Towards A Data Protection Soft Law Framework for the ASEAN Region

by

Arianne Vanessa Tanopo Jimenez

A dissertation submitted in partial satisfaction of the requirements for the degree of

Doctor of Juridical Science

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Paul M. Schwartz
Professor John Choon Yoo
Professor Deirdre Mulligan

Spring 2016
Abstract

Towards a Data Protection Soft Law Framework for the ASEAN Region

by

Arianne Vanessa Tanopo Jimenez

Doctor of Juridical Science
University of California, Berkeley

Professor Paul M. Schwartz, Chair

The ten Member States† of the Association of Southeast Asian Nations (ASEAN) are working towards integrating their economies. The general steps to achieve this goal are laid out in the ASEAN Economic Community Blueprint. The specific measures to be taken towards economic integration are prescribed and outlined in various Plans and Strategic Schedules. One particular measure to be undertaken is the promotion of information security and data protection in the region. In furtherance of this objective, ASEAN plans to work towards having all ten Member States implement up-to-date data protection laws and regulations. It also aspires to have a harmonized, comprehensive data protection legal framework for the region.

Considering that ASEAN – an international organization that has a strong soft law tradition – is aiming for the implementation of data protection laws in all ten Member States, and intends to have a harmonized data protection legal framework for the region, the main question of this dissertation is: What are the ideal features and characteristics of a data protection soft law framework for the ASEAN region?

To answer this question, the following sub-questions must first be answered: (a) What is a “data protection soft law framework” and why is it being considered as a way to promote data protection in the ASEAN? (b) What are the lessons to be learned from the use of soft law in the ASEAN region? More specifically, what types of measures, features, and characteristics are likely to help achieve policy goals, and what are the challenges to be expected when ASEAN resorts to the use of soft law instruments in order to achieve policy objectives? (c) What are the lessons to be learned from other international data protection soft law frameworks? More particularly, what are the advantages and disadvantages of certain features and characteristics of the OECD Privacy Guidelines and the APEC Privacy Framework? What are the

† Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Viet Nam.
successes of and challenges involved in the implementation of these features and characteristics?

The answers to these questions will be distilled into a set of features and characteristics that are ideally suited to fulfill the purpose of an ASEAN data protection soft law framework.

Chapter 1 of this dissertation provides a background and introduction and, among other things, presents the rationale and significance of this study.

Chapter 2 acquaints the reader with the ASEAN as an organization, illustrates its plans for economic integration and data protection, and briefly describes the current state of data protection in the region. Chapter 2 also presents the data protection risks and challenges that will arise because of economic integration. It concludes with a discussion on soft law, in general, and soft law specifically within the context of ASEAN. The main objective of this chapter, apart from giving the reader some background and context, is to establish the timeliness and aptness of the examination of soft law as a possible tool to promote data protection in Southeast Asia.

Chapter 3 reviews significant implemented ASEAN soft law instruments, their implementation, and their results, both positive and negative. The aim of this chapter is to help demonstrate the effectiveness of soft law in attaining various goals set by ASEAN. It will also present the challenges to be expected when ASEAN resorts to the use of soft law instruments in order to achieve policy objectives. In presenting both the successes and challenges, the author intends to show which types of soft law measures previously implemented by ASEAN could likely attain specified policy objectives, and the challenges that the Association will have to contend with, if it decides to use soft law to promote data protection in the region.

Chapter 4 examines the current use of soft law in international data protection law and governance. It will look at the OECD Privacy Principles and the APEC Privacy Framework. The chapter draws out some of the features and characteristics of soft law in international data protection law, and presents the benefits and successes, and drawbacks and failures of these features and characteristics. In doing so, the author seeks to identify the distinct and prevailing elements that constitute an international data protection soft law framework. The author also shows which of these have proven beneficial and successful in attaining their purposes. Furthermore, it also aims to identify the likely challenges of using soft law to promote data protection within a region. In addition, this chapter gives a workable definition of “international data protection soft law framework” for purposes of this work, and to enhance further discussions and studies on data protection.

Chapter 5 presents, as a result of the analysis of the findings in the previous chapters, the ideal features and characteristics of a data protection soft
law framework for the ASEAN. It will begin with the possible foundation of such a framework – an ASEAN Data Protection Agreement. It proceeds to present a potential data protection standard for the ASEAN data protection soft law framework and Agreement, in the form of a set of privacy principles. The chapter will then go on to discuss additional measures, features, and characteristics that could help ensure the effectiveness of the Agreement. These are classified in accordance with their relevance to the three types of government networks: information networks, harmonization networks, and enforcement networks.

Chapter 6 provides a summary and conclusion, and discusses the challenges that could be encountered in the implementation of an ASEAN data protection soft law.
For two noble Filipino men of the law:

Numeriano G. Tanopo, Jr.
1924 - 2015

and

Chief Justice Renato C. Corona
1948 – 2016
Towards a Data Protection Soft Law Framework for the ASEAN Region

Outline

1. Introduction

2. The ASEAN: The organization, its plans for economic integration and the promotion of data protection in the region, and soft law as a possible tool to address data protection concerns in Southeast Asia

2.1 Chapter abstract
2.2 The Association of Southeast Asian Nations (ASEAN)
   2.2.1 Brief history, composition, and background information
   2.2.2 The road to the ASEAN Charter and the ASEAN Economic Community
   2.2.3 The ASEAN Charter
   2.2.4 The ASEAN Economic Community (AEC) and the AEC Blueprint
   2.2.5 The Master Plan on ASEAN Connectivity and the Strategic Schedule for ASEAN Economic Community (and their brief mention of data protection)
   2.2.6 Taking ASEAN Economic Integration one step further: The ASEAN Economic Community Blueprint 2025
2.3 Consequences of ASEAN Economic Integration relevant to this dissertation
2.4 Data protection issues and controversies in Southeast Asia
2.5 The lack of a data protection soft law for the ASEAN Region: The status quo and the ASEAN’s plans
2.6 Soft law and ASEAN’s strong soft law tradition
   2.6.1 What is soft law?
   2.6.2 The “ASEAN way”: Consensus-building; eschewal of excessive institutionalization and enforceable commitments; non-confrontation
2.7 Chapter conclusion

3. What lessons could be learned from the use of soft law in the ASEAN region?

3.1. Chapter abstract
3.2. Review of significant implemented ASEAN soft law instruments and their results:
   3.2.1. Peace-keeping and geo-political stability
      3.2.1.1. ASEAN Convention on Counter Terrorism
      3.2.1.2. ASEAN-China Cooperative Operations in Response to Dangerous Drugs
   3.2.2. Economic Cooperation
      3.2.2.1. ASEAN Trade in Goods Agreement
      3.2.2.2. ASEAN Comprehensive Investment Agreement
3.2.2.3. ASEAN Framework Agreement on Services
3.2.3. Socio-cultural Cooperation
  3.2.3.1. ASEAN Agreement on Disaster Management and Emergency Response
  3.2.3.2. ASEAN Agreement on Transboundary Haze Pollution
3.2.4. Other harmonization, cooperation, and standard-setting efforts
  3.2.4.1. e-ASEAN Framework Agreement
  3.2.4.2. ASEAN Framework on Intellectual Property Cooperation
3.3. Lessons learned from the implementation of these ASEAN soft law instruments
  3.3.1 Types of measures that are likely to achieve ASEAN policy objectives
  3.3.2 Challenges to be expected when ASEAN resorts to the use of soft law instruments in order to achieve policy objectives
3.4. Chapter conclusion

4. International Data Protection Soft Law: What is it, and what are the lessons to be learned from its implementation by the APEC and OECD?

