ASEAN Model Contractual Clauses: Low and Ambiguous Data Privacy Standards

Graham Greenleaf

[2021] *UNSWLRS* 83
(2021) 174 *Privacy Laws & Business International Report* 22-24

UNSW Law
UNSW Sydney NSW 2052 Australia

ASEAN Model Contractual Clauses: low and ambiguous data privacy standards

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

(2021) 174 *Privacy Laws & Business International Report* 22-24.

The Association of Southeast Asian Nations (ASEAN) *Model Contractual Clauses* ('ASEAN MCCs')[1] are contractual terms and conditions that may be voluntarily included by companies in binding legal agreements for the cross-border transfer of personal data. The ASEAN Digital Ministers endorsed them in January 2021.

ASEAN has 10 'ASEAN Member States' (AMS), of which six have data privacy laws: Singapore, Malaysia, Thailand (not yet in force), Indonesia (undergoing reform), Vietnam (new decree in process), and the Philippines. Brunei has a draft Bill under consultation. The remaining three, Myanmar, Cambodia, and Laos, have no significant data privacy laws. The data privacy standards set by the seven laws, including their requirements for personal data exports, are not at all uniform.[2] Therefore, unlike in the EU where the GDPR sets a common standard that data exports must meet, including for Standard Contractual Clauses (SCCs) (GDPR, art. 46(2)(c) and (d)), it is a more challenging exercise to develop such clauses for transfers within and from AMS.

ASEAN's MCCs therefore differ from the EU's SCCs in that there is no legal basis for their effectiveness, either in legislation (like the GDPR) or in a treaty or other agreement between AMS. As yet, there is no legislation in any AMS that states that if these clauses are utilised then the transfer will comply with the law of that AMS. The MCCs specifically state that they are 'a voluntary standard' which can be modified 'as long as they do not contradict the MCCs'.[3] However, such contradiction does not have any apparent consequences. The MCCs also state that parties using them are 'also free to use any other valid data transfer mechanisms recognised within ASEAN, if or when they are available or relevant to AMS. As yet, the only such mechanisms are those which are set out in the national laws of AMS.[4]

Standard (or model) contractual clauses can be a valuable way of regulating the flow of personal data, provided they align with the requirements of the exporting country's data privacy laws. They are of particular value to SMEs as a low-cost means of compliance, because companies do not have to negotiate them in each instance but can rely on their being pre-approved as complying with the country's data export requirements. This can be achieved at the national level, but it is more difficult to achieve across a group of countries such as the ASEAN member states which have considerable differences in their data export requirements.

Therefore, while MCCs are a valuable idea in principle, finding suitable clauses to meet the needs of a group of countries may be difficult in practice.

---

[1] *ASEAN Model Contractual Clauses for Cross Border Data Flows*, January 2021 <https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf >

[2] See G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), and many articles since then in issues of this Report.

[3] ASEAN MCCs, p. 4.

[4] The APEC Cross border Privacy Rules (CBPRs) are not 'recognised within ASEAN', and Singapore is the only ASEAN country that is a full participant in CBPRs, so they do not seem to be relevant here,.

A 1980s standard for the 21st century?

The ASEAN MCCs state that they are 'primarily designed for intra-ASEAN flow of personal data', they may be adapted for 'transfers to non-AMS, particularly those with legal regimes based upon the principles of the *APEC Privacy Framework* or *OECD Privacy Guidelines*, from which the principles in the *ASEAN Framework on Personal Data Protection* (2016) are derived'.[5] This ASEAN Framework[6] does not add anything to its 1980 (OECD) and 2004 (APEC) predecessors, except:

(i) Transfers of personal data to another country require that an organisation should obtain the data subject's consent or 'take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles' (cl. 6(f)).
(ii) A very weak 'retention' principle requires destruction or anonymisation after the information is no longer of use for 'legal or business purposes'.

These are inconsequential additions to the underlying 1980 OECD standards: (i) does not require 'standards equivalent to those of the law of the exporting AMS', which may be higher than those of the ASEAN Framework; and (ii) does not require that retention is consistent with 'the purpose of collection,' but just any business purpose.

The irony of this lowest-common-denominator standard for the MCCs is that most AMS countries that have data privacy laws (or are revising them) do not base those laws on the OECD Guidelines, but are more influenced by the EU's Data Protection Directive (1995) and GDPR (2016). This is the case for Thailand, and for the proposed reforms in Indonesia and Vietnam.[7] Malaysia and the Philippines have some standards higher than OECD standards. What use is it for ASEAN countries to agree on standards for data exports which are weaker than their own national laws require?

