UNSW Law & Justice Research Series

Model provisions for data protection in Commonwealth countries: How do they fit?

Graham Greenleaf

[2024] *UNSWLRS* 7
(2023) 184 *Privacy Laws & Business International Report*, 21-27

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@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

Model provisions for data protection in Commonwealth countries: How do they fit?

Graham Greenleaf, Professor of Law & Information System, UNSW Sydney.

[2023] 184 Privacy Laws & Business International Report, 21-27

The Commonwealth comprises 56 Member States[1] almost all of which have English as a *lingua franca,* a legal system based on the common law, and a colonial/constitutional history linked to the UK. Nevertheless, they do not have a great deal in common when it comes to data protection and privacy laws. The traditional common law did not include a tort of invasion of privacy, but some Commonwealth jurisdictions have introduced versions of such a tort (e.g. in Canada, and New Zealand), and some have extended the action for breach of confidence to protect personal information (e.g. the UK). Data privacy legislation has been enacted, albeit with very significant variations, in 41 Member States, but that still leaves 15 Commonwealth jurisdictions (UN member states) with no such legislation.[2]

This article examines the potential significance of a new Commonwealth initiative for the global development of data privacy laws and considers where that initiative sits in comparison with other international data privacy standards.

Development of model provisions

The Commonwealth's *Model Provisions on Data Protection*[3] (CMP) was adopted in November 2022[4] by Commonwealth Law Ministers meeting in Mauritius, after all Members were asked for final comment. The process of developing the model provisions began in 2018, with the convening of an expert working group nominated by Commonwealth countries. After discussion of desirable scope, a draft of the law was prepared by data privacy experts Dr Orla Lynskey (LSE Law School)[5] and Ms Judith Rauhofer (Edinburgh Law School).[6] The group agreed that the provisions 'should reflect general principles that are

---

[1] Member States of the Commonwealth <https://en.wikipedia.org/wiki/Member_states_of_the_Commonwealth_of_Nations>

[2] Dominica; Fiji; Kiribati; Maldives; Mozambique; Namibia; Nauru; Palau; Papua New Guinea**;** Samoa; Solomon Islands; South Sudan; Tonga; Tuvalu; and Vanuatu.

[3] Commonwealth Secretariat *Model Provisions on Data Protection* 2023 <https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-02/ROL%20Model%20Law%20Provisions%20on%20Data%20Protection.pdf?VersionId=Fpgmtvhd6E3dm3JfQiEVp8lP0zO_mGy0>

[4] 'Commonwealth ministers adopt new model law to strengthen data protection rules' 1 December 2022 <https://thecommonwealth.org/news/commonwealth-ministers-adopt-new-model-law-strengthen-data-protection-rules>

[5] Dr Orla Lynskey <https://www.lse.ac.uk/law/news/2022/orla-lynskey-model-law>

[6] Ms Judith Rauhofer < https://www.law.ed.ac.uk/news-events/news/judith-rauhofer-co-authors-major-review-commonwealth-model-laws-data-protection>

augmented by detailed rules where appropriate'.[7] The working group negotiated the complex text of the provisions through five revisions (to October 2020), before finalising the version that was adopted first by a senior officials meeting (2021), and then by law ministers in Mauritius (2022).

Although described as 'model provisions', the result is a comprehensive data privacy Bill, but one that includes optional provisions, with optional text in square brackets. Despite their potential significance, the Model Clauses are as yet little known or analysed.

Potential significance

These provisions could be of future significance in two main ways. First, the fifteen Commonwealth countries that have no data privacy laws as yet could use the whole of the Model Provisions as a template for their law, particularly in the Pacific Islands where no countries have data privacy laws as yet. Second, the 41 Commonwealth countries that already have a data privacy law could use the Model Provisions as a source of suggestions for revisions to their law to bring it more into line with international standards.

There is no association of data protection authorities from Commonwealth countries,[8] or anglophone countries (unlike the francophone association), so there is no obvious forum, other than the Commonwealth itself, to encourage compliance with the Model Provisions.

There is no known suggestion or indeed likelihood that the Model Provisions should be converted into the clauses of a Commonwealth-wide Treaty or Convention. The Commonwealth has no Treaties or Conventions. Their closest analogy is to the OECD privacy Guidelines and APEC Privacy Framework, which are recommendations. In this sense the CMP contrasts with Council of Europe Convention 108/108+, or the African Union Convention, or the GDPR. However, all of these are the international privacy instruments with which the CMP should be compared.

