University of New South Wales Law Research Series

‘GDPR CREEP’ FOR AUSTRALIAN BUSINESSES BUT GAP IN LAWS WIDENS

GRAHAM GREENLEAF

(2018) 154 *Privacy Laws & Business International Report* 1, 4-5
[2018] *UNSWLRS* 54

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

‘GDPR creep’ for Australian businesses but gap in laws widens

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2018) 154 *Privacy Laws & Business International Report* 1, 4-5 (June 2018)

Australia’s privacy protections are not regarded as ‘adequate’ by the European Union, under the 1995 Directive, despite occasional misapprehensions that they are.[1] There has been some strengthening of Australia’s *Privacy Act 1988* in the decade since the EU last examined the question of the adequacy of Australian law.[2] In relation to the private sector, the most significant points on which it was then found wanting were the exemptions from the Act for ‘small’ businesses, and for employment records – gaps which have not since been plugged.

However, as the EU’s General Data Protection Regulation (GDPR) entered into force on 25 May 2018, the distance between Australian and EU data privacy protections may be greater than it was under the Directive. This article considers the ‘gaps’ remaining between the GDPR and Australian law, and whether they are likely to be significant for the question of adequacy, if and when it arises again.

The pre-GDPR character of Australian law does not, however, mean that Australian businesses are unaffected by the GDPR. As is now notorious, the extra-territorial reach of the GDPR will have serious implications for some Australian businesses, outlined below. These effects are likely to be overshadowed by another, potentially more pervasive, side-effect of the GDPR, which I call ‘GDPR-creep’.[3]

GDPR-creep affecting Australian businesses

Anna Johnston, Director of Salinger Privacy concludes from enquiries from current and prospective clients[4] that ‘Australian businesses serving the B2B market, which don’t themselves have customers in the EU, are being pressured by their own clients (i.e. other businesses, even in other non-EU countries like the US) to ensure that their products such as software will be “GDPR-complaint”’. She thinks that ‘the most immediate impacts will be around tightening up what it means to obtain a valid consent; being more rigorous in having an expert and independent Data Protection Officer [DPO]; much more emphasis on the use of PIAs [Data Protection Impact Assessments (DPIAs)]; and maybe eventually some progress on the more novel “data subject rights” in the GDPR on topics like algorithmic transparency’.[5]

---

[1] Australia’s Passenger Name Record (PNR) arrangements are regarded as adequate. The EU has signed bilateral passenger name record (PNR) agreements with the United States, Canada and Australia. ‘The transfer of PNR data from the EU to third

[2] The European Commission examined the adequacy of Australia’s laws in 2005 (with an update in 2006). An Expert Report was prepared, and discussed with Australian agencies, but the Commission did not proceed further to request an Opinion of the Article 29 Working Party. This is mentioned in G. Greenleaf ‘Privacy in Australia’, Chapter in Rule J and Greenleaf G (Eds) *Global Privacy Protection: The First Generation* (Edward Elgar, Cheltenham, 2008). <https://ssrn.com/abstract=3072270>

[3] ‘GDPR-creep’ is derived from ‘*function creep* (in British. noun.) the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy’ (Collins English Dictionary). The use is ironic, because the creep here is in the direction of greater privacy protection.

[4] Salinger Privacy < www.salingerprivacy.com.au>; the comments following are from correspondence between Anna Johnston and the author.

[5] A. Johnston (above).

Peter Leonard of Data Synergies makes much the same point when he says that, where operations of a transnational business group have 'upstream' obligations imposed on them (such as in the EU) then 'it is necessary to repeat those more prescriptive requirements in downstream arrangements' (such as in Australia) 'in order to discharge with the upstream operations'.[6] He concludes that 'it appears likely that the requirements of the EU's GDPR will become the default international standard'. Leonard considers that this will be irrespective of what is the best policy approach, unless there are major changes to the international approach to interoperability of standards.

