹⁸⁰
Additional <i>Bundesdatenschutzgesetz</i> rights	For information about data collection, including the right to complain to the Federal Commissioner for Data Protection and Freedom of Information ('Federal Commissioner'), to be publicly available. ¹⁸¹	APP 1 ¹⁸²
	The right to complain to the Federal Commissioner ¹⁸³	APP 1 ¹⁸⁴
	The right to appeal against decisions of the Federal Commissioner ¹⁸⁵	Provided elsewhere ¹⁸⁶

Data storage is also preconditioned on rigorous security protocols. Data-holders are required to prove not only compliance with the above rights and principles, but also to:

implement appropriate technical and organisational measures...designed to implement data-protection principles...in an effective manner and to integrate the necessary safeguards into the processing in order to...protect the rights of data subjects.¹⁸⁷

Several specific security measures are provided to this end at *GDPR* art 32, governed by a (voluntary) data protection certification regime administered under the *Bundesdatenschutzgesetz*.¹⁸⁸ Special 'data protection officers' are also required by certain organisations storing data at-scale.¹⁸⁹

¹⁷² *GDPR* (n 8) art 16.

¹⁷³ *Privacy Act 1988* (Cth) sch 1 s 1.4(d).

¹⁷⁴ *Ibid* s 13.1.

¹⁷⁵ *GDPR* (n 8) art 17.

¹⁷⁶ *Ibid* art 18.

¹⁷⁷ *Ibid* arts 21-22.

¹⁷⁸ *Ibid* art 34.

¹⁷⁹ *GDPR* (n 8) art 34.

¹⁸⁰ *Privacy Act 1988* (Cth) pt IIIC div 3.

¹⁸¹ *Bundesdatenschutzgesetz* (n 9) s 55. See also *GDPR* (n 8) arts 13-14.

¹⁸² *Privacy Act 1988* (Cth) sch 1 s 1.4(e).

¹⁸³ *Bundesdatenschutzgesetz* (n 9) s 60. See also *GDPR* (n 8) art 13(2)(d).

¹⁸⁴ *Privacy Act 1988* (Cth) sch 1 s 1.4(e).

¹⁸⁵ *Bundesdatenschutzgesetz* (n 9) s 61.

¹⁸⁶ *Administrative Decisions (Judicial Review) Act 1977* (Cth) ss 5-7. See also 'Your complaint review rights', *OAIC* (Web Page, accessed 19 November 2022) <<https://www.oaic.gov.au/privacy/privacy-complaints/your-complaint-review-rights>>.

¹⁸⁷ *GDPR* (n 8) art 25(1).

¹⁸⁸ *GDPR* art 42.

¹⁸⁹ *GDPR* arts 37-39.

2 Transfer

Data transfer is provided in similarly rigid terms to principles and rights, with the *Bundesdatenschutzgesetz* governing domestic transfers by public bodies,¹⁹⁰ and the *GDPR* governing transfers ‘to third countries or international organisations’.¹⁹¹ Crucially, data can only be transferred to countries and organisations with data protection regimes deemed ‘adequate’ by the European Commission,¹⁹² and only where suitable safeguards are in place.¹⁹³ To this end, the Commission does not consider several significant economies’ data protection rules adequate – including those of Australia and the US.¹⁹⁴ The *GDPR* here codifies the CJEU’s *Schrems I* decision,¹⁹⁵ which found that pre-*GDPR* data transfers to the USA violated the applicant’s privacy rights, and that US data protection rules were inadequate.¹⁹⁶ The *Bundesdatenschutzgesetz* provides limited exceptions to this, imposing obligations on data-holders to guarantee data rights during the transfer process and not to transfer inaccurate/outdated/unnecessary data.¹⁹⁷

C Penalties

In keeping with other EU penalty regimes, both the *GDPR* and *Bundesdatenschutzgesetz* take a severe approach to data breaches.¹⁹⁸ Beyond rights to complain to the Federal Commissioner,¹⁹⁹ or the courts,²⁰⁰ a discrete right to compensation is established under both enactments where persons ‘have suffered material or non-material damage’ from a *GDPR/Bundesdatenschutzgesetz* violation by a data-holding entity.²⁰¹ Several mandatory considerations, including the ‘intentional or negligent character of the infringement’,²⁰² and ‘the degree of cooperation with the supervisory authority’,²⁰³ qualify the *GDPR*’s tiered penalty framework for data-holders.²⁰⁴ Breaches of storage and data security obligations are treated less harshly, with a fine of ‘up to’ EUR€10,000,000 or 2% of *global* turnover

¹⁹⁰ *Bundesdatenschutzgesetz* (n 9) s 25

¹⁹¹ *GDPR* art 44.