4.1 Chapter abstract
4.2 International Data Protection Soft Law
  4.2.1 What is International Data Protection Soft Law?
    4.2.1.1 Definitions
      4.2.1.1.1. Privacy and / versus Data Protection
      4.2.1.1.2 Data Protection Law
      4.2.1.1.3 Data Protection Soft Law Framework
    4.2.2 The emergence of International Data Protection Soft Law Frameworks
4.3 Examination of the use of Soft Law in International Data Protection: Lessons learned from the OECD Privacy Guidelines and the APEC Privacy Framework
  4.3.1 The OECD Privacy Guidelines and the APEC Privacy Framework
    4.3.1.1 The OECD Privacy Guidelines
    4.3.1.2 The APEC Privacy Framework
  4.3.2 What are the advantages and disadvantages of the following features and characteristics of the APEC Privacy Framework and the OECD Privacy Guidelines? What are the successes of and challenges involved in the implementation of these features and characteristics?
    4.3.2.1 National / domestic implementation strategies
      4.3.2.1.1 Review of domestic frameworks
      4.3.2.1.2 Establishing Data Protection Authorities / Privacy Enforcement Authorities / Privacy Commissions
      4.3.2.1.3 Promotion of legislative approaches
      4.3.2.1.4 Promotion of self-regulation
      4.3.2.1.5 Encouraging the establishment of privacy management programs
4.3.2.1 Professionalizing the privacy practice / instituting data protection and privacy law credential programs
4.3.2.1.7 Encouraging the deployment of privacy-enhancing technologies
4.3.2.1.8 Having Member States report on their domestic implementation of the framework’s recommendations

4.3.2.2 International implementation strategies
4.3.2.2.1 OECD’s Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy
4.3.2.2.1.1 APEC Cross Border Privacy Rules System and the APEC Cross Border Privacy Enforcement Arrangement
4.3.2.2.1.2 The advantages and successes of the APEC CBPR and CPEA System
4.3.2.2.2 The disadvantages and weaknesses of and challenges involved in implementing the APEC CBPR System

4.4 Chapter conclusion

5. The Ideal Features and Characteristics of an ASEAN Data Protection Soft Law Framework

5.1 Chapter Abstract
5.2 An ASEAN Data Protection Agreement
5.2.1 Matters of form
5.2.1.1 Clear and precise objectives and specific goals
5.2.1.2 Provides flexibility in the means to be used to attain the objectives and goals
5.2.1.3 Seeks compatibility and interoperability with existing data protection soft law frameworks
5.2.1.4 Comprehensive and consolidates related instruments
5.2.1.5 Specifies and provides different deadlines
5.2.1.6 Has Implementation Guides and Checklists
5.2.2 Matters of substance / Measures to Promote Data Protection in the ASEAN Region
5.2.2.1 Encourage the use of Privacy-Enhancing Technologies
5.2.2.2 Encourage the establishment of Privacy Management Programs and publication of Accountability Guides
5.2.2.3 Makes provisions for the professionalization of the privacy practice
5.2.2.4 Provides for a system of reporting and monitoring
5.2.2.5 Provides a venue for participation of various stakeholders
5.2.2.6 Regular meetings and reviews of the Agreement
5.3 An ASEAN data protection standard deemed adequate and robust enough by stakeholders
5.4 Information Network Features
   5.4.1 Establishing a network of Data Protection Authorities
   5.4.2 Providing technical assistance, training, and capacity-building for regulators, law enforcement, legislators, and judges

5.5 Undertaking a Hard Harmonization Project: Working through Harmonization Networks and Tools
   5.5.1 Having Data Protection Authorities Participate in Harmonization Efforts
   5.5.2 Begin with a review of domestic frameworks
   5.5.3 Facilitate the enactment of harmonized data protection laws through model laws
   5.5.4 Encourage the development of comprehensive legislation instead of sectoral laws
   5.5.5 An interim measure: voluntary model codes

5.6 Enforcement Network Features
   5.6.1 Independent Data Protection Authorities equipped with the necessary powers and functions to cooperate on cross-border matters
   5.6.2 Encouraging the development of a system of co-regulation
   5.6.3 Looking into jurisdictional matters over data protection offenses
   5.6.4 An improved Cross Border Privacy Rules System

5.7 Chapter conclusion

6. A summary, conclusion, and the challenges that could be encountered in the implementation of an ASEAN Data Protection Soft Law Framework
Acknowledgements

“Gratitude is the memory of the heart.”
- Massieu to the Abbé Sicard

My husband and dissertation-writing partner, Brady de Castro, for the endless support, precious companionship, and for making dreams come true;

My parents, Jose Vicente E. Jimenez and Milwida T. Jimenez, for 31 years (and counting) of tireless, open-hearted giving, inspiration, and guidance – for everything;

My parents-in-law, Arturo M. de Castro and Soledad Cagampang-de Castro, for the immense generosity, kindness, and encouragement – this degree is as much mine as it is yours;

Professor Paul M. Schwartz, who, by his dedication to teaching Privacy Law with so much gusto, gave a young lawyer from the Philippines direction in her career, and something in the law about which to be passionate;

My Tanopo-Jimenez family in San Juan, and Cagampang-de Castro family in Manila and California, for the support and encouragement;

Candy Drilon-Dalman, Moksy Gonzales, and JC Valenzuela, my dearest friends, and Br. Aikee Esmeli, FSC, Yanie Dizon, Monika Reunilla-Visenio, Marion Villegas-Watson, Tracy Cruz, Mico Geronimo, and Edrix Crisologo for being the best cheerleaders, despite the distance;

Professors John Yoo, Deirdre Mulligan, and Chris Hoofnagle, for the guidance, wisdom, and the time you dedicated to helping me write this dissertation;

Shylee and Ahmes Magsano, Belen Mandapat, their families, and the community of friends they helped build, for welcoming us into their supportive American Canyon tribe; and

All the dedicated teachers I had, from pre-school at the Children’s Talent Education Center Manila, Colegio San Agustin-Makati, De La Salle University-Manila, Ateneo Law School, and Berkeley Law, who took the time to teach me how to read, write, form sentences, compose paragraphs, construct chapters, intelligently argue and debate, interpret and appreciate the law, and create a dissertation.