In a further irony, the ASEAN MCCs are not content with the standards set by the ASEAN Framework on Personal Data Protection (PDP). They require two additional standards to be observed, and recommend a third:[8]

(a) Data exporters must warrant 'that the data is collected, used, disclosed and transferred in accordance with applicable AMS law', or (where there is no such law) 'Data Subjects have been notified and given consent to the purposes, where reasonable and practicable'.
(b) A Data Breach Notification (DBN) requirement (to 'relevant authorities' within a 'reasonable time') is added, reflecting that a DBN requirement has been added to the 2013 review of the OECD Guidelines, and the APEC Framework, but not to the ASEAN Framework.
(c) Unfortunately, the OECD/APEC/ASEAN standards do not deal with onward transfers by an importer of personal data from an AMS. The ASEAN MCCs are content to 'encourage' the importer in the MCC contract to voluntarily 'conduct due diligence [on

[5] ASEAN MCCs, p. 4.
[6] ASEAN Framework on Personal Data Protection (PDP) (2016) <https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf>
[7] See; Greenleaf, G 'Vietnam: Data privacy in a communist ASEAN state' (2021) 170 Privacy Laws & Business International Report, 1, 5-8; Greenleaf, G. and Rahman, A. A. 'Indonesia's DP Bill lacks a DPA, despite GDPR similarities' (2020)164 *Privacy Laws & Business International Report* 1, 3-7; Greenleaf G and Suriyawongkul A 'Thailand – Asia's Strong New Data Protection Law' 160 Privacy Laws and Business International Report 1, 3-6, 2019.
[8] ASEAN MCCs, p. 5.

> the 3rd party importer] to ensure that they area also able to meet the obligations imposed by these MCCs'.

The effect of obligation (a) is that exporters must warrant that they comply with many of the key obligations of their local law (collection, use, disclosure and transfer), even though these obligations may be more onerous than those required by the ASEAN Framework. Compliance with the Framework's principles is therefore not the real basis of the MCCs, what is required is compliance with the requirements of the 'applicable AMS law'. Data controllers could easily be confused about what standard they are required to meet when data is transferred.

Provisions (a) and (b) are desirable but (a) is ambiguous. It is necessary to imply that the 'relevant AMS law' is that of the country in which the exporter is based, but it is possible that the exporter might also be bound to comply with some other AMS law, for example because of extra-territoriality provisions. The ambiguity of 'relevant AMS law' will also be apparent in the text of the MCCs themselves.

The failure of (c) to do more than 'encourage' controls on onward transfers is likely to create insurmountable problems with these clauses being regarded as 'interoperable' (or some other form of 'compatible') with EU GDPR requirements, including EU SCCs.

The texts of the MCCs

The ASEAN MCCs include two sets of clauses, Module 1 for a 'Controller to Processor Transfer', and Module 2 for a 'Controller to Controller Transfer'.

Controller to Processor Transfer

These clauses incorporate Appendix A, a template where the identities of the exporter and importer, description of the data, and the purposes of the processing are recorded. The clauses have repeated references to 'applicable AMS law', which is ambiguous in relation both to the legal obligations of the exporter, and (as noted above) in relation to the importer's obligations concerning onward transfers.

The clauses provide that the data exporter warrants 'that the data has been collected, used, disclosed and transferred to the Data Importer under this contract in accordance with applicable AMS law', or (where there is no such law) that 'the Data Subjects have been notified of and given consent to the purpose(s) of the collection, use, disclosure and/or transfer of his/her Personal Data.' (cl 2.1). An optional clause warrants accuracy and completeness (cl. 2.2), and another warrants security during transmission (cl. 2.3). The exporter is only required to respond to 'enquiries from Data Subjects or Enforcement Authorities' 'as required by applicable AMS law', with no provision for what happens when there is no such law (cl. 2.4).

The obligations of the Data Importer are lengthier. The processor can only process the data in accordance with the Exporter's instructions and the purpose(s) set out in Appendix A (cl. 3.1). Sub-processing is not allowed unless the exporter has had 'reasonable opportunity … to object' (cl. 3.3).