¹⁹² *GDPR* art 45.

¹⁹³ *GDPR* art 46.

¹⁹⁴ ‘Adequacy decisions’, *European Commission* (Web Page, accessed 20 November 2022)

<https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en/>.

¹⁹⁵ *Maximilian Schrems v Data Protection Commissioner* (C-362/14) [2015] ECLI:EU:C:2015:650.

¹⁹⁶ *Ibid* 24-25 [91]-[98].

¹⁹⁷ *Bundesdatenschutzgesetz* art 74

¹⁹⁸ See below at section V(C).

¹⁹⁹ *GDPR* (n 8) art 77

²⁰⁰ *Ibid* arts 78-79

²⁰¹ *Ibid* art 82. Contributory negligence by the individual is factored in by *Bundesdatenschutzgesetz* art 83(1).

²⁰² *GDPR* (n 8) art 83(2)(b).

²⁰³ *Ibid* art 83(2)(f).

²⁰⁴ *Ibid* art 83.

from the previous year – whichever is greater.²⁰⁵ By contrast, more serious breaches of ‘basic principles’ like consent, ‘data subjects’ rights’, and improper cross-border transfers carry penalties ‘up to’ the greater of EUR€20,000,000 or 4% of the previous year’s global turnover.²⁰⁶

V COMPARISON

A Fundamental Principles

Generally, the APPs and the *GDPR*’s fundamental principles overlap. Indeed, there are broad APP analogues for most *GDPR* principles (other than minimal necessary collection),²⁰⁷ although the *GDPR* uses much stricter, clearer terms. The most significant difference between the two is that, whereas the APPs are exhaustive, the *GDPR* provides an additional body of data rights, as detailed at 5.2 below. The other main difference is structural, and goes to the legal environment within which each enactment sits. Where the APPs are prescriptive sovereign national legal rules, and thus better understood as rules than as principles, the *GDPR* is a supranational instrument designed to influence member state laws as much as to lay down rules of its own. Commonwealth law has no need to guide State/Territory laws in this way, simply overriding them to the extent that the two conflict.²⁰⁸ Differences between the *Privacy Act* and *GDPR/Bundesdatenschutzgesetz* become more pronounced as regards storage and transfer rules, however.

B Storage and Transfer Rules

Of the three areas of comparison, storage and transfer rules arguably differ most. The APPs only require that data be destroyed or de-identified once APP entities ‘no longer [need it] for any purpose for which [it] may be used or disclosed...under [the Act]’²⁰⁹ – giving such entities abundant discretion. By contrast, the *GDPR/Bundesdatenschutzgesetz* proceed on the principle of storage no longer than

²⁰⁵ *Ibid* art 83(4).

²⁰⁶ *Ibid* art 83(5).

²⁰⁷ See table four, below.

²⁰⁸ *Commonwealth Constitution* s 109. There has been extensive HCA jurisprudence on s 109, see, inter alia, *Ex parte McLean* (1930) 43 CLR 472, 483-484 (Dixon J); *Victoria v The Commonwealth* (1937) 58 CLR 618, 630-631 (Dixon J); *Telstra Corporation Ltd v Worthing* (1999) 197 CLR 61, 76; *Jemena Asset Management (3) Pty Ltd v Coinvest Ltd* (2011) 244 CLR 508. For a recent prominent example, see *Commonwealth v Australian Capital Territory* (2013) 250 CLR 441 (‘*Marriage Equality Case*’). See also Dan Meagher et al., *Hanks Australian Constitutional Law: Materials and Commentary* (LexisNexis Butterworths, 10th ed, 2016) 567-616; Anthony J Connolly, *The Foundations of Australian Public Law: State, Power, Accountability* (Cambridge University Press, 2017) 168-170.

