GRIFFITH UNIVERSITY

# A New World Standard? Why Australian Businesses should be Ensuring their Compliance with the EU General Data Protection Regulation


## Author

Englezos, Elizabeth

## Published

2019

## Journal Title

Intellectual Property Forum

## Version

Version of Record (VoR)

## Rights statement

© 2019 IPSANZ. The attached file is reproduced here in accordance with the copyright policy of the publisher. Please refer to the journal's website for access to the definitive, published version.

## Downloaded from

http://hdl.handle.net/10072/388752

## Griffith Research Online

https://research-repository.griffith.edu.au

# A New World Standard? Why Australian Businesses Should be Ensuring their Compliance with the EU *General Data Protection Regulation*

**Elizabeth Englezos**[1]

## Introduction

The *General Data Protection Regulation* ("GDPR")[2] was the product of a revolutionary process of law-making in the European Union ("EU"). The GDPR is designed to accommodate transborder flows of information and to apply equally regardless of jurisdiction. The extra-territorial scope of the GDPR requires countries and organisations outside the EU to understand and even adopt GDPR-compliant processes in order to retain access to EU data. The result is a GDPR that intends and possibly hopes to be de facto adopted worldwide. At the very least, the GDPR will shape and inform advancements in information law for years to come, and become a foundational part of information and privacy law. Anyone processing or controlling EU data will need to be compliant with GDPR obligations.[3]

While the similarities with Australian legislation such as the *Privacy Act* 1988 (Cth) ("Privacy Act") and development of new legislation such as the proposed *Data Sharing and Release Act* and the new Consumer Data Right proposed by the Australian Competition and Consumer Commission ("ACCC") (in response to the 2017 Productivity Commission Report on Data Availability and Use) may bring Australian law into closer alignment with GDPR requirements, other government reforms such as the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 seem to prevent the negotiation of any overarching agreements between Australia and the EU in the near future. Australia is currently negotiating a free-trade agreement with the EU. As a block, the EU is Australia's second largest trading partner, third largest export destination, and second largest services market. The EU was also Australia's largest source of foreign investment in 2017.[4] This means that Australia can ill afford to ignore the GDPR. However, exemptions or concessions created under this agreement will not enter into force in the immediate future.[5] Proactive adoption of GDPR-compliant mechanisms now will prepare Australian businesses for inevitable changes to Australian privacy and consumer policies,[6] enable continued access to crucial EU data and markets, reduce the risk of hefty penalties and sanctions for failing to meet GDPR requirements, and may help counter any shortfall between Australian legislative protections and GDPR requirements.

To provide a proper understanding of the GDPR, this article traces its evolution and attendant controversies, as well as the new protections and safeguards created by the GDPR. As Australia remains a net importer of useful and exploitable information through the global information infrastructure, the GDPR is arguably current best practice for Australian businesses and the factors that influenced the GDPR's development are particularly salient. In the *Data Availability and Use* report, the Australian Productivity Commission noted that Australia is:

> *… too small a country to stem or redirect the global tide of data generation, sharing and use [and cannot] exert much control over what large companies that collect Australian's data do with it …*[7]

In order to continue Australia's tradition of globally-focussed trade and engagement, understanding the origins, evolution and requirements of the GDPR will be critical to our ongoing participation in the lucrative and substantial EU market.

The article is structured as follows: the next part provides a brief snapshot of the current and emergent privacy and data legislation within Australia followed by a chronological overview of the development of the GDPR including the foundational directives, guidelines and cases that contributed to the regulation in its present form. The following discussion analyses the extraterritorial scope of the GDPR and the lack of clarity regarding its precise application and then reviews some of the more contentious aspects of the GDPR during its development. The article then considers the implementation of GDPR protections in third countries and reviews the updated privacy policies of both Google and Fitbit as case studies to illustrate the impact of the GDPR. The article concludes that the GDPR provides a best practice standard which will guide current and future information exchange policies and notes that implementation is not impossibly complex. By adopting GDPR compliant policies now, Australian business can ensure continued access to EU data while at the same time preparing for future Australian Law Reforms.[8]

### Australia's Data and Privacy Protections

The Privacy Act remains the key legislation regarding individual privacy and data protection rights for Australians. The 2017 Productivity Commission report on *Data Availability and Use* identified several important areas for further privacy reforms including a creation of new consumer rights that provide greater insight and control over how an individual's personal data is collected and used, the right to view and edit their personal data held by others, and a right to receive or transfer a copy of their personal data to a nominated third party.[9] The Commission also proposed new legislation, the *Data Sharing and Release Act*, to streamline data and privacy protection law and to provide a broad-reaching framework capable of extending beyond current technologies and policies and allows for a scalable approach that ensures the protections offered are proportionate to the sensitive (or non-sensitive) nature of the data involved.[10] Further amendments to the Privacy Act in February 2018 expanded these protections to include a notifiable data breach scheme and now requires Australian businesses to notify consumers in the event of any data access or disclosure which is "likely to result in serious harm to any of the individuals to whom the information relates".[11] In May 2018, the Australian Government responded to the Productivity Commission report by introducing a new Consumer Data Right ("CDR") which began with the banking, electricity and telecommunications sectors before rolling out to other market sectors over time.[12] The CDR will allow consumers to request access to their personal data, as well as its transfer to third parties on their behalf.[13] While there are many parallels between Australian protections and the GDPR, there are also significant differences between the two, particularly in the application of their "GDPR-equivalent" provisions. The following table outlines the key differences between the GDPR and Australia's current privacy laws.[14]

| | **General Data Protection Regulation** | ***Privacy Act* 1988 (Cth)** |
|---|---|---|
| Who does it apply to? | Controllers or processors of data:<br>• with an establishment in the EU; or,<br>• outside the EU that offer goods or services to individuals in the EU, or that monitor the behaviour of individuals in the EU.<br>There are no exemptions for small businesses. | Government agencies.<br>Private sector and not-for-profit organisations which are:<br>• incorporated in Australia ow which carry on a business in Australia; and,<br>• collect personal information on Australians or hold that information within Australia<br>Does not apply to organisations with an annual turnover less than AU$3 million.<br>Includes private health service providers and some small businesses. |
| What data is covered? | Personal data – any data or information relating to an identified or identifiable person. | Personal information – includes information or opinions about identifiable individuals or an individual who is reasonably identifiable. |
| Quality of consent | Must be:<br>• freely given, specific and informed;<br>• indicative of an unambiguous indication of the data subject's wishes; and<br>• given in the form of a statement or clear affirmative action | Must be:<br>• gained after individual has been adequately informed of the purposes for data collection;<br>• given by someone capable of giving and communicating their consent;<br>• voluntary; and<br>• current and specific to the purposes for collection. |
| Rights of data subject | Rights include:<br>• right to erasure or rectification (art 17);<br>• data portability; and<br>• right to object to the collection of their data. | At present, no equivalent rights exist in Australia, however, the Productivity Commission has recommended that Australians should have greater insight and control over how their data is used and recommends:<br>• a right to view collected data and request edits;[15] and<br>• a right to receive a machine-readable copy of their information or to have that information passed on to a nominated third party.[16]<br>The new Consumer Data Right[17] will have some applications similar to the right of data portability as provided by Article 20 of the GDPR. |

| | General Data Protection Regulation | *Privacy Act* 1988 (Cth) |
|---|---|---|
| Overseas transfer of information or data | Permitted in limited circumstances such as:<br>• where receiving country is deemed to be "adequate" and thereby provides sufficient data protections;<br>• where receiving company or organisation applies the "standard data protection clauses" or "Binding Corporate Rules"; or<br>• where receiving entity follows an approved code of conduct or has received prior certification. | Before disclosing personal information, the business must ensure that the recipient will not breach the Australian Privacy Principles.<br>Should the recipient breach any of the Australian Privacy Principles, the entity transferring the information is accountable for the breach. |
| Notification of Data Breaches | Data Breach notifications are mandatory for controllers and processors under arts 33—34 | Amendments to the Privacy Act now mandate reporting where a data breach has occurred and is likely to result in a real risk of harm to the data subject.[18] |
| Accountability and governance | Controllers must:<br>• implement sufficient and appropriate technical measures to ensure data is protected and business operations remain GDPR compliance;<br>• appoint a data protection officer; and<br>• undertake compulsory data protection impact assessments. | Organisations must:<br>• take reasonable steps to ensure compliance with Australian Privacy Principles; and<br>• appoint key roles and responsibilities to facilitate privacy management and conduct privacy impact assessments. |
| Sanctions | Fines of up to EU€10-20 million or 2-4 percent of annual turnover (which ever is greatest). | Facilitative, investigative and enforcement powers to ensure compliance are set out in the Privacy Act Parts IV and V. |

Having now identified the key differences between the GDPR and Australian law as well as the areas of Australian law ear-marked for review, this article will now examine the evolution of the GDPR and its structure before focussing more deliberately on the GDPR's expanded scope and the increased protections which differentiate the GDPR from current Australian data protection law.