Before any onward transfer or other disclosure to a third party, the importer must 'ensure that the third party shall be subject to and bound by' the same obligations as in the MCCs (cl 3.3). So in this Module the restrictions on onward transfers are not merely 'encouraged', they are a contractual requirement.

There are many more obligations on Data Importers, including provisions on handling enquiries from data subjects, data security, handling of data after the processing is completed, and details of requirements concerning data breaches (cl. 3.4-3.12).

Controller to Controller Transfer

In default, these clauses aim to ensure that 'the Data Importer' need not accept limitations on future processing of the transferred data and shall instead have the same rights and obligations possessed by the exporter … unless it specifically agrees otherwise'.[9] This is implemented by the clause 'The Data Importer shall Process the Personal Data only for the purposes described in Appendix A.' (cl. 3.1) being an optional clause. In the absence of such a restriction, it seems to be assumed that the Data Importer can do whatever they like with the data. It might not so simple if the law of the data exporter has provisions for their law to have extra-territorial effect, as will be the case in Thailand, Indonesia and perhaps other AMS.

As with controller to processor contracts, the exporter must warrant that collection, use, disclosure and transfer of the data is 'in accordance with applicable AMS law' (cl. 2.1). Those AMS provisions are therefore most important, not those in the ASEAN Framework. The exporter also must provide copies of the laws of the country 'in which the Data Exporter is established' (optional cl. 2.3).

There are various obligations on the Data Importer concerning aspects of preventing or mitigating data breaches , and disposal of data (cl. 3.2-3.6), as well as a vague optional clause attempting to shift responsibility for the data to the importer.

One clause not present, in contrast with Module 1, is any limit on onward transfers. This is where imposing standards on the third-party importer is merely 'encouraged' – or more likely, ignored.

What rights does the data subject have?

Insofar as data subjects are concerned, the ASEAN MCCs give no enforceable rights to data subjects. Some of the AMS are common law countries (Malaysia, Brunei, Singapore, and Myanmar to some extent) where part of their inheritance of the common law from the UK included the doctrine of privity of contract, which prevents data subjects from relying on provisions in an exporter-importer contract because they are not a party to it. Statutory provisions do override this in some countries, in some cases, but there must usually be a clear intention in the contract that the data subject must benefit, and that is not obvious from the ASEAN MCCs. A morass of ambiguity and statutory interpretation is not much help to data subjects.

Conclusions – not yet 'interoperable' with EU SCCs

The ASEAN MCCs are likely to be a useful tool for transfers of data between countries which have a low level of statutory data privacy provisions (ie. those based on the 1980 OECD 'family' of low standard international instruments) or have no data privacy law at all. They will be less useful for transfers where the exporter is from a country with higher standard laws more strongly influenced by the GDPR. Legislative endorsement of the MCCs could put at risk that country's position in relation to 'GDPR adequacy'.

Some ASEAN-based companies are concerned that, although the MCCs state that their use is voluntary, it is possible that some ASEAN Member States might decide to make their use

[9] ASEAN MCCs, p.15.

compulsory. Many companies are now required by their head offices to use EU SCCs, and it would be difficult to reconcile this instruction with also incorporating the ASEAN MCCs.

The MCCs have too many inconsistences and ambiguities and should be improved. Insofar as data subjects are concerned, the ASEAN MCCs give no enforceable rights to data subjects – or at least none that are predictable. This should be improved.

The EU launched its revised standard contractual clauses (SCCs) for cross-border data transfers on 4 June 2021 to reflect new GDPR requirements. Panellists at an EU-ASEAN Business Council webinar are reported to have said that more convergence is needed between ASEAN's model contractual clauses (MCCs) and the EU's revised standard contractual clauses (SCCs) for cross-border transfer of data.[10] A European Commission representative said that SCCs can help bridge differences and build convergence on a contractual level. 'It's easy for companies to use them as they provide a uniform way of dealing with data'. He said that 'once enough companies become familiar with certain aspects of data protection …they also help to raise the level of protection in certain countries.' [11]

While the MCCs do not yet provide the same standards of protection as the EU's SCCs, there seems to be value in the EU continuing to explore contractual clauses as an area where 'bridging the gap' between EU and other laws might be achieved.

[10] Karry Lai 'ASEAN model contractual clauses need convergence with the EU' *International Financial Law Review* (Jun 8, 2021) (available on Proquest).
[11] ibid