²⁰⁹ *Privacy Act 1988* (Cth) sch 1 pt 4 ss 11.2(b), (d). Emphasis added.

necessary,²¹⁰ and require data-holders to disclose how long they will hold data and to explain individuals' right to erasure.²¹¹ Similarly, whereas the *Privacy Act* requires only 'such steps as are reasonable in the circumstances to protect [data]',²¹² the *GDPR/Bundesdatenschutzgesetz* proscribe onerous and detailed data security standards.²¹³ Taken together, it is likely that a *GDPR*-style storage and security regime would have sharply circumscribed the reach of the Optus/Medibank hacks, either by compelling greater security beforehand, or by reducing the volume of (identifiable) data available to the hackers. *Privacy Act* rules on cross-border transfers are stronger, and indeed take a similar approach to the *GDPR/Bundesdatenschutzgesetz* by requiring 'such steps as are reasonable in the circumstances to ensure that...overseas recipient[s do] not breach the [APPs]',²¹⁴ though this is still not as severe as the European Commission's 'adequacy' threshold for overseas data protection laws.²¹⁵ Domestic transfer rules are prone to abuse, however, allowing non-consensual transfers as long as they 'relate to the primary purpose [of collection]' and individuals 'would reasonably expect' them.²¹⁶ Again, the *GDPR/Bundesdatenschutzgesetz* here place a much heavier emphasis on informed consent,²¹⁷ and individual rights to object and/or opt-out.²¹⁸ Crucially, in terms of both storage and transfer, the *Privacy Act* only very sparingly employs the language of rights.²¹⁹ By contrast, the idea of 'data rights' permeate the European approach both constitutionally and at the *GDPR/Datenschutz* level. Where the APPs are provided as rules for agencies/organisations, the *GDPR/Bundesdatenschutzgesetz* are focused squarely on the protection and enforcement of individual rights.

C Penalties

Privacy Act and *GDPR/Bundesdatenschutzgesetz* convergence on penalties is already in-train with the government's recent *Privacy Act* amendments.²²⁰ Though not stratifying graver and lesser breaches as in Europe, proposed amendments borrow the *GDPR*'s 'greater of' mechanism based on numerical fines/annual turnover.

Table Six

Maximum data breach fines: Comparison as applied to the Optus case

²¹⁰ *GDPR* (n 8) art 5(1)(e); *Bundesdatenschutzgesetz* (n 9) s 47(5).

²¹¹ *GDPR* (n 8) art 13(2)(a)-(b); *Bundesdatenschutzgesetz* (n 9) ss 55, 57.

²¹² *Privacy Act 1988* (Cth) sch 1 pt 4 s 11.1.

²¹³ *GDPR* (n 8) arts 25, 32, 35; *Bundesdatenschutzgesetz* (n 9) ss 64, 67.

²¹⁴ *Privacy Act 1988* (Cth) sch 1 pt 3 s 8.1.

²¹⁵ *GDPR* (n 8) art 45.

²¹⁶ *Privacy Act 1988* (Cth) sch 1 pt 3 s 6.2(a).

²¹⁷ Cf *Privacy Act 1988* (Cth) sch 1 pt 3 s 6.1(a).

²¹⁸ *GDPR* (n 8) arts 6(1)(a), 7, 8, 9(2)(a), 13(2)(c), 14(2)(d), 17, 18, 21; *Bundesdatenschutzgesetz* (n 8) s 51.

²¹⁹ Cf *Privacy Act 1988* (Cth), long title, citing *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976); *Australian Human Rights Commission Act 1986* (Cth).

²²⁰ *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* (Cth).

(based on Optus' annual worldwide turnover FY2021/22: AUD\$7.836bn) ²²¹				
Privacy Act s 13G, amended by Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth)		GDPR art 83		
			Lesser breaches (art 83(4))	Greater breaches (art 83(5))
Greater of	30% of FY2021/22 'adjusted turnover' (max: AUD\$2.3508bn)	Greater of	2% of total worldwide annual turnover FY2021/22: EUR€156.72m	4% of total worldwide annual turnover FY2021/22: EUR€313.44m
	AUD\$50m		EUR€10m	EUR€20m