### The evolution of the GDPR

The evolution of the GDPR was a slow and deliberate process guided by privacy ideals and shaped gradually by reforms, legal challenges and case law. The GDPR came into effect on 26 May 2018.[19] The GDPR intends to be "future-proof" and remain "technologically neutral and fit for innovation", thereby ensuring "that the fundamental right to personal data protection is guaranteed for all". [20] To address the vast prevalence of modern technology,[21] the GDPR builds upon the principles of the Organisation for Economic Co-operation and Development ("OECD") *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*[22] ("OECD Guidelines") and the *Data Protection Directive* 95/46/EC of October 1995 ("DPD")[23] to ensure uniformity of protections within EU Member States and third countries.[24]

At present, the EU is comprised of 28 sovereign nations. The *Treaty on the Functioning of the European Union*[25] enabled the European Council and Parliament to use regulations to enact national legislation by means of ordinary legislative procedure.[26] Regulations are binding legislative acts that must be applied in their entirety within EU Member States.[27] Consequently, Regulations such as the GDPR guarantee uniform legislation across the EU while directives allow some discretionary modification by the enacting State.[28] Thus, directives are a secondary form of EU legislation which are legally binding but depend on the government of individual Member States to transpose them into national law,[29] and allows national authorities to decide the form and method of implementation.[30] The breadth of legislative discretion allowed in the directive will determine whether each State will enact laws which are either identical to, or merely similar to those of the directive.[31] Guidelines such as the OECD Guidelines are not binding,[32] and have "great moral force as representing the will of [OECD members]".[33] The 1980 OECD Guidelines represented the first attempt at uniform personal data laws and provided a non-binding model for individual nations to consider when drafting data security legislation.[34] The OECD Guidelines were first adopted on 23 September 1980 and proposed eight principles for the processing and regulation of personal data:

1. Data should not be collected unless lawful to do so and where the data subject knows of its collection or has consented to it ("Collection Limitation Principle").[35]
2. Collected Data must be accurate, complete, up-to-date and relevant to the purpose of collection ("Data Quality Principle").[36]
3. The purpose of data collection should be specified at the time of collection and should not be used for any other purpose unless consented to by the data subject or permitted by law ("Purpose Specification Principle").[37]

4. Data should only be used in accordance with the disclosed purposes for collection unless permitted by law or with the subjects' consent ("Use Limitation Principle").[38]
5. Secure data storage measures must be in place to protect personal data against risks and losses such as unauthorised access, disclosure, modification or destruction ("Security Safeguard Principle").[39]
6. The reasons, methods, nature and existence of the data, including the identities of those processing or controlling the data, should be transparent and open to the data subject ("Openness Principle").[40]
7. Data subjects should be informed when their data is collected. Data subjects also have the right to access their data, challenge inaccurate data, and to request erasure of data which is incorrect ("Individual Participation Principle").[41]
8. Data controllers are accountable for compliance or non-compliance with these prescribed guidelines ("Accountability Principle").[42]

The DPD sought to retain these principles while harmonising data protection laws across the EU[43] in a way that minimised obstacles to information flow.[44] The DPD also extended these protections to personal data transferred to "third countries" outside of the EU which provided the data was governed by EU Community law[45] or processed data at an establishment within a Member State or via the equipment of a Member State.[46] As a consequence, only third countries that provided the same levels of data protection could access EU-based data.[47] To address some of the complexities and uncertainties created by different data standards, further agreements with third countries were required. For example, the *EU-US Safe Harbor Agreement*[48] ("Safe Habor Agreement") was enacted to ensure the free flow of information between the United States and Members of the EU.[49] The EU Member States then transposed the DPD into national law based on the precise conditions of each State.[50] The European Parliament and the Council of the European Union supplemented the DPD in 2002 to address the pervasiveness of electronic communications and the lag between technology and the law and strengthen the privacy protections for natural persons.[51] The ubiquity of "cookies" – a form of spyware, hidden identifiers, or webbugs which may (or may not) offer legitimate benefits to the data subject[52] – led to further amendments in 2009.The 2009 amendment also addressed the prevalence of spam and monitoring of web traffic,[53] but failed to improve the protection of personal data in all cases.[54] The GDPR was intended to replace and update the DPD and ensure an unprecedented level of uniformity in data protection standards across the EU.[55] However, many concerns related to the DPD were the subject of litigation prior to and during the development of the GDPR.These cases are discussed below and given their influence on the development of the GDPR, provide important context for Australian businesses seeking greater clarity in whether the GDPR apples to their commercial transactions.

The extraterritorial reach of the DPD was questioned in *Weltimmo v Hungarian Data Protection Authority* ("*Weltimmo*").[56] In *Weltimmo*[57] the third chamber of the Court of Justice of the European Union ("CJEU") considered whether the *Weltimmo* company which was registered in Slovakia (and used the information of Hungarian businesses), could be sanctioned by the Hungarian Data Protection Authority and under Hungarian law.[58] The CJEU upheld the decision of the Hungarian Supreme Court and expanded the meaning of "establishment" under the DPD to any establishment that controlled data "through stable arrangements in the territory of [a] Member State, [and conducted any] real and effective activity – even a minimal one".[59] This interpretation is echoed in recital 22 of the GDPR.[60] The DPD's requirements (and, consequently, the GDPR), therefore, applied regardless of the nationality of the persons involved.[61] Australian businesses which use data collected from the EU or obtain information from establishments which have an effective link to an EU Member State therefore have an obligation to comply with the DPD, and consequently, the GDPR.

Five days later in *Schrems v Data Protection Commissioner* ("*Schrems v DPC1*")[62] the Grand Chamber of the CJEU considered whether the Irish Data Protection Commissioner had correctly rejected a request to prohibit Facebook's transfer of personal data to the United States.[63] The complainant, Maximillian Schrems, (who remains a user of Facebook today) is an Austrian national and lawyer who was concerned about the amount of personal data collected by Facebook.[64] After the 2013 Snowden revelations regarding the surveillance activities of United States Intelligence agencies and the National Security Agency ("NSA"), Schrems did not want his personal data processed in the United States.[65] Schrems filed a complaint with the Data Protection Authority which sought to prevent any further transfer of his data to US soil, Schrems' application was dismissed on the grounds that the Safe-Harbor Agreement prevented any intervention in the activities of US data processors.[66] The CJEU disagreed, holding that legislation which prevented individuals from pursuing any legal remedy in relation to their personal data did not "respect the essence of the fundamental right to effective judicial protection as enshrined in article 47[67] of the Charter."[68] *Schrems v DPC1*, therefore, conclusively invalidated the Safe Harbor Agreement which had previously protected information exchange with US-based establishments. This decision opened US-based establishments to complaints and required them to prove their compliance with their obligations under the (then) DPD before engaging with any EU data.[69] Interestingly, Schrems filed three further claims with the Data Protection Commissioners of Ireland (as a resubmission of the first claim), Belgium and Germany.[70] Schrems also brought a reformulated version of *Schrems*[71] before the CJEU again as *The Data Protection Commissioner v Facebook Ireland Limited & Maximilian Schrems*[72] in February 2017.[73] Schrems has

also sought a class action against Facebook in late 2017 in *Maximilian Schrems v Facebook Ireland Limited* (C-496/16)[74] but was denied standing to file claims on the behalf of other Facebook users.[75] In May 2018, Schrems filed cases against Facebook (and subsidiaries Whatsapp and Instagram) and Google (as the provider of the smart phone operating system) claiming that users of Facebook and Google etc. are "coerced" into giving consent. Coerced consent cannot be considered to be "freely given" and consequently, fails the requirements set out in Article 7.4 of the GDPR.[76]

The litigation by Maximillian Schrems confirmed that the GDPR's application had expanded beyond EU borders even before its implementation. While Article 3 describes the intended application of the GDPR, its actual reach remains unclear. What *is* clear, is that Australian businesses are not subject to any Safe-Harbor or other agreements which indemnify them from sanctions or penalties. Australian businesses need to be proactive about meeting GDPR standards. At the same time, the increasing parallels between current Australian law, proposed law reforms and the GDPR suggest that the effort invested in early compliance will be worthwhile. The following discussion outlines the structure of the GDPR before engaging in a detailed review of the provisions which will inform future questions as to the scope of the GDPR.

### The structure of the GDPR

The GDPR is comprised of 11 chapters:

- Chapter 1 contains general provisions which dictate the subject matter and objective for the GDPR[77] as well as its material[78] and territorial scope.[79] Article 3 is included within the general provisions chapter of the GDPR and gives the GDPR its extraterritorial reach. The next part of this article provides a detailed analysis of Article 3 and the extraterritorial reach of the GDPR.
- Chapter 2 outlines central principles of the GDPR such as lawful processing of personal data,[80] the revised requirements for consent, and special considerations for child data subjects.[81]
- Chapter 3 explains the rights of the data subject and implements the requirements for transparency in the data collection process,[82] as well as clarifying the width and breadth of the data subject's right to access information held about them.[83] This chapter also includes the new rights to data rectification, data erasure, data portability as well as the right to object to the collection or holding of data.[84] Chapter Three also includes restrictions on the use of automated decision-making processes and activities such as profiling.[85]
- Chapter 4 describes the obligations for Data Controllers and Data Processors within the EU. The creation of direct regulatory liabilities for data processors under the GDPR is a notable addition to the GDPR. Under the Directive, the processor was effectively an agent of the controller who had sole responsibility for all compliance matters.[86] Chapter Four also introduces the requirement for an internally appointed Data Protection Officer[87] and introduces the concepts of "Codes of Conduct"[88] and certification processes[89] for companies accessing EU data.
- Chapter 5 introduces the concept of "Adequacy Decisions" under Article 45.[90] The remainder of Chapter Five addresses compliance matters for third countries and including those subject to an adequacy decision, and legal persons who operate within third countries which have been deemed inadequate or have yet to receive a favourable decision.
- Chapters 6 and 7 continue the theme of consistency and protection regardless of venue and introduce the independent supervisory Authority.[91] Together, Chapters 6 and 7 codify the requirements of co-operation and consistency between the various regulatory bodies involved in GDPR enforcement.[92]
- Chapter 8 addresses remedies, liability matters and potential sanctions under the GDPR.
- Chapter 9 focuses on specific instances of processing such as employment purposes,[93] or the interplay between processing requirements and their effect on the freedom of information or expression.[94]
- Chapter 10 sets out the requirements for delegated Acts under the GDPR.
- Chapter 11 includes the final provisions of the GDPR such as the repeal of preceding directives,[95] relationship with previous agreements,[96] as well as enactment,[97] and legislative review of other Acts relevant to data protection.[98] Chapter 11 also institutes a process of continued review for the GDPR. From 25 May 2020,the European Commission is to provide a report on the efficacy and implementation of the GDPR to the European Parliament and Council.[99] The report must give particular consideration to Chapter Five (on data transfers to third countries) and Chapter Seven (on cooperation and consistency).[100] Findings of the European Parliament and European Council[101]should also be included as well as information from member states and supervisory authorities where deemed necessary by the commission.[102] As part of this report, the commission may also propose amendments or other alterations to the GDPR where necessary.[103]

For the purposes of this article, the key provision of the GDPR is Article 3 of Chapter 1 which details the extraterritorial scope of the GDPR and makes GDPR-compliance an important and pressing issue for Australian

legal persons who have an establishment in the EU, wish to continue accessing EU data or intend to continue their engagement with EU markets.