My heartfelt thanks and gratitude to every single one of you.
**Introduction**

The Association of Southeast Asian Nations (ASEAN, or the Association) has embarked on an ambitious project, the creation of an ASEAN Community. This Community has three pillars: the ASEAN Economic Community (AEC), the Security Community (ASC) and the Socio-cultural Community (ASCC). This dissertation focuses on the AEC, which has, as its main goal, the integration of the economies of the ten ASEAN Member States.\(^2\)

The general steps to achieve this goal are laid out in the AEC Blueprint. Specific steps are laid out in various Master Plans, one of which is the Master Plan on ASEAN Connectivity. One Key Strategy in this Master Plan is to “[a]ccelerate the development of ICT infrastructure and services in each of the ASEAN Member States.” A Key Action under Strategy 6 is to promote information security and data protection.

In addition to the Master Plan, the e-commerce section of the Strategic Schedule for the AEC states that by 2015 (later adjusted to 2020), all ASEAN Member States must have legislation in line with regional best practices and regulations in e-commerce activities, including data protection. Significantly, the same Schedule expresses the ASEAN leadership’s objective of having a harmonized legal infrastructure for e-commerce, with an emphasis on data protection. These plans form part of ASEAN’s strategy for economic integration.

The plans for ASEAN economic integration are geared towards having a regional environment which operates as a single market and production base, that fosters the (i) free flow of goods; (ii) free flow of services; (iii) free flow of investment; (iv) freer flow of capital; and (v) free flow of skilled labor. It also intends to heighten the integration of financial institutions, increase cross-border investments, trade, and transactions, and encourage further information exchange. These plans and the ongoing proliferation of businesses that process personal data locally and engage in cross-border transfers of this type of data, lead to the need for a regional response to the risks commonly associated with international transfers of personal data. Data protection, as the Association expressed, must indeed be promoted.

However, with only three ASEAN Member States \(^3\) that have comprehensive national data protection laws, and no regional framework in place to promote data protection, now is an appropriate time and opportunity to seek possible solutions. A possible solution that will be evaluated by this dissertation is the development of a data protection soft law framework for the

---

\(^2\) Indonesia, Malaysia, Philippines, Singapore, Thailand, Brunei Darussalam, Viet Nam, Lao PDR, Myanmar, and Cambodia.

\(^3\) Malaysia, Singapore, and the Philippines.
ASEAN region. This framework is intended to encompass those legal structures that provide for broad, general rules that influence, in a non-binding and unenforceable manner, the ways in which personal data is processed, both within national borders, and when the data crosses those borders.

Since this dissertation is premised upon the development of a regional data protection soft law framework, the broad objectives of which are based on the following ASEAN goals: a) to promote data protection in the region by facilitating the creation of data protection legislation and regulations in line with regional best practices in all Member States; b) to harmonize data protection laws in the region; and c) to manage the challenges that will arise from the increase in cross-border data flows within the Southeast Asian region, the question now arises: what are the ideal features and characteristics of an ASEAN data protection soft law framework?

In order to answer this question, the following major inquiries must first be made:

a) What is a “data protection soft law framework” and why is it being considered as a way to promote data protection in the ASEAN?

b) What are the lessons to be learned from the use of soft law in the ASEAN region? More specifically, what types of measures, features, and characteristics are likely to help achieve policy goals, and what are the challenges to be expected when the Association resorts to the use of soft law instruments in order to achieve policy objectives?

c) What are the lessons to be learned from other international data protection soft law frameworks? More particularly, what are the advantages and disadvantages of certain features and characteristics of the APEC Privacy Framework and the OECD Privacy Guidelines? What are the successes and challenges involved in the implementation of these features and characteristics?

The answers to these questions will be distilled into a set of features and characteristics that are ideally suited to fulfill the purpose of an ASEAN data protection soft law framework.

Chapter 2 of this dissertation will first provide a background of the ASEAN, and then illustrate the progress of its plans for regional economic integration. It will explain why and how the need for a data protection soft law framework emerged. Chapter 2 will also explain why a soft law approach is being considered as a possible way to promote data protection in the region.

Chapter 3 will look at various ASEAN soft law instruments that were entered into by its Member States in order to achieve certain policy objectives. The objective of this chapter is to identify the lessons, both positive and
negative, that can be learned from ASEAN soft laws. The intended result are recommendations as to which soft law measures, features, and characteristics are ideal for an ASEAN data protection soft law framework, because they are more likely to achieve policy goals. It also aims to identify the likely challenges of using soft law to achieve certain policy objectives in the Southeast Asian region.

Chapter 4 has two main objectives: first is to give a workable definition of “international data protection soft law framework” for purposes of this work, and to enhance further discussions and studies on data protection; second is to draw lessons from two existing international data protection soft law frameworks: the OECD Privacy Guidelines and the APEC Privacy Framework. The product of the discussions in Chapter 4 will be a set of recommendations, this time, as to which data protection soft law framework features, characteristics, and measures could be adapted by the ASEAN when it decides to create its own framework for the Southeast Asian region. The inevitability of the emergence of such a framework for the region will also be explained.

The salient data protection soft law framework measures, features, and characteristics are briefly explained, and then their benefits discussed. The drawbacks, weaknesses, or the challenges involved in implementing each measure, characteristic, and feature are presented. This is followed by suggestions on how to address these drawbacks, weaknesses, or challenges.

Chapter 5 will be the result of the analyses conducted in Chapters 3 and 4. It will present the ideal features and characteristics of an ASEAN data protection soft law framework, based on the experience of the ASEAN with soft law instruments, and the experience of the OECD and APEC with their own data protection soft law frameworks. It will begin with the possible foundation of such a framework – an ASEAN Data Protection Agreement. After briefly explaining why the ASEAN will likely choose an Agreement for this purpose, it will go on to describe the ideal features of this Agreement, first as to its form, and second as to some of its possible contents or suggested measures to promote data protection in the region.

This chapter will also present a potential data protection standard for the ASEAN data protection soft law framework and Agreement, in the form of a set of privacy principles. Chapter 5 will then go on to discuss additional measures, features, and characteristics that could help ensure the effectiveness of the Agreement. These measures, features, and characteristics are classified in accordance with their relevance to the three types of government networks: information networks, harmonization networks, and enforcement networks.