Though this is a promising development, penalties offer an example of learning from European mistakes as much as successes. The EU has a tradition of exemplary penalties, notably in the antitrust law space.²²² Though fines with global scope numbering into the millions (and billions) of euros capture headlines,²²³ their efficacy is not uncontested. Some contend that such fines are misdirected and unduly burden shareholders.²²⁴ Others argue that they do not significantly impact offending organisations' balance sheets, though a similar number hold that they do.²²⁵ There is some support for the idea that corporate cultures would better be changed – and thus the risk of repeat-infringement lowered – by attaching civil liability to organisational leadership.²²⁶ Such proposals utilise the common law vehicle of directors' duties, and penalties like disqualification which only affect responsible leadership,²²⁷ as well as fines mitigated by best practice behaviours.²²⁸ Currently, however, the *Privacy Act* and *GDPR/Bundesdatenschutzgesetz* only conceive of whole-of-organisation penalties for failures like data breaches, though the *GDPR* does account for best practice.²²⁹ Neither regime accounts for individual liabilities in the

²²¹ Optus, 'Optus delivers growth in a challenging year' (Media Release, 27 May 2022) 3.

²²² See, recently, *Google LLC and Alphabet, Inc. v European Commission* (European General Court, T-604/18, ECLI:EU:T:2022:541, 14 September 2022); *Summary of Commission Decision of 18 July 2018 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.40099 – Google Android)* [2019] OJ C 402/19; Foo Yun Chee, 'Google loses challenge against EU antitrust decision, other probes loom', *Reuters* (Web Page, 15 September 2022) <<https://www.reuters.com/technology/eu-courts-wed-ruling-record-44-blm-google-fine-may-set-precedent-2022-09-14/>>. See also Vanessa Franssen, 'The EU's Fight Against Corporate Financial Crime: State of Affairs and Future Potential' (2018) 19(5) *German Law Journal* 1222; Dreher and Kulka, *Wettbewerbs- und Kartellrecht* (n 40) 699-725.

²²³ This paper follows the uncapitalised spelling of 'euro', per the European Commission's *English Style Guide* (European Union, 2021) 48 [8,5].

²²⁴ Alexander Reuter, 'EU Corporate Fines Hit the Wrong and Fail their Purpose: Empirical Considerations and their Consequences from the Perspective of Shareholders' Fundamental Rights' (2020) 10(3) *European Criminal Law Review* 365.

²²⁵ See, eg, Luca Aguzzoni, Gregor Langus, and Massimo Motta, 'The Effect of EU Antitrust Investigations and Fines on a Firm's Valuation' (2013) 61(2) *Journal of Industrial Economics* 290; Adrian Ford et al., 'The Impact of GDPR Infringement Fines on the Market Value of Firms' (Conference Paper, University of East London, July 2021).

²²⁶ See, inter alia, Nick Werle, 'Prosecuting Corporate Crime when Firms Are Too Big to Jail: Investigation, Deterrence, and Judicial Review' (2019) 128(5) *Yale Law Journal* 1368; Gregory M Gilchrist, 'Individual Accountability for Corporate Crime' (2018) 34(2) *Georgia State University Law Review* 335. But see (albeit in the criminal context) Samuel W Buell, 'The Responsibility Gap in Corporate Crime' (2018) 12(3) *Criminal Law and Philosophy* 471.

²²⁷ Samet Caliskan, 'Individual Behaviour, Regulatory Liability, and a Company's Exposure to Risk: The Deterrent Effect of Individual Sanctions in UK Competition Law' (2019) 10(6) *Journal of European Competition Law & Practice* 386; Andreas Stephan, 'Disqualification Orders for Directors Involved in Cartels' (2011) 2(6) *Journal of European Competition Law & Practice* 529. See generally, on common law directors' duties in Australia, Stephen Bottomley et al., *Contemporary Australian Corporate Law* (Cambridge University Press, 2018) 258-286.

²²⁸ Karl Hofstetter and Melanie Ludescher, 'Fines against Parent Companies in EU Antitrust Law: Setting Incentives for "Best Practice" Compliance' (2010) 33(1) *World Competition* 55.

²²⁹ *GDPR* (n 8) art 83(2).

corporate setting, although the Australian Securities and Investment Commission has expressly adverted to the overlap between cyber security and directors' duties. Furthermore, the Federal Court of Australia recently held that failure to adequately manage cybersecurity risks breached licensing requirements in the case of *ASIC v RI Advice Group Pty Ltd*.²³⁰ Considering these developments, it is likely that directors' duties will be expanded in this space.