### The Expanded Scope and Increased Protections of the GDPR.

Current estimates suggest that more than 508 million people live in the EU.[104] Article 3 of the GDPR deliberately expands the territorial scope of the GDPR beyond those 508 million people and surpasses that of its predecessor, Article 4 of the DPD.[105] Article 4 stated:

> *(1) Each member state shall apply the national provisions it adopts pursuant to This Directive to the processing of personal data where:*
>
> *(a) The processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State …*
>
> *(b) The controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;*
>
> *(c) The controller is not established on Community territory, and for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community*[106]

As part of a Directive, Article 4 of the DPD was implemented according to the precise conditions of each Member State,[107] while GDPR Article 3 must be implemented *verbatim*.[108] Despite many similarities between the two texts, the inclusion of the words "whether the processing takes place in the Union or not" represents a vital difference between the GDPR and the DPD. *Weltimmo*[109] and *Schrems*[110] highlighted the practical difficulties of regulating transborder flows of information. Article 3 aims to clarify and simplify the application of the GDPR by explicitly stating the types of data which fall within its regulatory ambit:

> *(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*
>
> *(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
>
> *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
>
> *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*
>
> *(3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law [emphasis added].*[111]

Together with a new independent supervisory authority to settle disputes under Chapter 6 of the GDPR (the key article of which is Article 51),[112] Article 3[113] ensures that the new regulations are implemented consistently regardless of venue or geography.[114] While the GDPR does not apply to individuals who are collecting information for non-commercial use or during other household or personal activities,[115] Article 3 sets a minimum level standard for protection for any commercial entities accessing EU data,[116] "regardless of whether this processing takes place in the Union or not".[117]

A minimum standard of protection undoubtedly sets clear expectations for the privacy of those covered by the GDPR. However, the difficulty in demarcating the limits of the GDPR's application[118] is likely to prove problematic. The competing considerations of public international law and State sovereignty (also known as "conflicts of laws") rarely sit together without some concessions by one party or another. *Microsoft Corporation, Appellant v United States of America* [2016] 829 F.3d 197. ("*Microsoft Warrant Case*")[119] was a particularly important case which crossed jurisdictional borders and weighed national security considerations against the individual's right to privacy. United States criminal investigators sought access to a Microsoft user's information which was, at that time stored in Ireland.[120] A New York magistrate issued a warrant requiring Microsoft to disclose the contents and metadata of a Microsoft user's email account. Microsoft complied with the request for metadata but moved to quash the warrant for the email contents on the grounds that data stored in Ireland was beyond the jurisdiction of a US court.[121] The case was appealed to the Second Circuit Court of Appeals of the United States on 27 February 2018 before being withdrawn by the US Department of Justice on 30 March 2018.[122] The introduction of the US *Clarifying Lawful Overseas Use of Data (CLOUD) Act*[123] nullified the need for any decision in the *Microsoft Warrant Case*.[124] This was a lost opportunity for valuable guidance on the resolution of conflict of laws disputes that relate to criminal investigations. Of note, is a submission from the European Commission stating that where domestic laws create cross-border obligations, these laws should be applied and interpreted in a way that pays "mutual regard to the spheres of jurisdiction" of the legislating country. In addition, the venue of interpretation must be considered and any decision made in a manner consistent with international law.[125] It would, therefore, seem reasonable to infer that the Commission remains cognisant of the sovereign rights of non-Member States although the no decision was delivered by the US court. With this position in mind, EU case law on the equivalent provision of the DPD[126] provides some

further guidance on the conceivable limits of the GDPR's application. Despite the expressed acknowledgement of the sovereign rights of non-Member States, the cases mentioned below expanded the application of the DPD again, yet did little to define a clear limit.

Several cases have attempted to clarify the application of the DPD. As mentioned previously, *Weltimmo* expanded the nature of "activities" to those with any "real and effective activity" in a Member State.[127] Businesses or organisations with "stable arrangements" within a Member State must, therefore, comply with the data protection laws of that State.[128] According to *Verein für Konsumentinformation v Amazon EU Sàrl,*[129] *enquiries as to where* electronic commerce directs (any or all of) its activities can be used to resolve such jurisdictional issues. [130] If those activities were directed to a Member State was subject to DPD oversight, then the DPD would apply.[131] Businesses who seek to sell or offer services to parties within a Member State subject to DPD oversight were consequently required to comply with the DPD,[132] but what of international subsidiaries or offices of multinational companies?

*Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles ("Google Spain")*[133] considered similar jurisdictional issues to that of the *Microsoft Warrant Case*:[134] whether US-based Google Inc. is subject to the same EU laws as its local branch, Google Spain.[135] In *Google Spain,* the court held that processing or control also included endeavours which improved the profitability of an entity *within* a Member state.[136] While Google Spain was not the same entity as the US-based Google Inc, the success of Google Spain undoubtedly influenced the public opinion or perception of Google Inc. Google Inc, therefore was subject to the same laws as Google Spain. In *Pammer v Reerderei Karl Schlüter GmbH & KG,*[137] the CJEU also provided a non-exhaustive list of "indicators" which could be used to identify data activities which "target" consumers in the EU,[138] thereby requiring their compliance with the DPD. The decision flagged behaviours such as the use of certain languages or currencies in a company's online content as "indicators" of an intention to engage in activities[139] as outlined in Article 3.2 of the Regulation.[140] Furthermore, the abolition of protective agreements such as the *EU-US Safe Harbour Agreement* (invalidated by *Schrems*[141]) and replacement with the more stringent *Privacy Shield Framework*[142] ("Privacy Shield") "imposes stronger obligations on US companies exchanging data with EU states."[143] Unlike the Safe Harbor Agreement, the Privacy Shield does not absolve US traders from meeting their obligations under the GDPR. Instead, the Privacy Shield merely streamlines the compliance process and allows US traders to self-certify their GDPR-compliance rather than relying on external certification mechanisms.[144] This is a significant departure from the much softer Safe Harbour Agreement but remains an important concession for US businesses who have fewer compliance hurdles to cross than Australian businesses.

Businesses established in countries outside of the EU and the US have no such safeharbor agreements to protect them. Instead, non-Member States can apply for an "adequacy decision" under Article 45 of the GDPR. Article 45 empowers the Commission to assess the legislative protections afforded to data subjects in the applicant country and decides whether they are "adequate" when compared with those offered under the GDPR.[145] To date, only 11 countries (including Canada and New Zealand) have been granted adequacy by the Commission.[146] Fortunately, Article 45 also provides for adequacy decisions where organisations adopt appropriate safeguards[147] such as Binding Corporate Rules ("BCR"),[148] contractual obligations and inter alia Codes of Conduct ("CoC")[149] that have been approved by the supervisory authority. When such safeguards are implemented in accordance with Chapter 5 of the GDPR, the organisation may accept data transfers in the absence of any specific authorisation from a supervisory authority.[150]

Given new legislative developments such as the highly controversial *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (Cth) which would allow discretionary access to encrypted and personal communications,[151] it appears unlikely that Australia will receive a favourable adequacy determination within the foreseeable future. However, it remains a reality of the new global economy and the global movements of individuals that Australian businesses will not be exempt from meeting the GDPR's requirements. Even those businesses which attempt to abandon the EU markets entirely cannot guarantee they will not receive data from EU citizens. The simplest way for Australian businesses to ensure regulatory compliance and the free flow of EU data, therefore, appears to be to adopt these model codes and rules as provided by the European Commission. At the time of writing, the European Commission has published several working documents to assist the compliance process,[152] including guidance documents which set out the structural requirements for BCRs,[153] and a checklist that ensures BCRs are appropriately tailored to the Commission's requirements.[154] As time progresses, more and more service types (particularly those with online-based businesses) are publishing model codes of conduct online.[155] Some industry advisory bodies have published Codes of Conduct online for other industry members to use.[156] Other companies have made their *approved* BCRs available to the general public.[157] Consequently, countries and organisations within these third countries are expected to adopt GDPR-like protocols to ensure their obligations are met, expanding the influence of the GDPR even further.

In addition to formally expanding the application of the EU's data protection laws, the GDPR expands on the existing Directive and amendments[158] in the following ways:

- The regulations introduce penalties for those controlling the data as well as those processing the

data.[159] These penalties range from up to 2-4 per cent of worldwide annual turnover or EU€10-20 million (whichever is higher).[160] "Cloud" storage providers, i.e. those that provide off-site data storage for other businesses, are also captured by the GDPR.[161]

- Consent must follow clear and intelligible communication with the data subject that uses clear and plain language.[162] Failure to meet these requirements will nullify consent.[163]
- Data subjects must be informed 'without undue delay' in the event of any breach to data security.[164]
- The Right to Access now includes a right to know whether data has been collected and processed, by whom and for what purpose.[165]
- Once the original purpose for data collection is fulfilled, the Right to be Forgotten (or of "Data Erasure") allows the subject to request the erasure of their personal data.[166] The "right to erasure" must be "balanced against the public interest."[167]
- Data portability requires processors or controllers to provide any data they have accumulated on an individual to that individual on request and in a "commonly used machine-readable format".[168]
- The requirement for privacy by design and by default[169] requires systems to implement privacy protection measures from the design and implementation stage,[170] instead of a post hoc remedy or control.
- Legal persons processing large amounts of data must appoint a data protection officer[171] and consider devising and instituting a code of conduct[172] to ensure they comply with the Regulations.