This dissertation will end with Chapter 6, which will present the work’s summary and conclusions, and the possible challenges that could be encountered in the implementation of an ASEAN data protection soft law framework.
The overarching purpose of this dissertation is to help drive the discussion towards an ASEAN strategy for the promotion of data protection in the Southeast Asian region. Considering that the discussion on this matter is at a very nascent stage in the Association, it is hoped that this work will contribute to the body of knowledge that could assist the ASEAN leadership as they decide on various approaches that could be used to attain one of their stated policy goals.
1. The ASEAN: The Organization, its Plans for Economic Integration and the Promotion of Data Protection in the Region, and Soft Law as a Possible Tool to Address Data Protection Concerns in Southeast Asia

Chapter Two Outline:

2.1 Chapter Abstract

2.2 The Association of Southeast Asian Nations (ASEAN)
   2.2.1 Brief history, composition, and background information
   2.2.2 The road to the ASEAN Charter and the ASEAN Economic Community
   2.2.3 The ASEAN Charter
   2.2.4 The ASEAN Economic Community (AEC) and the AEC Blueprint
   2.2.5 The Master Plan on ASEAN Connectivity and the Strategic Schedule for ASEAN Economic Community (and their brief mention of data protection)
   2.2.6 Taking ASEAN Economic Integration one step further: The ASEAN Economic Community Blueprint 2025

2.3 Consequences of ASEAN Economic Integration relevant to this dissertation

2.4 Data protection issues and controversies in Southeast Asia

2.5 The lack of a data privacy soft law for the ASEAN Region: The status quo and the ASEAN’s plans

2.6 Soft law and ASEAN’s strong soft law tradition
   2.6.1 What is soft law?
   2.6.2 The “ASEAN way”: Consensus-building; eschewal of excessive institutionalization and enforceable commitments; non-confrontation

2.7 Chapter Conclusion

1.1. Chapter Abstract

The Association of Southeast Asian Nations (ASEAN, the Association, or the Organization) is an organization geared towards regional economic, social, and cultural cooperation, and the promotion of peace and stability within Southeast Asia. It has gone through an evolution of its functions, powers, and objectives, as can be seen in its various Conventions, Declarations, and Agreements. This evolution eventually led to its current major project: the creation of an ASEAN Community. One important element of this envisioned entity is the ASEAN Economic Community, one that will usher in the region’s economic integration.

To achieve ASEAN’s economic integration, the Organization’s leadership proposed numerous measures, which are outlined and described in Plans, Blueprints, and Strategic Schedules. One specific measure involves the promotion of information security and data protection. ASEAN also set, as a goal, the creation of a harmonized and comprehensive legal framework for data protection.
It is foreseen that ASEAN economic integration will inevitably lead to an increase in transborder data flows, due to an upswing in intra-regional transactions and information exchange. With an increase in transborder data flows come specific risks and challenges. Considering these facts and an impending deadline, only three ASEAN Member States have comprehensive data protection legislation, and as of this writing, concrete plans to achieve the Organization’s goal of a regional harmonized and comprehensive legal infrastructure for data protection are yet to be drawn up. For these reasons, this dissertation, due to ASEAN’s strong soft law tradition, will examine and evaluate soft law as a possible tool to promote data protection in the region and address the risks and challenges that will arise due to the expected increase in intra-regional transborder data flows resulting from ASEAN’s economic integration.

1.2. The Association of South East Asian Nations

1.2.1. Brief history, composition, and background information

The ASEAN was established on August 8, 1967 in Bangkok, Thailand, with the signing of the ASEAN Declaration (Bangkok Declaration) by the founding Member States of the ASEAN, namely Indonesia, Malaysia, Philippines, Singapore and Thailand. Brunei Darussalam joined in 1984, Viet Nam in 1995, Lao PDR and Myanmar both in July 1997, and Cambodia in 1999, completing what is today the 10 Member States of ASEAN.

The aims and purposes of the Association, as set out in the two-page ASEAN Declaration, are “cooperation in the economic, social, cultural, technical, educational and other fields, the promotion of regional peace and stability through abiding respect for justice and the rule of law, and adherence to the principles of the United Nations.”

In their interactions with one another, ASEAN Member States agreed upon the following fundamental principles, as contained in the Treaty of Amity and Cooperation in Southeast Asia of 1976:

1. Mutual respect for the independence, sovereignty, equality, territorial integrity, and national identity of all nations;
2. The right of every State to lead its national existence free from external interference, subversion or coercion;
3. Non-interference in the internal affairs of one another;

---

5 Id.
4. Settlement of differences or disputes by peaceful manner;
5. Renunciation of the threat or use of force; and
6. Effective cooperation among themselves.

These principles have come to be known as the “ASEAN way.”

1.2.2. The Road to the ASEAN Charter and the ASEAN Economic Community

In the years after the signing of the ASEAN Declaration, Southeast Asia succumbed to energy crises, rice shortages, increases in the prices of raw materials, and instability in global commodity markets. To cope, in 1976, ASEAN leaders entered into Bali Concord I, a declaration that called for mutual support and preferential trade agreements. Dictated by ongoing economic challenges in the Southeast Asian region, 1992 saw the establishment of the ASEAN Free Trade Area; 1995 the ASEAN Framework Agreement on Services, and in 1998, the ASEAN Investment Area. Efforts to foster regional integration in the hopes of strengthening the economy of the region eventually led to an ambitious plan – the ASEAN Community.

In December 1997, “ASEAN leaders adopted the ASEAN Vision 2020, a fundamental step for the long-term road map for ASEAN.” The plan sought to establish an ASEAN Community by 2020, made up of three pillars: an ASEAN Economic Community (AEC), an ASEAN Security Community (ASC) and an ASEAN Socio-cultural Community (ASCC). Each pillar has its own Blueprint, and, together with the Initiative for ASEAN Integration (IAI) Strategic Framework and IAI Work Plan Phase II (2009-2015), they form the Roadmap for an ASEAN Community 2009-2015.

Most relevant to this dissertation is the ASEAN Economic Community due to, among other things, the transborder data flows that would increase because of its implementation. This will be further discussed in later sections.

The ASEAN Economic Community is the realization of the goal of economic integration, and it seeks to establish ASEAN as a single market and production base by facilitating the free flow of goods, services, foreign direct investment, skilled labor, and a freer flow of capital. Bali Concord II, adopted in 2003, expressed the intention of the ASEAN leaders to realize the ASEAN Economic Community.

---

9 Id. at 21.
10 Id.
11 Id. at 24.
13 Id.
ASEAN leaders decided that a charter was needed to move ASEAN from an informal grouping to a more rules-based intergovernmental organization; they believed that by imposing rules, the development of the ASEAN Economic Community could be more easily achieved. Thus, the ASEAN Charter was drafted, and it entered into force on December 15, 2008.

1.2.3. The ASEAN Charter

The ASEAN Charter “serves as a firm foundation in achieving the ASEAN Community by providing legal status to, and an institutional framework for, ASEAN. It also codifies ASEAN norms, rules and values; sets clear targets for ASEAN; and presents accountability and compliance.” The ASEAN Charter built a new legal framework for the Association, and paved the way to the establishment of new organs to boost its community-building process. The Charter has become a legally binding agreement among the 10 ASEAN Member States – a notable feat, considering that the “ASEAN has always been regarded as a group of sovereign nations operating on the basis of ad hoc understandings and informal procedures rather than within the framework of binding agreements arrived at through formal processes.” Indeed, by entering into a legally binding document, the ASEAN leaders have signified their assent to an unprecedented body of obligations and enforceable commitments. It is worth mentioning, however, that the enforceability of obligations contained in the ASEAN Charter is subject to debate, and has yet to be tested.