Comparison of Model Provisions with other international standards

The *Commentary and International Comparisons* ('Commentary') included in the CMP includes an excellent clause-by-clause comparison of most Provisions against the most important international data privacy instruments (OECD Guidelines, APEC Framework, Convention 108/108+, GDPR and African Union Convention), using the same numbering as CMP. However, the Commentary does not give an overall comparison of the whole of the Provisions against each of these instruments, in order to estimate where the CMP 'fits' in terms of the strength of its requirements. For example, will laws enacted based on the CMP enable ratification of Convention 108+, or facilitate a positive GDPR adequacy finding, or suffice for African Union Convention ratification? Or would they only meet the weaker standards of compliance with the OECD Guidelines or APEC Framework?

Such comparisons cannot be precise, for the simple reason that the CMP includes many sub-provisions which are optional (indicated by enclosure in square brackets). As a result, the

---

[7] *Model Provisions* 'Background'.

[8] BIIDPA (British, Irish and Islands' Data Protection Authorities) has existed since the 1980s and has 8 members. It hosts annual roundtables, the most recent in Malta (2023). BIIDPA members included the UK, Ireland, Cyprus, Jersey, Isle of Man, Malta, Gibraltar and Bermuda, with no new members since 2016.

'strength' of the CMP depends on how many of these optional inclusions are assumed to be part of it. When a countries' law is enacted or amended based on the CMP, its strength will depend to a significant extent on how many optional elements it includes.

In order to facilitate such an overall comparison, the following Tables classify each of the principles in the Model Provisions as being 1st, 2nd, or 3rd 'generation' principles,[9] according to where they first appeared in the European or international instruments under consideration. These 'generations' of data privacy principles are cumulative: '1st generation' standards such as the individual right of access continue to exist in new instruments such as the GDPR which embody '3rd generation' standards.[10] This approach to analysis via 'generations' of data privacy principles, has been more fully explained and utilised elsewhere.[11]

The conventions used in these Tables are generally self-explanatory (e.g. CoE108 = Council of Europe Convention 108 1981).[12] A dash (–) indicates the absence of the principle from an instrument (so '– CoE108' means that the particular principle is not found in Convention 108).

Basic elements

There are a few foundational elements of a data privacy law, common to all international instruments, that do not appear in the four sets of 'generational' principles following. CMP's adherence to those basic requirements should be noted:

- *Comprehensive sectoral scope* – CMP applies comprehensively to both private sector and public sector bodies. CMP 3 defines 'data controller' to include 'public authority or other entity'.
- *Processing* is given a comprehensive functional definition (CMP 3), and includes both automated processing and non-automated processing if part of a file (CMP 4(1).
- *Rights apply to all data subjects*, irrespective of nationality, residence, or citizenship. CMP 3 defines 'data subject' to include 'any natural person' (see later re legal persons).

---

[9] '1st generation' refers those standards which are common to Convention 108 of 1981 and the OECD privacy Guidelines of 1980. '2nd Generation' refers to principles first found in the EU data protection Directive of 1995 (DPD) and the Amending Protocol to Convention 108 of 2001. '3rd Generation' refers to the additional principles found in the EU GDPR of 2016 and in Convention 108+ of 2018. There are two Tables for '3rd Generation' principles because they are divided into those common to both the GDPR and Convention 108+, and those which are only found in the GDPR but not in Convention 108+, thus providing four Tables.

[10] As a result of this approach, instruments (such as the 3rd generation GDPR and CoE108+) which post-date a particular generation of standards (such as Table 2 for the 2nd Generation') do appear in the Table concerning those earlier principles, because they may embody them.

[11] Greenleaf, Graham and Cottier, Bertil '*International and regional commitments in African data privacy laws: A comparative analysis*' [2022] *Computer Law & Security Review* Volume 44, April 2022, 105638; Preprint April 22, 2020 available at <https://ssrn.com/abstract=3582478>

[12] To clarify further: OECD 1980 = OECD privacy Guidelines 1980; CoE108 = Council of Europe Convention 108 1981; &AP = Additional protocol of 2001 to Convention 108; C108+ = 'modified' Convention 108 of 2018; DPD = EU Data Protection Directive of 1995; GDPR = EU General Data Protection Regulation of 2016; AUC = African Union Convention 2014.

