‘European’ data privacy standards implemented in laws outside Europe

GRAHAM GREENLEAF

(2017) 149 *Privacy Laws & Business International Report*, 21
[2018] *UNSWLRS* 2

UNSW Law
UNSW Sydney NSW 2052 Australia

'European' data privacy standards implemented in laws outside Europe

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia
(2017) 149 *Privacy Laws & Business International Report* 21-23

The implementation of 'European' data privacy principles in laws outside Europe continues to be substantial, including in high-GDP countries. This article is based on ongoing work on the extent to which '2nd generation' data privacy standards, which I also call 'European standards' are found in data privacy laws in countries outside Europe.

The term 'European standards' means standards required of European countries by the EU data protection Directive (1995) and by Council of Europe (CoE) data protection Convention 108 (1981) as modified by its Additional Protocol (2001), but which are *not* standards required by the '1st generation' standards of the OECD Guidelines (1980) and original CoE Convention 108 (1981). Put briefly, 'European' or '2nd generation' standards are the difference between what was required by the EU Directive as compared with the OECD. To be manageable, this has been limited to the ten most important differences, as set out in the attached Table.

In 2012 I assessed[1] 33 of the 39 data privacy laws that then existed outside Europe (as at December 2011) to determine the extent to which they included these ten 2nd Generation' 'European standards'. That analysis showed that they had been substantially incorporated into these 33 non-European laws. On average these laws included 7 out of the 10 'European principles'. Some occurred in more than 75% of the laws assessed: 'destination-based' data export restrictions (28/33); additional protection for sensitive data (28/33); deletion requirements (28/33); minimum collection (26/33); and two enforcement-related principles (an independent DPA (25/33) and recourse to the courts (26/33)).

Five years later, by February 2017, the number of non-European laws had increased from 39 to 66.[2] Assessment of all 66 countries with data privacy laws, while having the virtue of thoroughness, also has the disadvantage that it treats all countries as of equal weight (as done in the 2012 study). So the data privacy law in Burkina Faso is given the same significance as that in South Africa, and that of a small Caribbean island is given the same weight as that in Argentina. All 66 data privacy laws is also too large a number of laws to be a practical basis for an initial assessment – that task must come later.

Limiting comparison to the 'most significant' countries

For both reasons an objective selection of a particular sub-set of laws outside Europe is needed. An alternative pragmatic approach is to assess the laws of countries with the largest Gross Domestic Product (GDP) (nominal)[3] as a measure of their economic significance. The 20 highest-ranked countries outside Europe that do have data privacy laws covering at least most of their private sectors occur in the first 53 countries ranked by GDP.[4] They are, in order of GDP: Japan; India;

[1] For the basis of this analysis, see Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2(2) *International Data Privacy Law*, pp. 68–92 <http://papers.ssrn.com/abstract_id=1960299>..

[2] Greenleaf 'Global data privacy laws 2017: 120 national data privacy laws now include Indonesia and Turkey' 145 Privacy Laws & Business International Report (PLBIR) 10-13.

[3] Wikipedia: 'List of countries by GDP (nominal)' <https://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal)>: 'Gross domestic product (GDP) is the market value of all final goods and services from a nation in a given year.' Nominal GDP does not take in to account differences in the cost of living in different countries, whereas GDP by purchasing power parity (PPP) does so.

[4] As at 26 February 2017 in Wikipedia: 'List of countries by GDP (nominal)'; The IMF ranking is used instead of the World Bank ranking or the UN ranking beause it includes Hong Kong and Taiwan, but otherwise there is little difference among the three.

Canada; South Korea; Australia; Mexico; Indonesia; Argentina; Taiwan; Hong Kong; Israel; the Philippines; Malaysia; Singapore; South Africa; Colombia; Chile; Vietnam; Peru; and New Zealand. Their 20 laws are 30% of the 66 laws found at present in countries outside Europe.