What Johnston calls a 'ripple effect', and Leonard regards as a 'downstream' migration, I describe as 'GDPR-creep'. Johnston points out that Australians generally might indirectly be the beneficiaries of an overall lifting of privacy standards: 'If nothing else, GDPR is forcing companies, even small companies here in Australia which have in the past not minded too much about compliance with Australian law (or are exempt because they meet the 'small business' exemption), to sit up and take notice about the responsibilities.' However, GDPR-creep does not bring with it GDPR-strength remedies, or any remedies at all because (by definition) these are situations that existing Australian privacy laws do not reach.

Australia's Information Commissioner advocates that businesses consider GDPR-creep: 'Where additional measures are implemented and these are not inconsistent with the *Privacy Act*, Australian businesses could consider rolling these out across their Australian operations—this could improve consumer trust through enhanced privacy practices and allow for more consistent internal privacy practices, procedures and systems across the business'.[7]

Extra-territorial effects of the GDPR in Australia

The direct effect of the GDPR on some Australian businesses derives principally from its extra-territorial application, which has three forms. First, if an Australian business which is a data controller or processor has an 'establishment' in the EU, for example by having an office in the EU, it will be required to comply with the GDPR, even though it processes data outside the EU (including via a processor located outside the EU) (GDPR art. 3(1), rec. 22).

Second, if a business located in Australia (but without an EU establishment) offers goods or services (whether or not for payment) to people in the EU, the GDPR applies to the business. Mere accessibility of an Australian business' website in the EU, or use of European languages in use in Australia, will be insufficient, but other factors (e.g. use of EU currencies, or ordering facilities envisaging EU buyers) may point to EU-directed offers (GDPR art. 3(2)(a), rec. 23).

Third, the GDPR applies if the behaviour in the EU, of EU data subjects, is monitored (such as by Internet tracking in order to analyse or predict personal preferences, behaviours and attitudes) by an Australian business (GDPR art. 3(2)(b), rec. 24).

The result of such application is that any Australian businesses within these three forms of scope must comply with the GDPR in its entirety, including many obligations going beyond the requirements of Australia's Privacy Act (see the following section). This also applies to businesses or functions of organisations (such as political parties and employers) otherwise exempt from the *Privacy Act*. Sources of advice are available to Australian companies which

---

[6] P. Leonard 'Report on the Regulation of Cross-Border Data Transfers in Australia' (ABLI, February 2018), para. 12.

[7] OAIC *Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation* <https://www.oaic.gov.au/resources/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation.pdf.>

may be affected directly by these GDPR extra-territorial effects, and who therefore need to consider compliance steps.[8]

Gaps between the GDPR and Australian law

Australia's Information Commissioner (OAIC) provides a useful comparison between the *Privacy Act* and the GDPR,[9] but my assessment is that the breadth of the gaps between the two is wider than the OAIC states.

Some differences from EU law have been reduced by reforms to Australia's Privacy Act over the past decade, including:

- Data breach notifications to both the Information Commission and to data subjects are required since reforms which came into effect in February 2018 (*Privacy Act 1988*, Part IIIC)[10]. The criteria for notification are slightly different from those in the EU (GDPR arts. 33, 34, recs. 85-88).
- The Information Commissioner can refer to the Federal Court the imposition of administrative fines ('civil penalty orders') for some serious and/or repeated categories of breaches, up to AUD 2.1M (about 1.34M euros). While this is a relatively high maximum level for administrative fines by global standards, it is low compared with the GDPR's administrative fines of the greater of 20M euros and 4% of global turnover (GDPR, art. 83).
- Australian law has always had greater extra-territorial reach than most countries' data privacy laws (*Privacy Act 1988*, s5B), but with more limited reach than the EU provisions discussed above.
- While falling short of the obligation to demonstrate compliance (GDPR art. 5(2)), Australian businesses are required to take reasonable steps to implement practices to ensure compliance with the Australian Privacy Principles (*Privacy Act*, APP 1.2). This is argued by the OAIC to be implementation of 'data protection by design' (GDPR art. 25(1)).