- *Definition of* 'personal data', since the first laws and international instruments,[13] has been any information which provided 'identifiability' (not 'identification'). CMP 3 definition of 'personal data' 'means any information relating to an identified or identifiable individual'. Of international instruments, only the APEC Framework refers to 'personal information', but many national laws continue to do so.

- *Publicly available information* is not excluded from the definition of 'personal data', consistent with most international instruments.

- *Processing for personal or domestic purposes' is an exception from the law* (CMP4(3)(a), but the Commentary suggest that laws may require some balancing factors.

- *It is optional whether 'the law does not apply' to processing for each of these purposes: national security; law enforcement; journalistic, artistic or literary; and academic or archiving* (CMP 4(3)(b)-(e)). These are intentional unconditional exemptions from application of a data privacy law, to which the requirements to apply conditions protective of 'the essence of fundamental rights and freedoms' and 'proportionality' (CMP 22 and 6(5)) do not apply. However, if exceptions to controllers' obligations or data subject's rights are made under 'national law', they must provide such protections (CMP 22(1)), and for processing to be lawful it must be based on national law compliant with CMP 22(1). The Commentary says such national security and law enforcement complete exceptions must be 'subject to compliance with individual rights and freedoms', but the source of this protection remains unexplained. The completely different treatment of exceptions from the law under CMP 4(3) makes little sense and is CMP's weakest and worst provision.

CMP comparison with 1st Generation principles (1980-) (Table 1)

The 1st Generation principles are those common to both the OECD privacy Guidelines 1980 and CoE Convention 108 1981. These are the fundamental international privacy instruments from which others derive. Table 1 compares the sections where these ten principles are found with their equivalents in the CMP, and (where found) their equivalents in the African Union Convention (AUC). Their 3rdGeneration equivalents in the GDPR are also shown.

I	1st Generation principles	Commonwealth Model Provisions 2023	OECD 1980	CoE108 1981	AUC 2014	GDPR 2016
1.01	*Collection* – limited (not excessive), lawful (for legitimate purposes) and by fair means	CMP 6(1), 6(2)- lawful; 7 - fairness	OECD 7	C108 5(a), (c)	–	GDPR 5(1)(a)
1.02	*Data quality* – relevant, accurate, up-to-date	CMP 10 – 'adequate, relevant'; CMP 12 – 'accurate and complete', 'kept up-to-date'	OECD 8	CoE108 5(c)(d)	AUC 13(4)	GDPR 5(1)(d)
1.03	*Purpose specification* by time of collection	CMP 8(2)(b)	OECD 9	CoE108 5(b)	–	GDPR 5(1)(b)

[13] For example, both the OECD Guidelines and Convention 108 refer to 'any information relating to an identified or identifiable individual', and the French law of 1978 also used the 'identifiability' criterion.

1.04	*Notice of purpose/rights* [implied, but not explicit until later instruments.]	CMP 8(2) - notice	OECD 9	CoE108 5(b)	AUC 15	GDPR 13, 14
1.05	*Uses limited* (including disclosures) to purposes specified or compatible	CMP 9(1) - processed	OECD 10	CoE 108 5(b)	AUC 13(3)(a)	GDPR 5(1)(b)
1.06	*Security* through reasonable safeguards	CMP 13 – data security	OECD 11	CoE 108 7	AUC 13(6);20; 21	GDPR 5(1)(f), 32
1.07	*Openness* re personal data practices (not limited to data subjects)	CMP 8(1) - transparency	OECD 12	CoE 108 8(a)	–	GDPR 14(5)(b)
1.08	*Access* – individual right of access	CMP 19 – subject access	OECD 13	CoE 108 8(b)	AUC 17	GDPR 15
1.09	*Correction* – individual right of *correction*	CMP 20 – right to rectification	OECD 13	CoE 108 8(c), (d)	AUC 19	GDPR 16, 19
1.10	*Accountable* – identified data controller accountable for implementation	CMP 14 – accountability of data controller	OECD 14	CoE 108 8	–	GDPR 5(1)(f)

Table 1 demonstrates that the Commonwealth Model Provisions (CMP) satisfy all 10 of the requirements of the OECD Guidelines of 1980, noting that the 2013 revisions of the Guidelines added a requirements of data breach notification and demonstrable accountability[14] (for CMP inclusion, see Tables 3 and 4). The APEC Framework is essentially the same as the OECD Guidelines (now including the 2014 data breach notification requirement). Tables 1 and 2 (following) show that the CMP also satisfies the requirements for CoE Convention 108 of 1981, although it is now too late for new countries to accede to it, rather than to Convention 108+.[15]

CMP comparison with 2nd Generation principles (1995–) (Table 2)

The 2nd Generation of data privacy principles is based on the EU data protection Directive of 1995 (DPD 1995), and CoE Convention 108 (with Additional Protocol 2001),[16] and can therefore be called 'European standards'. There is no OECD equivalent. Table 2 shows the CMP equivalents, the DPD and CoE108 provisions, and those of the AUC and the GDPR.