Information collected by Member States for foreign policy or security purposes remain exempt from the regulations.[173] Information collected relating to criminal activities is also exempt.[174] The end goal of the regulation is to ensure a consistent level of protection for natural persons throughout the EU and to prevent inconsistencies which would otherwise hamper the free movement of personal data within the internal market.[175] The harmonisation of personal data protection law for EU data subjects means the GDPR has an indisputable[176] and anticipated[177] extraterritorial impact. The sheer volume of legal persons captured by this Regulation will place considerable demands on the authorities responsible for the monitoring and enforcement of the GDPR such as the new Data Protection Authority ("DPA"). However, it is the number of legal persons (whether as potential customers, data entities or rightsholders) that makes GDPR compliance so important for Australian businesses looking to engage freely with online data. Companies who choose to rely on questions related to the efficiency or capacity of the DPA as a justification for non-compliance with GDPR expose themselves to the significant risks of sanction or penalty as outlined above.

The creation of the DPA is one of many controversial aspects of the GDPR that have shaped its development and implementation. The following section provides an insight into the controversies surrounding the DPA, and reviews the debates surrounding Data Portability protections. The discussion also offers more information about the requirement for n internally appointed Data Protection Officers ("DPO") and offers some guidance as to whether Australian businesses will need to their own DPOs Understanding the intentions and debate surrounding these provisions will help clarify how and when they will apply to Australian businesses.

### Other controversial aspects of the GDPR

In 2016, the EU data market had an estimated value of almost EU€300 million.[178] Given the current impact of the GDPR on global information flows and the value of the European data market, it is essential to understand the controversies and concessions made during the negotiation process. The European Commission proposed its final draft of the Regulations on 25 January 2012.[179] The European Parliament offered a revised version of the document for first reading on 12 March 2014[180] after reviewing the opinions of EU several advisory bodies. The European Economic and Social Committee includes representatives from workers' and employers' organisations as well as other interest groups.[181] The Committee of Regions consists of locally and regionally elected representatives of all 28 Member States.[182] The European Union Agency for Fundamental Rights ("FRA") provided expert opinion and advice on fundamental rights issues[183] while the European Data Protection Supervisor gave recommendations based on past data initiatives.[184]

Generally speaking, the parliamentary draft offered more specific and stringent protections than those proposed by the Council or Commission,[185] while the Data Protection Supervisor's recommendations centred on perceived loopholes in the legislation. These sentiments were often echoed by other advisory bodies, for example, the Economic and Social Committee ("ESC") noted that the data subject's right to object to the processing of their data was valid *unless* the controller could demonstrate "compelling legitimate grounds" that overrode the "rights, interests and freedoms of the data subject".[186] The ESC argued that the term "compelling legitimate grounds" was too vague and therefore "rendered the right meaningless."[187] The FRA expressed concern about the ability of children between the ages of 13 to 18 to provide full and voluntary consent and re-iterated the importance of the new "right to be forgotten"[188] for children who consent to the collection of personal information.[189] These concerns were recognised in Recital 65 but remained absent from the final version of Article 17.[190] The Data Protection Supervisor's recommendations centred on perceived loopholes in the legislation. The following discussion considers each of these provisions in more detail as well as the reasons for the controversy.

***Article 51 - The "One-stop-shop" and the Data Protection Authority***

Chapter 6 of the GDPR creates an Independent Supervisory Authority, the Data Protection Authority ("DPA") which has the power to investigate,[191] warn[192] or reprimand[193] data controllers or processors who may have breached their duties under the GDPR. The DPA may also suspend data flows to a third country recipient or international company,[194] impose temporary or definitive bans,[195] and impose administrative fines (under Article 83).[196] Without the DPA, different courts of varying jurisdictions will hear disputes under the GDPR without referring to the relevant case law of other jurisdictions. The DPA therefore, can decide all GDPR-based disputes, regardless of jurisdiction, and ensure consistency wherever the GDPR applies. Withdrawing supervisory authority from locally-based, non-judicial institutions proved highly controversial. This creation of a "one-stop-shop" was the subject of long debates. Much of this centred on the capacity of a centralised authority to arrive at supervisory decisions quickly and without significant administrative burden.[197] Debates also involved efficiency concerns where the supervisory authority was not within reasonable proximity of the issue under assessment, as well as deciding *which* authority would be the "relevant supervising body."[198] The precise role of the European Data Protection Board remains controversial as well as its capacity to hear complaints and thereby mitigate some of these complexities.[199]

The DPA is likely to come under significant scrutiny during the early stages of its implementation. Efficiency will be an important indicator of success and will require judicious and expedient management of complaints and claims. Efficiency, in turn, will necessitate a degree of selectivity regarding the progress and handling of disputes. Svantesson warns that such "selectivity" may appear subjective, discretionary and arbitrary.[200] Inconsistent monitoring or enforcement by the DPA (whether deliberate, necessary or otherwise) may, therefore, pose a real threat to the harmony envisaged by the drafters of the GDPR. It is important that legal persons recognise that inconsistencies in application, investigation or the imposing of sanctions under the GDPR cannot guarantee that breaches or compliance failures will go unnoticed. If anything, these inconsistencies (if they exist) could see businesses in third countries, particularly those deemed to have "inadequate" protections monitored more closely by the DPA. While it remains difficult to predict when (and perhaps even if) Australian businesses will first draw censure from the DPA, the significance of these penalties, the value of the EU market and its data, and the developments in Australian law provide a compelling argument in favour of proactive compliance with GDPR standards.

***Article 20 - Data portability***

In addition to the data subjects' "right to know",[201] data portability allows subjects to request the transfer of any personal data held about them to other nominated third-parties.[202] This is an entirely new right for members of the EU and has never been the subject of treaty or EU national law. Before the GDPR, the Philippines was the only non-EU state to enact a right to data portability.[203] While there seems to have been universal acceptance of the idea behind data portability, the European Parliament's first draft struck out the entire section before later adopting it on first reading.[204] With the trilogues' records sealed to the public, it is unclear exactly what the most contentious issues were. However, in its final form, Article 20 has been reworded to include personal data which has been provided to a controller (where that data has been obtained in accordance with the GDPR), and requires that the data be made available "without hindrance" and transmitted to the new controller "where technically feasible".[205] The European Data protection supervisor noted that this right to data portability should not be limited to that which is provided with consent or under contract.[206] However, Article 20 remains specific to those forms of "provided" data.[207] The right to data portability therefore has limited application when compared to other rights such as the right to be informed of data collection that occurs without any participation by the data subject.[208] Some may argue that the right to data portability does not go far enough. Nonetheless, the right to data portability is likely to present an impressive security challenge to data controllers who will need to verify the identities of data subjects with which they have had minimal prior contact.[209] Failure to properly verify the identity of the data subject risks breaching data portability requirements and possible data security obligations.[210] The burden and risks associated with data portability obligations remain unclear, as do the preconditions for internally appointed Data Protection Officers. As mentioned previously, the Australian government has confirmed the implementation of a Consumer Data Right in Australia which will begin in the banking sector.[211] Australian companies which provide data portability to their data subjects now will be well-prepared for this requirement as it is progressively rolled out across subsequent sectors of the Australian market.

***Article 37 and the threshold requirement for Data Protection Officers***

Another important obligation under the GDPR is the requirement under Article 37 which calls for larger companies or commercial entities to appoint a Data Protection Officer ("DPO") to monitor and ensure the organisation's compliance with the GDPR. However, it is unclear which companies or commercial entities are "large" enough for Article 37 to apply. In its 2012 version, Article 37 (as it is now known) only applied to entities with more than 250 employees.[212] The European Parliament sought to qualify this further by proposing that the requirement apply instead to legal persons processing the data of "more than 5000 data subjects in any consecutive 12 month period."[213] The Data Protection Supervisor recommended that the lower

threshold of 250 employees be adopted and clarified.[214] The final version of the GDPR removed both qualifications stating only that companies should designate a DPO in any case where "the core activities … consist of processing operations which by virtue of their scope and/or purposes, require regular or systematic monitoring of data subjects on a large scale."[215] Recital 13 helps define the threshold by reintroducing the requirement of 250 employees and referring back to the original registration which provided the definitions for small and medium enterprises.[216] The recitals may also offer further guidance as to the types of processing and control envisaged by the GDPR. Recital 18 provides the anticipated exemption of personal and household use from the scope of the GDPR.[217] Recital 80[218] may also be of note and states that organisations which exist outside the EU but fall under its scope by way of Article 3,[219] are required to appoint a representative to liaise with supervisory authorities in the event of a complaint or dispute under the GDPR.[220] This requirement applies unless the processing is unlikely to pose a risk to the rights and freedoms of data subjects and is either occasional only, does not include the large-scale processing of special categories of personal data or data related to criminal convictions.[221] While not specifically related to the provisions related to Data Protection Officers,[222] Recital 80 offer some insights into the more nuanced considerations regarding the processing and control requirements for small to medium enterprises under the GDPR. It appears that Australian business with fewer than 250 employees will not need a DPO, but at the same time, there must be a designated liaison for supervisory authorities in case of a complaint. Australian businesses will need to carefully consider whether they must appoint an internal Data Protection Officer in order to comply with GDPR obligations and avoid the risk of penalties under the GDPR.