The purposes of ASEAN are set out in Article 1 of the Charter. Article 1 remains faithful to the aims and purposes of the Association as set out in the ASEAN Declaration, with a few notable additions. Pertinent to this dissertation is Purpose 5, which makes mention of the objectives of economic integration in the ASEAN Charter:

5. To create a single market and production base which is stable, prosperous, highly competitive and economically integrated with effective facilitation for trade and investment in which there is free flow of goods, services and investment; facilitated movement of business persons, professionals, talents and labour; and freer flow of capital.

---

16 Id.
Article 5 significantly lays out the obligations of Member States to take all necessary measures, including the enactment of national legislation, to implement the provisions of the Charter.

Article 7 of the ASEAN Charter states that the ASEAN Summit, which consists of the heads of state of the ASEAN Member Nations, shall be the supreme policy- and decision-making body of the Association. The Summit is the ultimate arbiter on issues pertaining to the failure to reach a consensus and settlement of disputes between Member States.

Article 9 establishes ministerial-level councils to realize the objectives of the three pillars of the ASEAN Community - the Economic Community, the Security Community, and the Socio-cultural Community.

“An international organization’s legal personality affects its capacity under international law to enter into relations with other organizations or States and also their competence to conclude treaties.” Article 3 of the Charter addresses this concern, since it expressly confers legal personality on the ASEAN.

Article 20 reiterates the ASEAN way of decision-making through consultation and consensus; it, however, goes a step further by stating that the ASEAN Summit shall decide in situations wherein a consensus cannot be reached. More importantly, it authorizes the Summit to act in cases of serious breach of the Charter or non-compliance. However, the types of acts that the Summit could undertake to address serious breaches of the Charter or non-compliance have not been specified and agreed upon.

1.2.4. The ASEAN Economic Community (AEC) and the AEC Blueprint

Establishing a single market and production base is the goal of the ASEAN Economic Community. The general steps to achieve this goal are laid out in the ASEAN Economic Community Blueprint. According to the Blueprint, an ASEAN single market and production base has five core elements: (i) free flow of goods; (ii) free flow of services; (iii) free flow of investment; (iv) freer flow of capital; and (v) free flow of skilled labor. Other

---

9 Article 7(2)(e), ASEAN Charter.
21 Article 3, ASEAN Charter.
23 Article II (A)(9) AEC Blueprint.
areas of cooperation are also to be incorporated, such as human resources development and capacity building; recognition of professional qualifications; enhanced infrastructure and communications connectivity; development of electronic transactions; integrating industries across the region to promote regional sourcing; and enhancing private sector involvement for the building of the AEC. 24

Recognizing the importance of external trade to ASEAN and the need for the ASEAN Community to remain outward-looking, the AEC possesses the following key characteristics, in addition to having a single market and production base: a highly competitive economic region; a region of equitable economic development; and a region fully integrated into the global economy.

To foster a competitive economic region, ASEAN leaders identified several key areas of concern in the AEC Blueprint. Those relevant to this dissertation will be discussed. These are Consumer Protection, 25 Infrastructure Development, specifically Information Infrastructure, 26 and e-commerce. 27

The ASEAN leaders recognized that building an integrated economic region with a people-centered approach means that consumers cannot be precluded in all measures taken to achieve this integration. Hence, the AEC Blueprint mandates that consumer protection must be strengthened with the establishment of the ASEAN Coordinating Committee on Consumer Protection (ACCCP), and a network of consumer protection agencies to facilitate information sharing and exchange. 28 The Blueprint also prescribes the organization of regional training courses for consumer protection officials and consumer leaders in preparation for an integrated ASEAN market. 29

“A secure and connected information infrastructure is important for sustaining the region’s economic growth and competitiveness.” 30 More importantly, the AEC Blueprint gives emphasis to improving trust and confidence in the use of the Internet and security of electronic transactions, payments and settlements. 31 Hence, the Blueprint proposes measures to strengthen the region’s cyber-security network, and to deepen the regional policy and regulatory framework to deal with the opportunities and challenges in the area of Next Generation Networks. 32

24 Article II (A)(7) AEC Blueprint.
25 Article II (B)(2)(42) AEC Blueprint.
26 Article II (B)(4)(51) AEC Blueprint.
27 Article II (B)(5)(55) AEC Blueprint.
28 Article II (B)(2)(42) AEC Blueprint.
29 Article II (B)(2)(42) AEC Blueprint.
30 Article II (B)(4)(51) AEC Blueprint.
31 Article II (B)(4)(51) AEC Blueprint.
32 Article II (B)(4)(51) AEC Blueprint.
The Blueprint also seeks to lay the policy and legal infrastructure for electronic commerce within ASEAN through the implementation of the E-ASEAN Framework Agreement. A prescribed measure is to study and encourage the adoption of the best practices and guidelines of regulations and/or standards based on a common framework.  

Since the AEC Blueprint is a document that lays out very general, broad plans for the region’s economic integration, ASEAN leaders published detailed documents that lay out more specific plans to be implemented. These documents are considered instrumental in realizing the envisioned ASEAN Community. Among these documents are the Master Plan on ASEAN Connectivity and the Strategic Schedule for ASEAN Economic Community.

1.2.5. The Master Plan on ASEAN Connectivity and the Strategic Schedule for ASEAN Economic Community (and their brief mention of Data Protection)

Enhanced connectivity is essential to realize the goal of an ASEAN Community by 2015, because a well-connected ASEAN will contribute towards a more competitive and resilient region, as it will bring people, goods, services and capital closer together in accordance with the ASEAN Charter. The Master Plan on ASEAN Connectivity is a key step towards realizing this vision.

In 2010, ASEAN Leaders emphasized the need to identify specific measures, with clear targets and timelines, as well as the need to develop viable infrastructure financing mechanisms for the implementation of the Master Plan on ASEAN Connectivity. The Master Plan points out that "enhancing intra-regional connectivity within ASEAN and its sub-regional groupings would benefit all ASEAN Member States through enhanced trade, investment, tourism and development."