[14] See clauses 15(b) and (c) of *The OECD Privacy Framework* (OECD, 2013) <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>

[15] New countries must also accede to the Protocol which creates 'Convention 108+' – see Table 3.

[16] Although principles 2.01, 2.02 and 2.03 were in the original Convention 108, they are not included in the 1st generation principles, because they were not also included in the OECD Guidelines. They were therefore not part of the common set of principles shared by the OECD Guidelines and Convention 108 as at 1980/1981.

II	2nd Generation principles – 'European standards'	Commonwealth Model Provisions 2023	EU DPD 1995	CoE108 1981 & AP 2001	AUC 2014	GDPR 2016
2.01	*Minimum collection* necessary for purpose (data minimisation)	CMP 10 – Data Minimisation – 'not excessive'	DPD 6(1) (b),(c), 7	CoE108 5(c)	AUC 10(3)(b)	GDPR 5(1)(c);
2.02	*Destruction or anonymisation after purpose completed*	CMP 11 – Storage Limitation – identifiable 'for no longer than is necessary'	DPD 6(1) (e)	CoE108 5(e)	AUC 22	GDPR 5(1)(e);
2.03	*Additional protections for sensitive data* in defined categories	CMP 3 def. 'sensitive personal data' – [all categories optional]	DPD 8	CoE108 6	AUC 1def; 14	GDPR 9, 10
2.04	*Legitimate bases for processing defined*	CMP 6(2); 6(3) consent or 7 optional grounds	DPD 7	– CoE108	AUC 1 def; 13(1), (2)	GDPR 6
2.05	*Additional restrictions on some sensitive processing systems* (notification; 'prior checking' by DPA etc)	CMP 18 'Prior authorisation' if 'high degree of risk'	DPD 20	– CoE108	AUC 10(2)-(4)	GDPR 36
2.06	*Limits on automated decision-making* (incl. right to know processing logic)	CMP 21(1)(a) – [optional] basis for right to object	DPD 15, 12(a)	– CoE108	– AUC	GDPR 22
2.07	*To object to processing on compelling legitimate grounds*	CMP 20(2) – erasure if illegal; CMP 21(1) Right to Object [optional] on 'legitimate grounds'	DPD 14(a), (b)	– CoE108	AUC 18	GDPR 21
2.08	*Restricted data exports* requiring recipient country 'adequate', or alternative guarantees	CMP 23(1) (a) [DPA] / [govt.] decision that recipient country ensures [adequate] [equivalent] [appropriate] protection or [optional (b) 'appropriate safeguards'] or [optional (3) conditions]	DPD 25, 26	CoE108 AP 2	AUC 14(6)(a)	GDPR 45–47
2.09	*Independent Data Protection Authority(-ies)* (DPA)	CMP 24(1) 'independent supervisory authority' ; CMP 25 – 5 conditions of independence;	DPD 28	CoE108 AP 1	AUC 11(1)(b)	GDPR 51-59, 77
2.10	*Recourse to the courts* to enforce data privacy rights	CMP 29 – DPA can refer infringements to judicial authority; CMP 30 – (1)-(2) appeals against DPA; (3) right to an 'effective judicial remedy' against breaches;	DPD 22, 23	CoE108 AP 1(4)	– AUC	GDPR 78, 79, 82

Table 2 demonstrates that the CMP satisfies all ten 2nd Generation requirements, but with two caveats. Principle 2.06 (automated decision-making) is optional in CMP 21(1). Principle 2.08 (restricted data exports) is not optional, but CMP 23 allows three ways of expressing the level of protection required for a government or DPA positive decision. Other forms of protection are however optional. The data export requirements are very important to both GDPR and CoE108+ requirements, but it is possible that CMP meets their standards. The CMP requirements of eight to ten 2nd Generation principles puts CMP at either the same standard (or higher) than the average of the laws in the 164 countries that already have data privacy laws.[17] However, CMP also requires some inclusion of 3rd Generation principles, which makes it a clearly higher standard than the average national data privacy law.