### "Inadequate" third countries and the continued flow of EU data

In part IV, I discussed third country adequacy decisions as a way of expanding the application of the GDPR beyond the European Economic Area. The European Commission has granted adequacy to New Zealand, Canada and Israel under Article 45 of the GDPR.[223] Japan too may soon receive an adequacy decision.[224] Australia has not and is unlikely to obtain adequacy without substantial legislative review and amendment. The Privacy Act (not only offers fewer protections than the GDPR, but those offered have much narrower scope than their GDPR counterparts.[225]

The Australian Government has agreed to implement a CDR (somewhat analogous to data portability under the GDPR).[226] however, the government response remained silent on the Productivity Commission's[227] recommendation regarding the right to object or request the erasure of personal data.[228] The ACCC has subsequently also indicated its support for such a right in its Draft Report as part of its *Digital Platforms Inquiry*. Reforms recommended by the Productivity Commission as consumer reforms, such as the proposed *Data Sharing and Release Act*,[229] seem likely to narrow the gap between the GDPR and Australian legislation by "giving individuals more control over their digital data,"[230] and helping Australians know "when [their] data has been sold".[231] Currently, Australian businesses will need to ensure organisational compliance individually. Compliance may be a daunting task, especially for small to medium businesses for whom the value of the EU market is unknown or unclear. Some Australian businesses may choose to withdraw from the European market as a result. However, withdrawing from the EU market may impede or limit expansion opportunities in the future and may not protect those companies that use EU market data for marketing or design and development purposes. However, once the right to data portability[232] has been implemented and the *Data Sharing and Release Act*[233] becomes part of Australian law, withdrawal from the EU market may only offer short-term benefits.

To assist Australian businesses engaged with the EU market or its data, the Office of the Australian Information Commissioner has provided some guidelines on how Australian companies can meet GDPR obligations.[234] Putting GDPR-compliant processes and procedures in place, regardless of whether or not the enterprise falls within the scope of Article 3, also provides collateral benefits for businesses which streamline their data protection policies within and across their entire organisational framework while ensuring adequate protections for EU data flows.[235] Compliance requires the implementation of safeguards such as binding corporate rules, or standard data protection clauses which ensure enforceable rights for data subjects and provide an avenue for effective legal remedies in the event of a breach.[236]

While a more detailed exposition of the implementation processes falls beyond the scope of this analysis, a review of Article 46 provides a concise summary of the various compliance frameworks suggested by the GDPR. Article 46 provides an apparently straightforward list of options for implementing the required safeguards which include:

- adopting legally binding and enforceable corporate rules;[237]
- adopting the Commission-approved standard data protection clauses[238] completely and without adulteration;[239]
- the adoption of a DPA approved and legally enforceable code of conduct;[240] or
- certification via an approved certification mechanism.[241]

While these requirements will prove burdensome initially, streamlining and unifying the privacy protections organisation-wide, will reduce the administrative work created by data transfer across business units and may generate public goodwill due to the increased data protections available to third country data subjects.[242]

Unfortunately, small to medium businesses may receive limited benefits in exchange for compliance – other than their continued access to EU data and collateral benefits as outlined above. Australia's privacy framework, as set out in the *Privacy Act* does not apply to small businesses with a turnover of less than AU$3 million per financial year.[243] No such exemptions apply under the GDPR, with only minor concessions for small businesses regarding the appointment of Data Protection Officers.[244] Reducing the red tape and costs for small to medium businesses is one of the key aims for Australia as free trade negotiations continue with the EU.[245] Craig McAllister of the Cornell University Office of Risk Management and Insurance has suggested that in the short-term, tax credits or rebates may be the most appropriate way to minimise the costs and losses faced by small-medium businesses which fall within the scope of the GDPR.[246] Long-term, McCallister recommends legislative reforms to ensure an adequacy decision[247] for those countries currently deemed inadequate. It is important to note that McAllister's comments relate specifically to the US market which has more streamlined compliance processes as a result of the Privacy Shield.[248] As yet, no such agreement is in place to simplify the compliance process for Australian businesses.

Given that Australia has no applicable concessions regarding compliance, there is a strong argument in favour of the short-term and long-term recommendations discussed by McAllister. The GDPR forces Australian businesses to reassess their link with the EU and any dependence they may have on its data. However, given the significance of the EU market to Australian businesses, avoidance may not be possible. Government subsidies could help offset the implementation costs for small to medium businesses while ensuring that Australian Businesses remain engaged with the European market. Regardless, it appears that the adoption of GDPR-compliant procedures now will simplify the implementation of future reforms to Australian privacy, competition and consumer law, maintaining access to the lucrative EU market and avoiding penalties and sanctions of GDPR breaches.

***How has the* GDPR *been engaged extraterritorially?***

At the time of writing, there was a significant dearth of information on the implementation methods adopted by Australian and other third country businesses. To better understand the impact of GDPR obligations, I have conducted a brief review of the new privacy policies introduced by Google and Fitbit in preparation for the GDPR.

Both Google and Fitbit offer services which are largely dependent on access to unlimited user data. Interestingly, the two companies adopted notably different approaches: Google has sought greater transparency and offered increased protections regardless of the data subject's geographical location, while Fitbit appears to have taken an "opt-in or opt out but expect decreased functionality" approach. In the following discussion, some of the more telling changes to the privacy policies of each company are examined.

*Google*

Any discussion of a business or corporation should necessarily begin with an explanation of its market, its contribution to that market and perhaps an explanation of what makes it unique. As of May 2017, Google had over 2 million active mobile devices on Android operating systems alone per month.[249] This article therefore proceeds on the basis that the reader is familiar with the company and its products.

The key difference between Google's pre- and post-GDPR policies seem to lie in the adoption of a more user-focused and self-justificatory tone. The policy has been amended to include information on the export of user data (meeting the data portability requirement).[250] The category of "sensitive personal information" has been supplemented by a new category of "non-personally identifiable information."[251] The complies with GDPR requirements for pseudonymisation of information.[252] However, the user is also informed that data de-identified data that falls outside the scope of ordinary consent may still be shared with third parties.

> *We may share non-personally identifiable information publicly and with our partners – like publishers, advertiser, developers or rights holders. For example, we share information publicly to show trends about the general use of our services …*[253]

The difficulty, of course, with deidentified data is the relative ease of reidentification. This is not addressed in the policy statement.[254] The policy now offers a more explicit admission as to the level of scrutiny or surveillance that Google has over user-created content such as emails, photographs, and telephony data.

Replacing:

> *… many of our services require you to sign up for a Google Account. When you do we'll ask for personal information like your name, email address, telephone number or credit card to store with your account …*

With:

> *When you create a Google Account, you provide us with personal information that includes your name and a password … We also collect the content you create, upload or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs [sic] and spreadsheets you create and comments you make on YouTube videos.*

The section of the privacy policy related to the use of location services has also undergone significant elaboration from 48 words in the "December 18, 2017 policy" to 243 words in the "May 25, 2018 Policy".

Replacing:

> *When you use Google services, we may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers.*[255]

with:

> *We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you … The types of location data we collect depend in part on your device and account settings … In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse.*[256]

Google has also replaced its previous section on "how we use information we collect" with a section titled "We use data to build better services"[257] that contains (among other things) an explanation of how algorithms are used to process data.[258]

Overall, the framing of the policy appears to have shifted from an unapologetic statement of what Google does with your data[259] to a more persuasive argument as to why it is in the user's best interests to allow Google to continue doing what Google has done in the past.[260] This reflects a more user-centric privacy policy and an awareness that these policies may come under increased public scrutiny in future.

*Fitbit*

Fitbit is a popular producer of wearable fitness trackers which track the user's step-count, heart rate, location, sleep statistics and other health data. According to Statista, Fitbit has sold more than 76 million fitness trackers worldwide has at least 25 million active users.[261] The capacity of Fitbit wearable devices to track the user's location and movement is, therefore, an integral part of the services provided. Interestingly, Fitbit has adopted a different approach to Google when regarding new GDPR-based rights. In its updated privacy policy of 24 May 2018, Fitbit expanded its privacy policy to comply with the general obligations of the GDPR for all users, but limits the application of new user rights and protections (such as data portability and special categories of data as described in Article 9 of the GDPR).[262] Fitbit's policy draws a distinct line between data subjects protected by the GDPR and those who are not. Fitbit's approach seems to be one of "opt-in or miss out".

In the extracts below, notice how Fitbit invites users to agree when asked for "explicit consent" or otherwise, welcomes them to delete their accounts (although this will effectively disable many of the most valuable features of their device):

> *To the extent that the information that we collect is health data or another special category of data subject to the European Union's General Data Protection Regulation ("GDPR"), we ask for your explicit consent to process the data. We obtain this content separately when you take actions leading to our obtaining the data, for example when you pair your device to your account, grant us access to your exercise or activity data from another service, or use the female health tracking feature. You can use your account settings and tools to withdraw your consent at any time, including by stopping the use of a feature, removing our access to a third-party service, unpairing your device, or deleting your data account.*[263]

And:

> *We give you account settings and tools to access and control your personal data … regardless of where you live. If you live in the European Economic Area, United Kingdom and Switzerland ("the Designated Countries") you have a number of [additional] legal rights … You can limit how your information is visible to other users of the service … the notifications you receive … and you can revoke the access of third party applications … You can also use the Fitbit application to unpair your device from your account at any time …*
>
> *If you live in a Designated Country, in certain circumstances you can object to our processing of your information based on our legitimate interests …*
>
> *If you reside in a designated country, you can seek to restrict our processing of your data in certain circumstances. Please note that you can always delete your account at any time.*[264]

None of these paragraphs are particularly surprising given that a significant proportion of Fitbit's services rely on the collection and processing of personal data. One paragraph of the updated policy is problematic in that it requests unconditional and broad user consent to processing or data control activities which do not meet GDPR standards:

> *Please note that the countries where we operate may have privacy and data protection laws that differ from, and are potentially less protective than, the laws of your country. You agree to this risk when you create a Fitbit account and click "I agree" to data transfers, irrespective of which country you live in ...*

This paragraph seems to directly contradict the express intentions of the GDPR to ensure consistent protection for the privacy rights of EU data subjects.[265] A check of the model contract clauses mentioned in Article 46[266] and approved by the Commission, shows that EU authorities have approved no such clause (or waiver).[267]

A brief analysis of these two leading data-dependent services immediately highlights the different methods and approaches taken by companies to GDPR compliance and highlights the importance of regulatory oversight and consistent monitoring mechanisms. As mentioned previously, Maximilian Schrems has already commenced proceedings against Google citing non-compliance with the GDPR.[268] It is likely that any decision in this case will give further guidance as to how the GDPR should be implemented. Given the climate of uncertainty surrounding the GDPR and its application, and given the reforms proposed by the Australian government, the only thing that remains certain is that Australian businesses who comply with GDPR requirements now will be protected against sanctions not only in relation to the EU-related activities but to commercial activity at home as well.