This 'Top 20 by GDP' list includes all 8 OECD members outside Europe (except the USA), and 17/20 are also APEC economies, so this approach is also revealing of the position in OECD and APEC members. Another measure of global significance is membership of the G20. The Group of Twenty (G20), which has held largely annual meetings since 2008, has largely replaced the G7/G8 grouping as the principal meeting of world's most significant countries, although there is no clear objective basis for its membership.[5] It is comprised of the European Union plus 19 countries: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, South Korea, Turkey, the United Kingdom and the United States of America. Of the 13 non-European countries in the G20, the nine that do have data privacy laws are all included in the 'Top 20 by GDP' non-European countries with privacy laws. So there is significant consistency between the G20 and GDP lists. It seems therefore that GDP correlates well with other measures of significance.

First Generation data privacy laws and countries by GDP

Only eight non-European countries in the list of top 53 countries by GDP do not have data privacy laws (ie laws meeting the '1st generation'/OECD standards) covering most of their private sector. In order of GDP they are: United States; China; Brazil; Saudi Arabia; Nigeria; Venezuela; Pakistan; and Bangladesh. Since all European countries do have data privacy laws, only 8 of the top 53 countries by GDP do not have these minimum standard data privacy laws. Of these, China's laws come close to minimum international standards, Brazil is in the process of legislating, and the USA has laws of limited scope. Of the 13 non-European countries in the G20, only four countries (Brazil, Saudi Arabia, China and the United States) do not have data privacy laws meeting this minimum international standard.

By either of these measures, by far the majority (75% G20; 90% by GDP) of 'significant' countries in economic and political terms (including European countries) do have data privacy laws meeting these minimal '1st generation' international standards.

Second Generation privacy standards and 'Top 20 by GDP' countries

The next question to be assessed is the extent to which the ten 'European standards' which comprise the '2nd generation' of data privacy standards have been implemented by 2017 in the laws of the top twenty non-European countries by GDP with privacy laws.

In the Table the principles are sorted by their frequency of occurrence in these 'top 20 by GDP' laws outside Europe, from most often to least often occurring. The data privacy laws of the twenty countries include on average 5.95 (ie 6) of the 10 2nd generation 'European' standards. The most–implemented principles are:

- the right to seek remedies through the courts (17/20 countries);
- data deletion (16/20);
- provision of a DPA (14/20); and
- restrictions on data exports based at least in part on the laws of the recipient country (14/20).

Eight of the 10 principles are included in the laws of at least 11/20 countries, and only two have had relatively little inclusion:

- limits on automated processing (5/10); and

[5] See Wikipedia 'G20' for a discussion of the unclear basis of the selection of countries to be members <https://en.wikipedia.org/wiki/G20>.

- additional restrictions on some sensitive processing, such as prior checking (8/20).

If the same information as is in the Table is considered from the perspective of which of the 'top 20 by GDP' countries has the highest implementation of 'European principles', this analysis shows that Peru, South Africa and South Korea have the highest level of implementation (at least 9 of the 10 principles), whereas Chile and Indonesia have the lowest implementation (2 or less). The full result in order of country is as follows: Peru (10); South Africa (9); Korea (South) (9); Argentina (8); Colombia (8); Malaysia (8); Canada (7); Taiwan (7); Australia (6); Hong Kong (6); New Zealand (6); Philippines (6); Israel (5); Japan (5); Mexico (5); Singapore (5); India (4); Vietnam (3); Indonesia (2); and Chile (1).

In terms of impact of these laws on organisations processing personal data, a high score in terms of implementation of European principles is only part of the story, because this does not attempt to measure the effectiveness of enforcement. In some cases, despite a lower score in terms of number of European principles, a jurisdiction, such as Hong Kong with a mature data protection law and active DPA, may have a more significant impact on companies now than some other countries with higher adoption 'on paper' of European principles.

Future strengthening of 2nd generation principles

The above results are not static, because some of the 20 countries included in the Tables have significant reform Bills in progress. In the two lowest-scoring countries, Chile's Bill if enacted, will include creation of a DPA, and add principles concerning data exports, fair and lawful processing, deletion, and sensitive data,[6] and the proposed comprehensive Indonesian law[7] which will include a DPA, data export restrictions, and other '2nd generation' elements. Other legislation is under consideration in New Zealand.