CMP comparison with 3rd Generation Common European Principles (Table 3)

These 2nd Generation European standards have now evolved into a more strict 3rd Generation. The EU has enacted the GDPR, and the Parties to Convention 108 (including its non-European, predominantly African, parties) have adopted the amending protocol to convert it into Convention 108+ (not yet in force), with higher standards. These higher standards are reflected in the next two tables. Table 3 includes the ten 3rd Generation principles which are common to both the GDPR and Convention 108+. Table 4 includes eight other principles found only in the GDPR (as yet). There is no OECD or APEC equivalent to these third generation principles, except that principle 3.03 (*Data breach notification to DPA* for serious breaches) is included in the 2014 revision of the OECD Guidelines, and reflected in subsequent APEC Framework amendments.

IIIA	3rd Generation – Common European Principles	Commonwealth Model Provisions 2023	AUC 2014	C108+ 2018	GDPR 2016
3.01	*Data protection by design and by default*	CMP 17 – 'shall design and implement' … 'prevents or minimizes … interference'	– AUC	CoE108+ 10(2)-(4)	GDPR 25
3.02	*Demonstrable accountability* by controllers	CMP 14(1), (4)	– AUC	CoE108+ 10(1)	GDPR 5(2)
3.03	*Data breach notification to DPA* for serious breaches	CMP 13(4); CMP 3 defn. 'personal data security breach'	– AUC	CoE108+ 7(2)	GDPR 33
3.04	*Direct liability for processors* as well as controllers	CMP 13(3)(b)	– AUC	CoE108+ 7(1), 10(1)	GDPR 28-31
3.05	*Stronger consent requirements*	CMP 6(3)(a) – 'has [freely] given his or her [specific] [informed] [and unambiguous] consent'; CMP 6(4) – explicit consent for 'sensitive personal data'	– AUC	CoE108+ 5(2)	GDPR 7, 8

[17] The estimate of at least seven of ten 2nd Generation principles is the author's unpublished estimate, based on the 162 data privacy laws in G. Greenleaf 'Global Tables of Data Privacy Laws and Bills (8th Ed.) 2023'. <https://papers.ssrn.com/abstract_id=4405514 >, plus new laws in Grenada, and Democratic Republic of Congo.

3.06	*Proportionality required* in all aspects of processing	– CMP (but see CMP 22(1) and 6(5))	– AUC	CoE108+ 5(1), 10(4)	GDPR *passim*
3.07	*DPAs to make decisions and issue administrative sanctions* incl. fines	CMP 32 – data subjects or 3rd parties may lodge complaints; CMP 28 – DPA investigative powers; CMP 29 – DPA corrective powers	AUC 12(2)(h)	CoE108+ 12	GDPR 58(1)
3.08	*Biometric and genetic data require extra protections*	CMP 3 defn. 'sensitive personal data' – '[genetic] [biometric]'	AUC 104(a), (d)	CoE108+ 6(1)	GDPR 9
3.09	*Stronger right to erasure* incl. 'to be forgotten'	– CMP (but see CMP 20(2))	AUC 19	CoE108+ 9(1)(d),(e)	GDPR 17, 19
3.10	*DPAs to cooperate in resolving complaints with international elements*	CMP 30	AUC 12(2)(m)	CoE108+ 16-21	GDPR 50

Table 3 demonstrates that the CMP includes eight of the ten common European 3rd Generation principles, although 3.05 (stronger consent) and 3.07 (biometric and genetic data) could be made ineffective because their elements are optional. Two 3rd Generation principles, 3.06 (proportionality) and 3.09 (stronger erasure) are not explicitly included in CMP, but proportionality is central to CMP 22(1) and 6(5), and the 'right to be forgotten' is a possible interpretation of CMP 20(2). Their literal enactment is probably not vital to GDPR adequacy or CoE 108+ compliance. The inclusion of so many 3rd Generation elements in CMP makes it a very 'modern' international privacy instrument, bringing it close to meeting the requirements of the two most important 3rd Generation instruments, the GDPR and Convention108+. The CMP also clearly exceeds the requirements of the African Union Convention (AUC).

CMP comparison with 3rd Generation Additional (GDPR only) Principles (Table 4)

None of the eight principles in Table 4, required by the GDPR, are required by Convention 108+, so their omission is no detriment to CoE 108+ ratification, and it is not in the Table. The Table shows that the CMP meets four of the additional eight requirements of the GDPR.