## VII. Conclusion

While the intention and objectives of the GDPR build on familiar territory, new requirements such as data protection officers, data portability and a requirement for more proactive and "by-design" methods of data protection place a heavy burden on those responsible for compliance and enforcement, and legal persons wishing to continue using EU data. The challenge is compounded by a lack of certainty as to precisely *who* (outside of the EU) will fall within the GDPR. With this in mind, many legal persons are updating their privacy and data policies to incorporate GDPR-based codes of conduct or BCRs to ensure their compliance and minimise the risk of unpredictable penalties or sanctions from the DPA. Nonetheless, Australian businesses wishing to receive EU data or remain engaged with the EU market will need to comply with GDPR requirements. Impending and proposed Australian reforms are likely to bring Australian law into closer alignment with the GDPR. However, even if these reforms improve Australia's eligibility for GDPR "adequacy", any such development is likely to take a significant amount of time. In the meantime, Australian businesses will need to act now to ensure their compliance with the GDPR. As a result, the GDPR has the potential to become de facto international "law" and at the very least will form an instrumental part of future local and global data law reforms. While consumers may already be reaping the rewards of increased data protections, we have yet to see how these protections apply and whether they are appropriately monitored and enforced. Australian businesses which meet their GDPR obligations now will be well placed to avoid penalties and sanctions, while benefitting from streamlined data management processes, and are likely to save time implementing future Australian law reforms. Given that penalties for non-compliance can cost companies as much as EU€10-20 million or 2-4 percent of their annual turnover (or exclusion from the EU data pool) ignoring the GDPR is a risky move. Australian businesses who prioritise compliance early will protect themselves from such penalties or prohibitions and will be one-step ahead of the competition as GDPR-oriented reforms filter into the laws of Australia and other international jurisdictions.

1 PhD candidate Griffith Law School, Griffith University.

2 European Parliament and Council Regulation 2016/679/EC of 27 April 2016 on the 'Protection of natural persons with respect to the processing of personal data and on the free movement of such data, and repealing Directive 845/46/EC (General Data Protection Regulation)' *OJ L* 119/1.

3 Dan Jerker Svantesson, 'Article 3: Territorial Scope'in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles* (from *Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019 )1, 14.

4 Department of Foreign Affairs and Trade, "Australia – EU Free Trade Agreement: Summary of Negotiating Aims and Approach" <https://dfat.gov.au/trade/agreements/negotiations/aeufta/Documents/a-eufta-summary-of-negotiating-aims-and-approach.pdf> 1.

5 Department of Foreign Affairs and Trade, 'Australia-European Union Free Trade Agreement' <https://dfat.gov.au/trade/agreements/negotiations/aeufta/Documents/a-eufta-summary-of-negotiating-aims-and-approach.pdf>.

6 See for example Australian Government, Department of the Prime Minister and Cabinet, 'The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry' 6.

7 Productivity Commission, *Data Availability and Use,* Inquiry Report No. 82 (2017)171.

8 See for example the Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Issues Paper, 26 February 2018) <https://www.accc.gov.au/system/files/DPI%20-%20Issues%20Paper%20-%20Vers%20for%20Release%20-%2025%20F..%20%28006%29.pdf>, proposals for data portability (National Consumer Data Policy Research Centre, 'Consumer data and regulatory Reform' (ACCC Chair, Rod Sims, 16 July 2018) and the Notifiable Data Breaches provisions of the *Privacy Act 1988* (Cth) Part IIIC which came into effect on 6 November 2018 (see *Regulatory Powers (Standardisation Reform) Act* 2017, s 2).

9 Productivity Commission, *Data Availability and Use,* Inquiry Report No. 82 (2017) 191.

10 Productivity Commission, *Data Availability and Use,* Inquiry Report No. 82 (2017) 13.

11 *Privacy Act* 1988 (Cth) s.26WA.

12 Australian Government, Department of the Prime Minister and Cabinet, 'The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry' <http://dataavailability.pmc.gov.au> 6.

13 Australian Government, Department of the Prime Minister and Cabinet, 'The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry' <http://dataavailability.pmc.gov.au> 6.

14 This table has been adapted from the Office of the Information Commissioner, 'Privacy business resource 21: Australian businesses and the EU General Data protection Regulation' (June 2018) <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation> p 14. All information in the table was obtained directly from this resource unless noted otherwise.

15 Productivity Commission, *Data Availability and Use,* Inquiry Report No. 82 (2017)191.

16 Productivity Commission, *Data Availability and Use,* Inquiry Report No. 82 (2017)191.

17 Australian Government, Department of the Prime Minister and Cabinet, 'The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry' <http://dataavailability.pmc.gov.au> 6.

18 *Privacy Act* 1988 (Cth) s.26WE(2)(a).

19 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1, art 99; European Commission, 'Communication from the Commission to the European Parliament and the Council' (COM(2018) 43 Final, 24 January 2018) 1.

20 European Commission, 'Joint Statement on the final adoption of the new EU rules for personal data protection' (Statement, Brussels, 14 April 2016) retrieved from <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm>.

21 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1, 6 and 7.

22 OECD Council Recommendation, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, annex to the recommendations ('Recommendation of the Council of the 23rd September 1980: Guideline Governing the protection of privacy and transborder flows of personal Data') ("OECD Guidelines 1980").

23 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L 281/31 ("*Data Protection Directive*").

24 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1, rec.10.

25 Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47 ('TFEU').

26 *TFEU* [2012] OJ C 326/47 arts.14, 288.

27 *TFEU* [2012] OJ C 326/47 arts.14, 288.

28 European Union, "Regulations, Directives and other acts" *Europa* <https://europa.eu/european-union/eu-law/legal-acts_en>.

29 European Union, "Regulations, Directives and other acts" *Europa* <https://europa.eu/european-union/eu-law/legal-acts_en>.

30 *TFEU* [2012] OJ C 326/47 art.288.

31 *TFEU* [2012] OJ C 326/47 art.288.

32 *TFEU* [2012] OJ C 326/47 art.288.

33 OECD, *OECD Legal Instruments*, 'General Information' (2018) <https://legalinstruments.oecd.org/en/general-information>.

34 *OECD Guidelines* OECD Council Recommendation; Many of these of these principles are reflected in Australia's own *Australian Privacy Principles* which are located in Schedule one of the *Privacy Act.*

35 OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of Personal Data, (23 September 1980), 7 ("OECD Guidelines").

36 OECD Guidelines 8.

37 OECD Guidelines 9.

38 OECD Guidelines 10.

39 OECD Guidelines 11.

40 OECD Guidelines 12.

41 OECD Guidelines 13.

42 OECD Guidelines 14.

43 *Data Protection Directive* [1995] OJ L 281/31 rec.7.

44 *Data Protection Directive* [1995] OJ L 281/31 rec.8.

45 *Data Protection Directive* [1995] OJ L 281/31 rec.12, art.4(1)(b).

46 *Data Protection Directive* [1995] OJ L 281/31 arts.4(1)(a) and 4(10)(c) respectively.

47 *Data Protection Directive* [1995] OJ L 281/31 art.32.

48 European Commission, 'Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441)' 2000/520/EC [2000] OJ L 215/7.

49 European Commission, Press Release 'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield' Strassbourg, 2 February 2016 <http://europa.eu/rapid/press-release_IP-16-216_en.htm>.

50 See *Data Protection Directive* [1995] OJ L 281/31 art.5 which states "Member states shall … determine more precisely the conditions under which the processing of personal data is lawful."

51 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* ('*Directive on privacy and electronic communications*'), [2002] OJ L 201/37 rec.12, art.1.

52 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* ('*Directive on privacy and electronic communications*'), [2002] OJ L 201/37 rec. 24-25.

53 *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22EC on universal service and users' right relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws* [2009] OJ L 337/11 *("Directive 2009/136/EC").*

54 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.89.

55 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.9-10.

56 Weltimmo v Hungarian Data Protection Authority (C-230/14) [2015] EU:C:2015:639 ("Weltimmo")

57 *Weltimmo* (C-230/14) [2015] EU:C:2015:639.

58 *Weltimmo* (C-230/14) [2015] EU:C:2015:639 [9].

59 *Weltimmo* (C-230/14) [2015] EU:C:2015:639 [41].

60 "Establishment implies the effective and real exercise of any activity through stable arrangements." *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1, rec.22.

61 Dan Svantesson, 'The CJEU's Weltimmo data privacy ruling: Lost in the data privacy turmoil, yet so very important case C-230/14 Weltimmo, EU:C:2015:639' (2016) 2 *Maastricht Journal of European and Comparative Law*, 332, 337.

62 Mark Williamson and Helen Bourne 'European Union: Schrems and Weltimmo: The Shifting Sands of EU Data Protection Law' *Mondaq* (online) 28 October 2015.

63 Schrems v Data Protection Commissioner (C-362/14) [2015] EU:C:2015:650 [28] ("Schrems").

64 Hannah Kuchler, 'Max Schrems: the man who took on Facebook – and won' *The Irish Times* (online) 5 April 2018 retrieved from <https://www.irishtimes.com/business/technology/max-schrems-the-man-who-took-on-facebook-and-won-1.3451485>.

65 Hannah Kuchler, "Max Schrems: the man who took on Facebook – and won" *The Irish Times* (online) 5 April 2018 retrieved from <https://www.irishtimes.com/business/technology/max-schrems-the-man-who-took-on-facebook-and-won-1.3451485>.

66 *Schrems* (C-362/14) [2015] EU:C:2015:650 [29].