The reasons behind enhancing connectivity in ASEAN are manifold. Some of these are enhancing integration and cooperation; bolstering global competitiveness of ASEAN through stronger production networks; enhancing connections to economic centers both within the ASEAN region and within individual Member States; and narrowing the development gaps between the more economically prosperous ASEAN nations such as Singapore, and the developing countries, such as Cambodia, Laos, Myanmar, and Viet Nam, collectively known as the CLMV. However, the Master Plan, while recognizing

---

33 Article II (B)(B6)(59) AEC Blueprint.
34 Section 1, Master Plan on ASEAN Connectivity, accessed at http://www.asean.org/resources/publications/asean-publications/item/master-plan-on-asean-connectivity-2
35 Executive Summary, Section 1, Master Plan on ASEAN Connectivity.
36 Introduction, Section 2, Master Plan on ASEAN Connectivity.
37 Id.
the tangible benefits of closer connectivity, also anticipates that cross-border challenges should be addressed properly.\textsuperscript{38}

In order to address both the necessary steps to take in order to achieve closer connectivity within the Southeast Asian region and the cross-border challenges that could arise with greater connectivity, the Master Plan laid out seven Key Strategies to Enhance Physical Connectivity.\textsuperscript{39} The Key Strategy pertinent to this dissertation is Strategy 6, which is to “Accelerate the development of ICT infrastructure and services in each of the ASEAN Member States.” A Key Action under Strategy 6 is to promote information security and data protection.\textsuperscript{40}

In addition to the Master Plan, the E-commerce section in the Strategic Schedule for the AEC states that by 2015, all ASEAN Member States must have updated and/or amended legislation in line with regional best practices and regulations in E-commerce activities.\textsuperscript{41} All Member States must also adopt best practices and guidelines on other cyber-law issues (i.e. data privacy, consumer protection, IPR, ISP liability, etc.) to support the regional E-commerce activities.\textsuperscript{42} Moreover, the same Schedule expresses the ASEAN leadership’s desire to have a harmonized legal infrastructure for E-Commerce fully in place in ASEAN by 2015.\textsuperscript{43}

As of this writing, even if the implementation of the ASEAN Economic Community (AEC) Blueprint 2015 has had some success in “eliminating tariffs and facilitating trade; advancing the services trade liberalisation agenda; liberalising and facilitating investment; streamlining and harmonising capital market regulatory frameworks and platforms; facilitating skilled labour mobility; promoting the development of regional frameworks in competition policy, consumer protection and intellectual property rights; promoting connectivity; narrowing the development gap; and strengthening ASEAN’s relationship with its external parties,” a significant number of the goals set in the Schedule, including the E-commerce objectives, have not yet been achieved. For this reason, the Organization released, in November 2015, the ASEAN Economic Community Blueprint 2025.

\textsuperscript{38} Introduction, Section 9, Master Plan on ASEAN Connectivity.
\textsuperscript{39} Chapter 3.1, Master Plan on ASEAN Connectivity.
\textsuperscript{40} Chapter 3.1, Strategy 6 (iv), Master Plan on ASEAN Connectivity.
\textsuperscript{41} B.6. Strategic Schedule for ASEAN Economic Community, accessed at http://www.customs.go.th/wps/wcm/connect/807a2d74-19ba-4cc4-a058-e7dbcf6boddd/AEC+Strategic+Schd.pdf?MOD=AJPERS&CACHEID=807a2d74-19ba-4cc4-a058-e7dbcf6boddd4
\textsuperscript{42} B.6. Strategic Schedule for ASEAN Economic Community.
\textsuperscript{43} Id.
1.2.6. Taking ASEAN Economic Integration One Step Further: The ASEAN Economic Community Blueprint 2025

The ASEAN Economic Community Blueprint 2025 (AEC Blueprint 2025) builds on the AEC Blueprint 2015, and it consists of “five interrelated and mutually reinforcing characteristics, namely: (i) A Highly Integrated and Cohesive Economy; (ii) A Competitive, Innovative, and Dynamic ASEAN; (iii) Enhanced Connectivity and Sectoral Cooperation; (iv) A Resilient, Inclusive, People-Oriented, and People-Centred ASEAN; and (v) A Global ASEAN.”

This new Blueprint sets out concrete measures to be implemented in order to achieve these five goals. Pertinent to this dissertation, the AEC Blueprint 2025 aims to provide a new emphasis on the development and promotion of “digital technology as leverage to enhance trade and investments, provide an E-based business platform, and promote good governance.” Also relevant to this dissertation are the following objectives and proposed measures:

In line with its first reinforcing characteristic (A Highly Integrated and Cohesive Economy), one main objective of this new Blueprint is “to facilitate the seamless movement of goods, services, investment, capital, and skilled labour within ASEAN in order to enhance ASEAN’s trade and production networks, as well as to establish a more unified market for its firms and consumers.” Some key measures under this objective are minimizing compliance costs in dealing with regulations, i.e., “standards and conformance measures, e.g., equivalence in technical regulations, standards harmonisation, alignment with international standards and mutual recognition arrangements (MRAs).” Another measure includes strengthening financial integration “to facilitate intra-ASEAN trade and investment by increasing the role of ASEAN indigenous banks, having more integrated insurance markets, and having more connected capital markets.”

The second reinforcing characteristic of the AEC Blueprint 2025 (A Competitive, Innovative, and Dynamic ASEAN) has, as one of its goals, promoting consumer protection measures in products and services sectors such as finance, E-Commerce, air transport, energy, and telecommunications. Its third reinforcing characteristic (Enhanced connectivity and Sectoral cooperation), has, as a main objective, intensifying cooperation on E-Commerce, specifically developing an ASEAN Agreement on E-Commerce, to facilitate cross-border electronic transactions in ASEAN. More importantly,

---

45 ASEAN Economic Community Blueprint 2025 p. 3.
46 Id. at 4.
47 Id. at 7.
48 Id. at 14.
49 Id. at 24.
one goal under this objective is putting in place a “coherent and comprehensive framework for personal data protection.”

1.3. Consequences of ASEAN Economic Integration Relevant to This Dissertation

As previously mentioned, an ASEAN single market and production base shall comprise five core elements: (i) free flow of goods; (ii) free flow of services; (iii) free flow of investment; (iv) freer flow of capital; and (v) free flow of skilled labor. In addition, economic integration will see the increased integration of insurance markets and other financial institutions, a surge in cross-border investments, trade, and transactions, and an upswing in information exchange.

It is foreseeable that these will lead to an increase in transborder data flows, herein defined as “all cases of data crossing national borders,” within the Southeast Asian region. Indeed, the international transfer of personal data will result to “economic growth and efficiencies that have had a positive impact around the world, while at the same time subjecting the privacy of individuals to new and increased risks,” such as criminal attacks against users’ personal data conducted via the Internet and government access to and sharing of personal data.

With the increase in transborder data flows within the region, certain issues must be addressed. Christopher Kuner, in Transborder Data Flows and Data Privacy Law, pointed out some of the risks and challenges associated with transborder data flows:

*Society:* The protection of data as a societal value can be endangered if personal data are transferred for purposes that are illegal or against public policy, or if data transfers result in the national standard of data protection being weakened. The widespread processing and transfer of personal data for monitoring purposes can result in the creation of a ‘surveillance society.’

*Individuals:* The transfer of personal data across borders may adversely affect the exercise of individuals’ data protection rights by making it more difficult for them to bring claims and identify the responsible parties.

---

50 Id.
52 Id. at 2.
53 Id. at 4.
54 pp. 104-109.
Governments and public authorities: The ability of governments and public authorities to function effectively can be put at risk if data that they process (including data about their citizens) are accessed abroad by foreign governments and law enforcement authorities.