IIIB	3rd Generation – GDPR only (not in CoE 108+)	Commonwealth Model Provisions 2023	AUC 2014	GDPR 2016
3.11	*Mandatory Data Protection Impact Assessments (DPIAs) for high-risk processing*	CMP 14(2)(a) 'entails a risk' requires 14(3)(c) 'privacy risk assessment'; 15(1) 'likely … high risk' requires 'data protection impact assessment'	– AUC	GDPR 35, 36
3.12	*Extra-territorial jurisdiction,* where goods or services offered, or behaviour monitored	CMP 5(2) – requirement, not optional	– AUC	GDPR 3

3.13	*Extra-territorial controllers or processors must be represented within jurisdiction*	– CMP	AUC 2(3)	GDPR 27
3.14	*Right to data portability*	– CMP	AUC 23	GDPR 20
3.15	*Mandatory Data Protection Officers (DPOs)* for sensitive processing	CMP 16 – applies to *al*l controllers	– AUC	GDPR 37-39
3.16	*Data breach notification to data subjects* (if high risk)	CMP 13(5) – data controller obligation; CMP 29(1)(a) – DPA may order controller to notify	– AUC	GDPR 34
3.17	*Representative actions before DPAs or courts by public interest privacy groups*	– CMP (but local laws may allow such representative actions; also; CMP 34(1) – right to seek compensation, and 34(3) to appoint a representative to do so.)	– AUC	GDPR 80
3.18	*Maximum admin. fines based on annual turnover,* global or local	– CMP (but CMP 29(1)9h) requires DPAs to have powers to 'impose an administrative fine, but no objectives or upper limits stated)	– AUC	GDPR 83(4)-(6)

Table 4 demonstrates that the CMP includes four of these eight 'GDPR only' principles, but also partially satisfies two others (3.17 and 3.18). The two remaining omissions (3.14 data portability and 3.15 representation of extra-territorial controllers) are at the lesser end of importance of principles. The CMP is therefore very strong in its inclusion of 'GDPR-only' 3rd Generation principles.

CMP Principles not found in other instruments

In addition, the Commonwealth Model Principles has some provisions not found in other instruments, including:

- CMP applies to processing of data on deceased persons, for a period of years following their death, to be specified in the law (CMP 4(2)). Such laws are already found in six EU member states,[18] and elsewhere including some African states.
- Data subjects can also optionally include legal persons (CMP 3 defn. 'data subject'). Only the GDPR leaves open the possibility that legal persons can be protected. The Commentary points out some advantages of such inclusion, but not that there is a risk that corporate misconduct might be protected. CMP lacks provisions to safeguard against this risk, such as countervailing rights to others to be notified, or to oppose actions.
- The supervisory authority is required to publish at regular intervals information about data security breaches reported to it (CMP 13(6)).

Conclusions – Where do the Commonwealth Model Provisions fit?

The Commentary says the CMP's data protection principles (Pt IV) is 'designed to align with current international standards', and this could be said of all aspects of the CMP. Interpreted

[18] Commentary: Denmark, France, Hungary, Italy, Slovakia and Spain.

at its strongest, the CMP proposes implementation of 32/38 of the principles listed in the four tables (10/10; 10/10; 8/10; 4/8), but this is weakened by their full implementation being made optional in at least five principles. Nevertheless, of the 134 current laws in non-EU/EEA countries, there would be no more than a handful which embody such a strong implementation of data privacy principles.

However, CMP allows complete exceptions under CMP 4(3)(b) and (c) for national security and law enforcement purposes, instead of bringing them under the restrictions required of legislative exceptions under CMP 22. This inconsistency is unexplained, and if the option is exercised it could undo much of the good of the rest of CMP.

Subject to this qualification, the Commonwealth has therefore developed one of the strongest international privacy instruments. The effect of this could be evident both in the implementation of new laws in the 15 Commonwealth countries without such laws, or in the updating of existing laws in the 41 other Commonwealth countries. However, 'updating' is not necessarily 'strengthening' and it is important that strong standards for data exports in some recent laws (e.g. Kenya and Rwanda) should not be reduced. The CMP should make a major contribution to the quality of global data privacy laws. Such adoption is for the future and deserves to be monitored.

Information: Valuable comments have been provided by Tamar Kaldani (independent scholar), and by David Erdos (Cambridge Law Faculty), but all content is the responsibility of the author.