67 Charter of the Fundamental Rights of the European Union (2012/C 326/02) [2012] OJ C 326, 391 art.47.

68 *Schrems* (C-362/14) [2015] EU:C:2015:650 [91].

69 *Maximilian Schrems v Data Protection Commission and Digital Rights Ireland* (C-362/14) [2015] EU:C:2015:650.

70 Rob Price, 'After a Landmark court ruling, an activist is trying to force Facebook to put an end to a key data transfer' *Business Insider Australia* (online) 4 December 2015 <https://www.businessinsider.com.au/facebook-europe-max-schrems-legal-complaints-ireland-belgium-hamburg-safe-harbor-ecj-2015-12>.

71 Tobias Lutzi, 'What is a "consumer?" (Some) clarification on consumer jurisdiction, social media accounts and collective redress under the Brussels Ia Regulation' (2018) 25(3) *Maastricht Journal of European and Comparative Law* 374, 374.

72 *The Data Protection Commissioner v Facebook Ireland Limited & Maximilian Schrems* [2017] IEHC 545.

73 Tobias Lutzi, 'What is a "consumer?" (Some) clarification on consumer jurisdiction, social media accounts and collective redress under the Brussels Ia Regulation' (2018) 25(3) *Maastricht Journal of European and Comparative Law* 374, 374.

74 *Maximilian Schrems v Facebook Ireland Limited* (C-496/16) [2018] EU:C:2018:37.

75 See Tobias Lutzi, 'What is a 'consumer?' (Some) clarification on consumer jurisdiction, social media accounts and collective redress under the Brussels Ia Regulation' (2018) 25(3) *Maastricht Journal of European and Comparative Law* 374, for more details.

76 See, for example, Lucy Fielder, Douglas Busvine 'Austrian data privacy activist takes aim at 'forced consent' *Reuters* (online) 25 May 2018 retrieved from <https://www.reuters.com/article/us-europe-privacy-lawyer/austrian-data-privacy-activist-takes-aim-at-forced-consent-idUSKCN1IQ0ZI>; *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.7.4.

77 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.1.

78 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.2.

79 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.3.

80 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 arts.5-11.

81 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.8.

82 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.12.

83 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 Chapter 2 Section 2 arts.13-15.

84 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 arts.19, 17, 20-21 (respectively).

85 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.22.

86 Sahar Bhaimia, 'The General Data Protection Regulation: The Next Generation of EU Data Protection' (2018) 18 *Legal Information Management* 21, 26.

87 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.37.

88 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.40.

89 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.42.

90 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.45.

91 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.51.

92 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 arts.60-76.

93 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.88.

94 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.85.

95 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.94-95.

96 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.96.

97 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.99.

98 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.98.

99 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.97.1.

100 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.97.2.

101 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.97.4.

102 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.97.3.

103 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.97.5.

104 European Union, 'Living in the EU', <https://europa.eu/european-union/about-eu/figures/living_en>.

105 *Data Protection Directive* [1995] OJ L 281/31 art.4.

106 *Data Protection Directive* [1995] OJ L 281/31 art.4.

107 Trischa Mann (ed) *Australian Law Dictionary* (Oxford University Press, 2013, 2nd ed), 239.

108 European Union, 'Regulations, Directives and other act', *Europa* <https://europa.eu/european-union/eu-law/legal-acts_en>.

109 *Weltimmo* (C-230/14) [2015] EU:C:2015:639.

110 Mark Williamson and Helen Bourne 'European Union: Schrems and Weltimmo: The Shifting Sands of EU Data Protection Law', *Mondaq* (online) 28 October 2015.

111 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.3.

112 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 Chapter 6.

113 Extracted above, *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.3.

114 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.129.

115 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.18.

116 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.3.

117 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.3.1.

118 Dan Jerker Svantesson, 'Article 3: Territorial Scope' in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019) 1, 8.

119 *Microsoft Corporation, Appellant v United States of America* [2016] 829 F.3d 197.

120 Robert J. Currie, 'Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the *Microsoft Ireland* Case the "Next Frontier"?' 2016 *The Canadian Yearbook of International Law* 63, 65.

121 Robert J. Currie, 'Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the *Microsoft Ireland* Case the "Next Frontier"?' 2016 *The Canadian Yearbook of International Law* 63, 65.

122 *United States of America v Microsoft Corporation,* No. 17-2, 584 U.S. (2018) retrieved from <https://www.supremecourt.gov/DocketPDF/17/17-2/41851/20180330172237829_17-2motUnitedStates.pdf>.

123 *Consolidated Appropriations Act* 2018, H.R. 1625, Div. V 115th Cong., 2d Sess. (2018).

124 *Microsoft Corporation, Appellant v United States of America [2016] 829 F.3d 197 ('Microsoft Warrant Case').*

125 European Commission, 'Brief of the European Commission on Behalf of the European Union as *amicus curiae* in support of neither party', Submission in *United States of America v Microsoft Corporation* 17-2, 7.

126 *Data Protection Directive* [1995] OJ L 281/31 art.4.

127 *Weltimmo* (C-230/14) [2015] EU:C:2015:639 [41].

128 Mark Williamson and Helen Bourne, 'European Union: Schrems and Weltimmo: The Shifting Sands of EU Data Protection Law' *Mondaq* (online) 28 October 20152.

129 *Verein für Konsumentinformation v. Amazon EU Sàrl (C-191/15) [2016] ECLI 612 ('Verein für Konsumentinformation').*

130 Dan Jerker Svantesson, 'Article 3: Territorial Scope' in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019) 1, 6; *Verein für Konsumentinformation (C-191/15) [2016] ECLI 612 [82].*

131 Dan Jerker Svantesson, "Article 3: Territorial Scope" in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019) 1, 6; *Verein für Konsumentinformation (C-191/15) [2016] ECLI 612 [82].*

132 Dan Jerker Svantesson, 'Article 3: Territorial Scope' in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019) 1, 6; *Verein für Konsumentinformation (C-191/15) [2016] ECLI 612 [82].*

133 *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles (C.-131/12) [2014] ECLI 317 ("Google Spain").*

134 Microsoft Warrant Case [2016] 829 F.3d 197.

135 *Google Spain (C.-131/12) [2014] ECLI 317.*

136 See Dan Jerker Svantesson, 'Article 3: Territorial Scope' in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019) 1, 6; *Google (C.-131/12) [2014] ECLI 317 [55]-[56].*

137 *Joined Cases Pammer v Reerderei Karl Schlüter GmbH & KG (C-585/08) and Hotel Alpenhof GesmbH v. Oliver Heller (C144/09) [2010] ECLI 740.*

138 *Joined Cases Pammer v Reerderei Karl Schlüter GmbH & KG (C-585/08) and Hotel Alpenhof GesmbH v. Oliver Heller (C144/09) [2010] ECLI 740. [Ruling 2].*

139 *Joined Cases Pammer v Reerderei Karl Schlüter GmbH & KG (C-585/08) and Hotel Alpenhof GesmbH v. Oliver Heller (C144/09) [2010] ECLI 740 [84].*

140 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.3.2.

141 Mark Williamson and Helen Bourne 'European Union: Schrems and Weltimmo: The Shifting Sands of EU Data Protection Law' *Mondaq* (online) 28 October 2015.

142 See European Commission, 'European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows' (Press Release, Document number IP/16/2461, 12 July 2016) <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en>.

143 Craig McAllister, 'What about Small Businesses: The GDPR and its Consequences for Small, U.S.-Based Companies,' (2017) 12 *Brooklyn Journal of Corporate and Financial Law* 187, 199.

144 European Commission, Factsheet: EU-US Privacy Shield Factsheet" (July 2016) retrieved from <http://collections.internetmemory.org/haeu/20171122154227/http:/ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf>.

145 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.45.1.

146 <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>.

147 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.46.

148 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.47.

149 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.46.

150 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.46.2

151 Explanatory Memorandum, Telecommunications and Other Legislation (Assistance and Access) Bill 2018 [6]-[8].

152 These documents can be retrieved from <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en>.

153 Article 29 Data Protection Working Party, 'Working Document Setting up a framework for the Structure of Binding Corporate Rules (adopted 24 June 2008) retrieved from <http://collections.internetmemory.org/haeu/20180322140344/http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf>.

154 Article 29 Data Protection Working Party, 'Working Document setting up a table with the documents and principles to be found in Binding Corporate Rules' available at: <http://collections.internetmemory.org/haeu/20180322140344/http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf>.

155 See for example 'EU Cloud COC' available at: <https://eucoc.cloud/en/home.html> and "Cloud security alliance Code of Conduct' available at: <https://gdpr.cloudsecurityalliance.org/resource/csa-code-of-conduct-for-gdpr-compliance/> for cloud service providers.

156 See for example, 'Request the EU Cloud COC' available at: <https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html>.

157 See for example JP Morgan, 'First Data, and HP' available at: <https://iapp.org/resources/article/approved-binding-corporate-rules/>; 'Mastercard' available at: <https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf> and 'GlaxoSmithKline' available at: <https://www.gsk.com/en-gb/about-us/policies-codes-and-standards/binding-corporate-rules/>.

158 *Directive on privacy and electronic communications* [2002] OJ L 201/37 and *Directive 2009/136/EC* [2009] OJ L 337/11.

159 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.79.

160 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.83.

161 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.4(2); Elle Pyle at al, 'Decoding GDPR' (2018) 102 (1) *Judicature* 58, 62.

162 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.7.1.

163 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.7.2

164 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.34.

165 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.15

166 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.17.1-2

167 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.17.3.

168 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.20.

169 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.25.

170 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.25.1.

171 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.37-39.

172 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.40.

173 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.15.

174 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.10.

175 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.13.

176 Christoph Kuner, "Extraterritoriality and regulation of international data transfers in EU data protection law" (2015) 5(4) *International Data Privacy Law* 235, 235.

177 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.129.

178 IDC and Open Evidence "European Data Market SMART2013/0063, Executive Summary" (European Commission Report: Directorate-General for Communications Networks, Content and Technology) 1 February 2017, 10.