VI RECOMMENDATIONS

A *Discrete Data Rights Would Benefit Breach Victims*

The APPs strike a difficult balance between regulating organisational conduct and safeguarding individuals. Although some individual data rights are provided in the *Privacy Act*, their language is inaccessible and oblique. Compare the right to opt-out of data collection:

Table Seven

Comparing the language of 'opting-out' in the <i>Privacy Act</i> and the <i>GDPR</i>	
<i>Privacy Act</i>	'At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances...' ²³¹ ...to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances...[including] ²³² ...the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity' ²³³
<i>GDPR</i>	The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. ²³⁴

Important rights like informed consent and erasure are not covered by the APPs, with those that are being presented with undue complexity. **Clearly written data rights would enable individuals to effectively enforce data protection violations against them.** Additional rights should also be added to the APPs, especially those which minimise unnecessary storage, including:

- The right to data erasure;

²³⁰ [2022] FCA 496, see especially 13-14 [58]-[66].

²³¹ *Privacy Act 1988* (Cth) sch 1 s 5.1.

²³² *Privacy Act 1988* (Cth) sch 1 s 5.1(a).

²³³ *Ibid* s 5.2(e).

²³⁴ *GDPR* (n 8) art 7(3).

- The right to withdraw consent for data storage/transfer at any time; and
- The right to request data storage be restricted to the minimum necessary amount.

B Storage Rules Should be Reinforced

One of the main critiques of Optus following its hacking was that data had been held significantly longer than necessary. The *Privacy Act* enabled Optus to justify long-term retention as necessary ‘for any purpose for which [that data] may be used or disclosed’.²³⁵ A better approach, to borrow from Australian Tax Office Second Commissioner Jeremy Hirschhorn, would be to treat data like uranium rather than gold.²³⁶ **APP 11.2 should be amended to constrain how long data can be stored, and when it must be destroyed/de-identified:**

Table Eight

Improving data storage protection in APP 11.2	
Current Wording	<p>‘If</p> <p>(a) an APP entity holds personal information about an individual; and</p> <p>(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under [the APPs]; and</p> <p>(c) the information is not contained in a Commonwealth record; and</p> <p>(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;</p> <p>the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.’²³⁷</p>
Proposed Change	<p>If</p> <p>(a) an APP entity holds personal information about an individual; and</p> <p>(b) the information is not contained in a Commonwealth record; and</p> <p>(c) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;</p> <p>it must store that information no longer than is necessary for the specific purpose for which the data was obtained. Thereafter, the entity must immediately take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.</p>

Further, **more onerous GDPR-style data security provisions should also be introduced to replace APP 8**, requiring more than ‘such steps as are reasonable in the circumstances’. Although compliance would necessitate initial and continuing costs,²³⁸ these would be

²³⁵ *Privacy Act 1988* (Cth) sch 1 pt 4 s 11.2(b).

²³⁶ Jeremy Hirschhorn, ‘Commissioner’s Address’ (Speech, The Tax Summit: Shine Together, 20 October 2022). See also Lisa Cornish, “‘Treat data like uranium’: Lessons from the ATO playbook”, *The Mandarin* (Web Page, 16 November 2022) <<https://www.themandarin.com.au/205337-treat-data-like-uranium-lessons-from-ato-playbook/>>.

²³⁷ *Privacy Act 1988* (Cth) sch 1 s 11.2. Emphasis added.

²³⁸ *The Age of Privacy: The Cost of Continuous Compliance – Benchmarking the Ongoing Operational Impact of GDPR & CCPA* (Report, DataGrail, updated February 2020) 3-7.

mollified by both reduced criminal breach incidences and potential benefits under an EU-Australia FTA, by bringing Australia closer to achieving ‘adequacy’ in the view of the European Commission.²³⁹

C *Coupling Stronger Penalties with Directors’ Duty Approaches Could Increase Efficacy*

The government’s breach penalty amendments clearly mirror the European approach to corporate compliance.²⁴⁰ Although these reforms are commendable, **civil penalties for individual leadership should also be established under the remit of directors’ duties.** Discretion, as with fines, would remain with the judiciary, but would nonetheless render those individuals supervising for ‘serious and repeated interferences with privacy’ directly accountable.²⁴¹ This, in turn, could meaningfully change corporate culture in a manner which fines can struggle to do, thereby stemming repeat violations.