Companies: Companies can be harmed if data that they need to conduct business are not sufficiently protected, or if transfers of data to other countries cause individuals and business partners to lose trust in them.

In addition to these, the Article 29 Working Party identified the following as “categories of international data transfer that it regards as posing particular risks to privacy”55

- transfers involving sensitive data;
- transfers which carry the risk of financial loss (e.g., credit card payments over the Internet);
- transfers carrying a risk to personal safety;
- transfers leading to a decision that significantly affects the individual (e.g., recruitment or promotion decisions, the granting of credit, etc.);
- transfers which carry a risk of serious embarrassment or tarnishing of an individual's reputation;
- transfers which may result in specific actions which constitute a significant intrusion into an individual's private life, such as unsolicited telephone calls;
- repetitive transfers involving massive volumes of data (e.g., transactional data processed over telecommunications networks, the Internet); and
- transfers involving the collection of data in a particularly covert or clandestine manner (e.g., Internet cookies).

Furthermore, Kuner paraphrased the risks of transborder data flows reported by the State Services Commission of New Zealand as follows:

- non-compliance with national law;
- unauthorized release of personal information;
- inability to provide individuals with access to their personal information;
- inability to cooperate with national regulators regarding complaints;

• inability of the national regulator to investigate or enforce the law;
• inability to guarantee the protection of personal information in countries without privacy or data protection laws;
• conflicts between foreign laws and national law;
• possible access to data by foreign governments;
• overseas judicial decisions that might require the disclosure of data;
• problems with recovery or secure disposal of data;
• loss of trust if data are transferred and misused.

It is conceivable that ASEAN Member States, their citizens, and their resident companies and institutions will face these risks. This can be attributed to an increase in cross-border data flows that will result from the above-mentioned measures that will be undertaken to advance the objectives of ASEAN economic integration.

1.4. Data protection issues and controversies in Southeast Asia

The following are some examples of the data protection issues that Southeast Asia has had to contend with, thus far. For Singapore, an observation that has been made is that its data protection authority is not independent, and it does not cover the public sector. Its Minister may revoke any appointment to the Personal Data Protection Commission (PDPC) anytime, “without assigning any reason.”\(^\text{56}\) Should Singapore, in the future, expand the coverage of its data protection laws to cover the public sector, the PDPC’s independence will need to be reviewed.\(^\text{57}\)

In Malaysia, even though it is only one of three ASEAN Member States that has enacted a comprehensive data protection law, it has been shown that awareness about its Personal Data Protection Act (PDPA) among local companies is still relatively low, and that local companies may not be fully equipped to implement all the requirements set out in the law’s Standards.\(^\text{58}\)

The Philippines suffered one of the biggest recorded data breaches in April 2016. Leading up to the country’s May 2016 general elections, hackers were able to access, and subsequently leaked, the personal data of 55 million Filipino voters.\(^\text{59}\) This leak exposed complete names of voters, the names of their parents, birth dates, home addresses, election precinct numbers, email

\(^{56}\) Graham Greenleaf, Asian Data Privacy Laws, p. 309, citing the Personal Data Protection Act of Singapore, Section 49.

\(^{57}\) Id.

\(^{58}\) See Malaysia: Data users may not ‘be fully equipped’ to implement PDP Standards, accessed at http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=5676.

addresses, phone numbers, biometric data, particularly thumbprints, and for Filipinos registered to vote abroad, their passport numbers and foreign home addresses. As of this writing, the country’s newly-constituted National Privacy Commission is yet to offer a response.

Thailand’s data protection (DP) bill raised a concern among businesses, particularly that they are concerned that there is no separation and clear definition of “personal data processor” despite the wide definition of “data controller” under the DP bill. Under the DP bill, a third party that collects, uses, and discloses personal data on behalf of a data controller could share the same liability and duties as the controllers. Internet service providers, web hosting service providers, cloud service providers and content hosting platforms will be adversely affected as they could therefore be interpreted as data controllers under the DP bill. There are fears that this will not attract foreign investors into Thailand, because stringent legislation will hamper innovative technology businesses, rather than promote Thailand as a digital economic hub for the ASEAN Economic Community.

Viet Nam and Indonesia both have substantial data protection laws limited to their e-commerce sectors. If those Member States do not act to widen the scope of their data protection laws, it will leave data subjects, whose data are process by unregulated sectors, with very limited options for redress, in the event of a breach.

The constitution of Brunei Darussalam does not recognize any constitutional rights of citizens, let alone a right of privacy. It has a Computer Misuse Order that may provide some incidental data privacy protections; its Electronic Transactions Act and Consumer Protection Order both do not deal directly with data protection matters. Note, however, that “[t]he most likely influences towards Brunei enacting data privacy legislation are its ASEAN commitments...”

The economies of Cambodia, Lao, and Myanmar, are beginning to see greater growth and liberalization. This would lead to greater opportunities for businesses – businesses that would inevitably process personal data locally and transfer them beyond national borders. Despite this fact, there are no data protection laws in these countries, save for some incidental cybercrime, e-

---

60 Id.
62 Id.
63 Id.
64 Id.
66 Id. at 391.
67 Id.
68 Id.
commerce, and telecommunications provisions. The development of data protection laws in these countries is no longer a far-fetched likelihood in the medium term, thus the context in which such laws might develop requires consideration. As with Brunei, it is highly likely that any progress towards enacting data protection legislation will be prompted by ASEAN initiatives.

1.5. The lack of a data privacy soft law for the ASEAN Region: The status quo and the ASEAN’s plans

Considering the following:

(a) ASEAN has recognized that a necessary step that must be taken towards realizing the goal of an ASEAN Community is the promotion of information security and data protection;

(b) all ASEAN Member States must have, in accordance with the Strategic Schedule for the ASEAN Economic Community, data protection legislation and regulations in line with regional best practices;

(c) the same Strategic Schedule expressed the desire of the ASEAN leadership to have a harmonized legal infrastructure for e-commerce, which includes data protection law and regulations, for the Southeast Asian region;

(d) the ASEAN Economic Community Blueprint 2025 has identified, as a measure to enhance connectivity and sectoral cooperation, putting in place a coherent and comprehensive framework for personal data protection;

(e) the ASEAN Economic Community Blueprint 2025 has pointed out the necessity, among Member States, of equivalence in technical regulations, standards harmonization, and alignment with international standards;

(f) ASEAN’s economic integration will give rise to increased transborder data flows and the above-mentioned risks and challenges related to the latter; and

(g) the numerous and varied data protection issues that have come about, and will later emerge, in the region,

the following characterizes the status quo in the ASEAN:

(a) only three Member States, specifically Malaysia, the Philippines, and Singapore have enacted comprehensive data protection laws;

(b) there is no harmonized legal infrastructure for data protection in the region; and

69 Id. at 397.
(c) there is no mechanism through which alignment with international data protection standards could be achieved by all 10 Member States.