179 See European Commission, Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation") (Brussels, 25.1.2012, Document 2012/0011 (COD)).

180 European Parliament, *Protection of individuals with regard to the processing of personal data* European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation") (Ordinary legislative procedure: First reading) [2017] 12 March 2014 OJ C 378/399.

181 European Union, 'European Economic Social Committee' <https://europa.eu/european-union/about-eu/institutions-bodies/european-economic-social-committee_en>.

182 Committee of Regions *Opinion of the Committee of the Regions on "Data Protection Package"*(2012/C 391/13) on 18.12.2012 [2012] OJ C 391/127.

183 Agency for Fundamental Rights, *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*, (FRA Opinion – 2/2012, Vienna 1 October 2012).

184 European Data Protection Supervisor, Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package [2012] OJ C 192/7.

185 See, for example, the draft version of Article 5 supplied by Parliament on 12 March 2014 at OJ C 378/426-7 c.f. the original version proposed by the Commission on 25 January 2012 at 2012/0011 (COD), 43, or the final version Regulation (EU) 2016/677 OJ L 119/35-6.

186 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.21.

187 Economic and Social Committee, *Opinion of the European Economic and Social Committee on "The digital market as a driver for growth* (exploratory opinion) OJ C 229/1 at 4.23.

188 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.17.

189 Agency for Fundamental Rights, *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*, ("FRA Opinion – 2/2012, Vienna 1 October 2012") p 18.

190 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.65, art.17.

191 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.58.1.

192 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.58.2(a).

193 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.58.2(b).

194 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.58.2(j).

195 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.58.2(f).

196 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.58.2(i).

197 Council of the European Union, Press release 3279th Council Meeting, Justice and Home Affairs, 5-6th December 2013, Brussels, 17342/13) 12.

198 Council of the European Union, Press release 3279th Council Meeting, Justice and Home Affairs, 5-6th December 2013, Brussels, 17342/13) 12.

199 Council of the European Union, Press release 3279th Council Meeting, Justice and Home Affairs, 5-6th December 2013, Brussels, 17342/13) 12.

200 Dan Jerker Svantesson, 'Article 3: Territorial Scope' in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019) 1, 14.

201 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.13.

202 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.20.

203 Dr Orla Lynskey, 'Article 20: The Right to Data Portability' in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019) 68, 72-3.

204 See European Parliament, *Protection of individuals with regard to the processing of personal data* I: European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data ("*General Data Protection Regulation*") (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD) OJ C 378/399, 438.

205 See European Commission, *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such da*ta ("*General Data Protection Regulation*") (Brussels, 25.1.2012, Document 2012/0011 (COD)) art 18 c.f. *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.20.

206 European Data Protection Supervisor, Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package [2012] OJ C 192/7, 10.

207 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.20.

208 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.13.

209 Dr Orla Lynskey, 'Article 20: The Right to Data Portability' in Christopher Kuner, Professor Lee Bygrave, Christopher Docksey (eds) *Draft Commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation)* (Oxford University Press, 2019) 68, 78.

210 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.20, 33 respectively.

211 Australian Government, Department of the Prime Minister and Cabinet , 'The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry' <http://dataavailability.pmc.gov.au> 6.

212 European Commission, *Regulation of the European Parliament and of the Council on the protection* of individuals with regard to the processing of personal data and on the free movement of such data ("*General Data Protection Regulation*") (Brussels, 25.1.2012, Document 2012/0011 (COD)) art 35.

213 European Parliament, *Protection of individuals with regard to the processing of personal data* European parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("*General Data Protection Regulation*)" (Ordinary legislative procedure: First reading) [2017] 12 March 2014 OJ C 378/399 art 35.1 (b).

214 European Data Protection Supervisor, Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package [2012] OJ C 192/7, 11.

215 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.37.1(b).

216 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.13; See European Commission, Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC) [2003] OJ L 124/36 Annex, art 2.

217 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.18.

218 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.18.

219 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.3.

220 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.80.

221 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.80.

222 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.37-39.

223 A complete list of adequacy decision recipients can be found at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu>.

224 European Data Protection Board, *Press Release: Third Plenary Session: EU-Japan draft adequacy decisio*n, *DPIA lists, territorial scope and e-evidence* (26 September 2018), retrieved from <https://edpb.europa.eu/news/news/2018/press-release-third-plenary-session-eu-japan-draft-adequacy-decision-dpia-lists_en>.

225 Anna Johnston, 'Preparing your clients for the GDPR Privacy reforms' (2018) 44 *Law Society Journal of NSW* 74, 75-76.

226 Department of the Prime Minister and Cabinet, *Data Availability and Use: The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry* (2018), 6

227 Productivity Commission, *Data Availability and Use,* Productivity Commission Inquiry Report No. 82, (2017) 35.

228 Office of the Australian Information Commissioner, *Australian businesses and the EU General Data Protection Regulation* (June 2018), 14 retrieved from <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>.

229 Productivity Commission, *Data Availability and Use,* Productivity Commission Inquiry Report: Overview and Recommendations No. 82, (2017) 14.

230 Productivity Commission, *Data Availability and Use,* Productivity Commission Inquiry Report: Overview and Recommendations No. 82, (2017) 14.

231 Productivity Commission, *Data Availability and Use,* Productivity Commission Inquiry Report: Overview and Recommendations No. 82, (2017) 18.

232 National Consumer Data Policy Research Centre, *Consumer data and regulatory Reform* (ACCC Chair, Rod Sims, 16 July 2018).

233 Productivity Commission, *Data Availability and Use,* Productivity Commission Inquiry Report: Overview and Recommendations No. 82, (2017) 14

234 Office of the Australian Information Commissioner, *Australian businesses and the EU General Data Protection Regulation* (June 2018) retrieved from <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>.

235 John Bowman and Miriam Gufflet, "Meeting the Challenge of a Global GDPR and BCR Programme" (2017) 2 *European Data Protection Law Review* 257, 257-8.

236 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec. 108

237 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.46(2)(b).

238 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.46(2)(d), art.93(2).

239 Christopher Kuner 'Article 46: Transfers subject to appropriate safeguards' in Christopher Kuner, Prof. Lee Bygrave and Christopher Docksey *Draft Commentaries on 10 GDPR articles* (from *Commentary on the EU General Data Protection Regulatio*n, OUP 2019) retrieved from <http://works.bepress.com/Christopher-kuner/1/> 108, 116.

240 Christopher Kuner 'Article 46: Transfers subject to appropriate safeguards' in Christopher Kuner, Prof. Lee Bygrave and Christopher Docksey *Draft Commentaries on 10 GDPR articles* (from *Commentary on the EU General Data Protection Regulation*, OUP 2019) retrieved from <http://works.bepress.com/Christopher-kuner/1/> 108, 116; *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.46(2)(e), art.40.

241 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.46(2)(f), 42.

242 The precise requirements for the compliance application process is beyond the scope of this article. For more details see Office of the Australian Information Commissioner, *Australian businesses and the EU General Data Protection Regulation* (June 2018), 14 retrieved from <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>.

243 *Privacy Act 1988* (Cth) ss.6C-6D.

244 See part V of this article.

245 Department of Foreign Affairs and Trade, 'Australia – EU Free Trade Agreement: Summary of Negotiating Aims and Approach'. Available at: <https://dfat.gov.au/trade/agreements/negotiations/aeufta/Documents/a-eufta-summary-of-negotiating-aims-and-approach.pdf> 3.

246 Craig McAllister, 'What about Small Businesses: The GDPR and its Consequences for Small, U.S.-Based Companies' (2017) 12 *Brooklyn Journal of Corporate and Financial Law* 187, 204.

247 Craig McAllister, 'What about Small Businesses: The GDPR and its Consequences for Small, U.S.-Based Companies'(2017) 12 *Brooklyn Journal of Corporate and Financial Law* 187, 206.

248 More details regarding compliance requirements under the EU-US privacy shield fall outside of the scope of this article but can be found here <https://www.privacyshield.gov/US-Businesses>.

249 Ben Popper, 'Google announces over 2 billion monthly active devices on Android' *The Verge* (online) 17 May 2017 available at <https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users>.

250 *GDPR* (EU) 2016/679 [2016] OJ L 119/1 art.20; Google, 'Privacy Policy Comparison document',*Google* (25 May 2018) <https://policies.google.com/privacy/archive/20171218-20180525?hl=en&gl=ZZ> 20.

251 Google, 'Privacy Policy Comparison document' *Google* (25 May 2018) <https://policies.google.com/privacy/archive/20171218-20180525?hl=en&gl=ZZ> 19 ("Google Privacy Policy Comparison").

252 *GDPR* (EU) 2016/679 [2016] OJ L 119/1 art.4.

253 Google Privacy Policy Comparison, 19.

254 See for example Scott R Peppet, 'Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, And Consent'(2014) 93(1) *Texas Law Review* 85.

255 Google Privacy Policy Comparison,.

256 Google Privacy Policy Comparison, 6-7.

257 Google Privacy Policy Comparison, 7.

258 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.22; Google Privacy Policy Comparison pp 7-8, 10.

259 See, for example, the section on "Location" in previous version of Google Privacy Policy, Google Privacy Policy Comparison, 3,

260 As compared with 'Your location information' in updated version of Google Privacy Policy, Google Privacy Policy Comparison, 5.

261 Statista, 'Fitbit – Statistics & Facts' (online) <https://www.statista.com/topics/2595/fitbit/>.

262 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.20, 9; Fitbit Inc., 'Privacy Policy' (24 May 2018) <https://www.fitbit.com/au/legal/privacy-policy> 6 ("Fitbit Privacy Policy").

263 Fitbit Privacy Policy 3.

264 Fitbit Privacy Policy 6.

265 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 rec.10.

266 *General Data Protection Regulation* (EU) 2016/679 [2016] OJ L 119/1 art.46

267 See 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271).

268 See part III of this article.