If enacted, these Bills will result in the average implementation of principles increasing to greater than 6/10, probably more like 6.5/10. This 6.5/10 average is a result not very different from the average of 7/10 inclusions when 33 countries, not restricted to those with high GDP, were assessed in 2012. This suggests that there might only be a modest difference if all 66 countries outside Europe which currently have data privacy laws are assessed.

Conclusions: European influence continues

We can conclude that there are strong indications that 'European' or '2nd generation' data privacy standards are continuing to be adopted outside Europe to such a substantial extent that the 'global standard' is at present at least mid-way between the '1st generation'/'OECD' standards and the '2nd generation'/'European' standards.

[6] R Nelson-Daley 'Chile: Data protection amendment bill "fulfils Government's commitment to OECD" *Data Guidance* 23 March 2017.

[7] G. Greenleaf *2014-2017 Update to Graham Greenleaf's Asian Data Privacy Laws - Trade and Human Rights Perspectives* (July 12, 2017). UNSW Law Research Series; UNSW Law Research Paper No. 47. <https://ssrn.com/abstract=3000766>, p32.

2nd Generation – 'European standards' – post-1995	**EU 1995 Directive**	**Laws outside Europe implementing standards** (20 highest GDP countries with data privacy law)	**/20**
Recourse to the courts to enforce data privacy rights (incl. compensation, and appeals from decisions of DPAs)	EU Dir 22, 23 *GDPR 78, 79, 82*	Argentina, Canada, Chile, Colombia, HK, India, Indonesia, Israel, Korea, Mexico, New Zealand, Peru, Philippines, Taiwan, Singapore, South Africa, Vietnam	17
Destruction or anonymisation of personal data after a period	EU Dir 6(1)(e) *GDPR 5(1)(e)*	Argentina, Australia, Canada, Colombia, HK, Indonesia, Japan, Korea, Malaysia, Peru, Philippines, New Zealand, Taiwan, Singapore, South Africa, Vietnam	16
Restricted data exports based on data protection provided by recipient country ('adequate'), or alternative guarantees	EU Dir 25 *GDPR 44-49*	Argentina, Australia, Colombia, India, Israel, Japan, Korea, Malaysia, Peru, Mexico, New Zealand, Singapore, Taiwan, South Africa	14
Independent Data Protection Authority(-ies) (DPA)	EU Dir 28 *GDPR 51-59, 77*	Australia, Canada, Colombia, HK, Israel, Japan, Malaysia, Peru, Korea, Mexico, New Zealand, Philippines, Singapore, South Africa	14
Minimum collection necessary for the purpose (not only 'limited')	EU Dir 6(1)(c), 7 *GDPR 5(1)(c)*	Argentina, Australia, Canada, Colombia, HK, India, Korea, Malaysia, Peru, New Zealand, Taiwan, Singapore	12
General requirement of 'fair and lawful processing' (not only collection)	EU Dir 6(1)(a) *GDPR 5(1)(a), 6*	Argentina, Canada, Colombia, Israel, Korea, Malaysia, Mexico, Peru, Philippines, Taiwan, South Africa	11
Additional protections for sensitive data in defined categories	EU Dir 8 *GDPR 9, 10*	Argentina, Australia, Colombia, Japan, Korea, Malaysia, Mexico, Peru, Philippines, Taiwan, South Africa	11
To object to processing on compelling legitimate grounds, including to 'opt-out' of direct marketing uses of personal data	EU Dir 14(a), (b) *GDPR 21*	Argentina, Australia, Canada, HK, Israel, Korea, Malaysia, Peru, Taiwan, Vietnam, South Africa	11
Additional restrictions on some sensitive processing systems (notification; 'prior checking' by DPA etc.)	EU Dir 20 *GDPR 36*	Colombia, Canada, HK, Japan, Korea, Malaysia, Peru, South Africa	8
Limits on automated decision-making (incl. right to know processing logic)	EU Dir 15, 12(a) *GDPR 22*	Argentina, New Zealand, Peru, Philippines, South Africa	5
Av. over 20 countries = 5.95/10 principles			**119**