D *Closer Privacy Act-GDPR Alignment Would Benefit Australian Business*

Closer *Privacy Act-GDPR* alignment—especially in terms of data storage and security (and possibly also data transfer) rules—would carry tangible economic benefits for Australian business. Such reforms would elevate Australia to ‘adequate’ data protection status in the European Commission’s eyes, duly opening the single market up to Australian e-commerce. With EU market penetration by e-commerce representing 20% of annual enterprise turnover at a value of some USD\$828bn annually,²⁴² and three-quarters of Australian businesses earning part of their revenue in that space,²⁴³ long-term benefits would outweigh the initial costs of bringing data handling and security up to compliance. A concluded EU-Australia FTA—the negotiation of which is surely obstructed by the question of data protection guarantees—would only boost this market access and economic benefit further. However this is done, *some* reform towards more stringent data protection is necessary for Australian business to reap these benefits.

²³⁹ See below at section VI(D).

²⁴⁰ Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth).

²⁴¹ *Privacy Act 1988* (Cth)

²⁴² ‘Share of enterprises’ turnover on e-commerce - %’, *Eurostat* (Web Page, 17 March 2022)

<<https://ec.europa.eu/eurostat/databrowser/view/tin00110/default/line?lang=en>>; Lynn Beyrouthy, ‘E-commerce in the European Union – statistics & facts’, *Statista* (Web Page, 17 November 2022) <<https://www.statista.com/topics/3792/e-commerce-in-europe/#dossierKeyfigures>>; Christopher Hughes, ‘Distribution of businesses with e-commerce revenue in Australia 2021, by share of revenue’, *Statista* (Web Page, 7 June 2022)

<<https://www.statista.com/statistics/1102139/australia-share-of-businesses-with-e-commerce-revenue-by-share-of-revenue/>>.

²⁴³ Statista Research Department, ‘E-commerce in Australia – statistics & facts’, *Statista* (Web Page, 24 June 2022)

<<https://www.statista.com/topics/7683/e-commerce-in-australia/#dossierKeyfigures>>.

VII CONCLUSION

The ever-evolving data age, and the threats that this evolution brings, demand much of data protection regulation. Legislators are forced constantly to re-evaluate the stringency and scope of applicable law, as the *Privacy Act*'s long history attests. From initially guarding against the perceived overreach of government, to reacting to the internet and data ages, each new development has necessitated significant change. In the light of unprecedented data breaches in recent years, the tightening of storage, transfer, and security rules and penalties has emerged as a regulatory priority. In the *GDPR* and its national-level counterparts like the *Bundesdatenschutzgesetz*, Europe has fundamentally redesigned data protection law for this new age. They have done this by creating and prioritising individual data rights, thrusting the onus of compliance even more firmly onto data-holding organisations, and significantly reducing the amount of data available to criminal actors. Whether Australia chooses to follow this approach – as it is doing with penalties – or not, the Optus/Medibank breaches demonstrate that it nonetheless faces the same challenges. The advantages of pursuing *GDPR*-style reforms, however, are clear. Breaches, when they do occur, reveal less compromising information, duly reducing the costs that ensue. Data-holders are compelled to take measures which minimise breach risks, and can be brought to account by regulators and individuals alike. Stricter penalties, coupled with a focus on directorial conduct gleaned from the shortcomings of EU-style penalty regimes, can positively change organisational behaviour vis-à-vis data protection. Trading partners, reassured by a safer data environment, are more willing to open themselves up in the rapidly growing e-commerce space. Taken together, Australia is left with a stronger and more effective data protection regime, positioning it ideally for the future challenges of the data age.

With the support of the
Erasmus+ Programme
of the European Union



Jean Monnet Centre of Excellence for EU-Australia Economic Cooperation

The Jean Monnet Centre of Excellence for European Union–Australia Economic Cooperation at The Australian National University consolidates and expands understanding of EU–Australian economic cooperation at a pivotal moment in the bilateral relationship.