However, there are many aspects of the GDPR (some inherited from the 1995 EU Directive) where Australian law differs substantially or has no equivalents, including:

- Required Data Protection Officers (DPOs) (GDPR arts. 37-39);
- Mandatory Data Protection Impact Assessments (DPIAs) (GDPR arts. 35, 36), a much stronger requirement that the vague requirements of APP 1.2 to which the OAIC refers;
- Stronger consent requirements, including by clear affirmative actions or statements, and unbundled consent (GDPR arts. 7, 8), elements difficult to find in Australia's provision that consent may be express or implied;
- Extended sensitive data categories (biometric and genetic data) (GDPR art. 9);
- Limits on automated decision-making (GDPR art. 22);

---

[8] For example, A. Johnston 'Preparing your client for the GDPR privacy reforms', (2018(44) Law Society Journal (NSW) 74-76 <https://lawsociety.cld.bz/LSJ-May-2018/74/>; P. Leonard 'GDPR: A guide for Australian businesses' Data Synergies, April 2018 (contact Peter Leonard <pleonard@datasynergies.com.au>); D. Short and H. McDwyer 'How the EU General Data Protection Regulation (GDPR) will impact Australian business?' *Addisons website*, 28 April 2018 <http://www.addisonslawyers.com.au/knowledge/How_the_EU_General_Data_Protection_Regulation__GDPR__will_impact_Australian_business1052.aspx>.

[9] OAIC *Privacy business resource 21* (above).

[10] E. Coombs and S McLaughlan 'Australia's mandatory breach notification regime imminent' (2018) 150 *Privacy Laws & Business International Report*, 1, 3-5.

- Data protection by default (GDPR art. 25(2)), which is a separate requirement to 'data protection by design'.
- Right to data portability (GDPR art. 20);
- Right to deletion of data/ links ('right to be forgotten' if justifiable) (GDPR art. 17);
- Right to object to processing based on public interest or controller's legitimate interests (GDPR art. 21(1));
- Rights to restrict processing, including delaying it (GDPR art. 18), which can at best be implied in some types of disputes under the *Privacy Act*.

In relation to permissible personal data exports, the GDPR retains at its core the concept of 'adequacy' of protection provided in the jurisdiction of the recipient (GDPR arts. 44-49), as interpreted by the Court of Justice of the European Union (CJEU) in *Schrems* to mean 'essemtially equivalent' protection. Australia's APP 8 imposes significantly different tests which at some points are weaker than the GDPR approach because they are based on reasonable beliefs about overseas laws or schemes.[11]

Australian law also has exceptions and exemptions where there are no GDPR equivalents (including publicly available information; 'small' businesses; employment uses; and political parties). Australian governments have not followed Australian Law Reform Commission recommendation in 2008 to reduce or eliminate such exemptions.[12]

It is therefore clear that, if an Australian company either considers that is necessary for it to voluntarily 'comply' with the GDPR ('GDPR creep') or if it is legally required to comply because of the GDPR's extra-territorial impacts, such compliance will require the adoption of a very substantial set of practices that go beyond what is required by the *Privacy Act 1988*.

Adequacy implications (if and when relevant)

The 'adequacy gap' between the GDPR and the current Australian *Privacy Act* is therefore, on balance, wider now than they were a decade ago (compared then to the 1995 EU Directive). While 'adequacy' still does not require laws of identical strength, the *Schrems* test of essential equivalence may be higher than was applied a decade ago. With the GDPR only now coming into force, it is too early to be sure which of the GDPR elements listed above will be regarded as necessary or even important elements of adequacy, at least until some determinations of adequacy are made under the GDPR – and also perhaps until the CJEU has its say about them. However, it is clear enough that Australia will continue to find it very difficult to achieve a positive finding of adequacy, if and when the question arises again.

[11] N. Waters and G. Greenleaf 'Australia's 2012 Privacy Act Revisions: Weaker Principles, More Powers' (2013) 121 *Privacy Laws & Business International Report,* 12-13 <https://ssrn.com/abstract=2252569 >.

[12] ALRC *For Your Information: Australian Privacy Law and Practice* [2008] ALRC 108 <http://www.austlii.edu.au/au/other/lawreform/ALRC/2008/108.html>