For these reasons, it is submitted that now is an opportune time to examine the prospect of having a data protection soft law framework for the ASEAN region. The purposes of this envisioned framework are the promotion of information security and data protection; the facilitation of the creation of data protection legislation and regulations in line with regional best practices in all Member States; the harmonization of data protection laws in the region; and the management of the challenges that will arise from the increase in transborder data flows within the Southeast Asian region.

This examination aims to expose the lessons, both positive and negative, from the use of soft law in the ASEAN region; and the successes and failures of the use of soft law in international data privacy law and governance. An exploration as to which institutions and instruments could implement a data protection soft law framework for the ASEAN region will also be undertaken. This investigation will lead to a presentation of the ideal features of a data protection soft law framework for the Southeast Asian region – the result of the analyses of the successes and failures of the use of soft law in the ASEAN region, and soft law in international data privacy law and governance. The possible promises and challenges for a data protection soft law framework specifically for the ASEAN region will also be illustrated.

Since soft law and soft law in the ASEAN context, specifically, are important concepts in this dissertation, the following sub-chapter delves into a discussion of both.

1.6. Soft law and ASEAN’s strong soft law tradition
1.6.1. What is soft law?

It is difficult to present a singular, authoritative definition of “soft law” because the term has been the subject of fierce debate among international law scholars. However, to this author, one definition in particular seems able to embrace the complexity of the interactions between actors and legal instruments in the international sphere. Kenneth Abbott and Duncan Snidal first define hard law as “legally binding obligations that are precise (or can be made precise through adjudication or the issuance of detailed regulations) and that delegate authority for interpreting and implementing the law.”\(^70\) Abbott and Snidal thus define legalization in international relations “as consisting of a spectrum of three factors: (i) precision of rules; (ii) obligation; and (iii) delegation to a third-party decision-maker.”\(^71\) For them, “soft law begins once


\(^{71}\) Gregory Shaffer and Mark Pollack, Chapter 4: How Hard and Soft Law Interact in International Regulatory Governance in Systemic Implications of Transatlantic Regulatory Cooperation and Competition p. 69 (2011).
legal arrangements are weakened along one or more of the dimensions of obligation, precision, and delegation."

Gregory Shaffer and Mark Pollack\(^2\) skillfully explain Abbott and Snidal’s concept in this manner:

Thus, if an agreement is not formally binding, it is soft along one dimension. Similarly, if an agreement is formally binding but its content is vague so that the agreement leaves almost complete discretion to the parties as to its implementation, then the agreement is soft along the second dimension. Finally, if an agreement does not delegate any authority to a third-party to monitor its implementation or to interpret and enforce it, then the agreement again can be soft because the parties can discursively justify their acts in legalistic terms with less consequence, whether in terms of reputational costs or other sanctions.

For purposes of this dissertation, Abbott and Snidal’s soft law typology and continuum is the most appropriate gauge through which an instrument could be classified as hard or soft law.

1.6.2. The “ASEAN Way”: Consensus-building; eschewal of excessive institutionalization and enforceable commitments; non-confrontation

The primary reason why soft law is being examined as a possible tool to promote data protection in the ASEAN region is due to the manner in which its Member States interact with each other. This manner of interaction is called the “ASEAN way.” This sub-chapter will explain the ASEAN way, which could be described as operationalized soft law.

The beliefs and norms associated with the ASEAN way may be best examined within a socio-historical context.\(^3\) In traditional terms, Southeast Asian politics is, to a large extent, personalistic, informal, and non-contractual.\(^4\) Even though formal political institutions exist in the ten Member States, most of the countries in Southeast Asia were (and still are) ruled by a small elite class, which operate through patronage networks.\(^5\) According to


\(^5\) Id.
Gillian Goh, in her work on the ASEAN Way, “[t]his had the effect of institutionalizing a highly private and informal political culture; thus, even today, a set of social etiquette exists which has its basis in indirectness and social harmony.”

This approach to intra-regional interaction among the Southeast Asian states involves “a high degree of discreetness, informality, pragmatism, expediency, consensus-building, and non-confrontational bargaining styles.” In addition to these, seeking agreement and harmony, sensitivity, politeness, agreeability, quiet, private diplomacy versus public shaming, and being non-legalistic are highly characteristic of the ASEAN way.

The stand-out features associated with the ASEAN way could be grouped together and categorized as follows: the preference for consensus-building; eschewal of excessive institutionalization and enforceable commitments; and sensitivity, avoidance, and being non-confrontational. A brief discussion of these features of the ASEAN way is presented below.

1.6.2.1. Consensus-building

The underlying approach to decision-making in ASEAN is embodied in the Malay terms musyawarah and mufakat (consultation and consensus), which relies largely on patient consensus-building to arrive at informal understandings or loose agreements. The concept involves intensive informal and discreet discussions behind the scenes, the results of which act as the starting point around which a decision is accepted in more formal meetings, rather than “across-the-table negotiations involving bargaining and give-and-take that result in deals enforceable in a court of law.”

Consensus-building involves a non-hostile atmosphere, characterized by the searching for “an amalgamation of the most acceptable views of each and every member" in a setting in which 'all parties have power over each other.' Also, consensus does not require unanimity; it represents a commitment to finding a “way of moving forward by establishing what seems

76 Id.
79 Paul Davidson, The ASEAN Way and the Role of Law in ASEAN Economic Cooperation, 8 S.Y.B.I.L. 166 2004.
80 Paul Davidson, The ASEAN Way and the Role of Law in ASEAN Economic Cooperation, 8 S.Y.B.I.L. 166 2004, citing Rodolfo C. Severino, The ASEAN Way and the Rule of Law, Address by Rodolfo C. Severino, Secretary-General of the Association of Southeast Asian Nations, at the International Law Conference on ASEAN Legal Systems and Regional Integration, 3 September 2001.
to have broad support."\(^{82}\) In the ASEAN, it has been said that when a consensus is achieved, “not everyone would always be comfortable, but they tend to go along so long as their basic interests were not disregarded."\(^{83}\)

Consensus-building was demonstrated in the way the ASEAN handled the Asian Financial Crisis of the late ’90’s.\(^{84}\) The crisis was largely due to the Southeast Asian countries’ “increasing dependence upon foreign capital and bank loans, owing to their relatively underdeveloped financial markets.”\(^{85}\) The dispute involved managing the risks associated with unencumbered financial flows and currency speculation, and balancing those risks with the interests of the economies dependent on those same foreign direct investments and financial flows.\(^{86}\) In particular, Malaysia’s need to be protected from the risks involved in unfettered financial flows and currency speculation had to be balanced with Singapore’s anxieties over financial flight and a downturn in foreign investment.\(^{87}\) In coming to a compromise, ASEAN reached consensus “on the need to enhance their own risk management abilities in order to prevent and resolve any future financial crises.”\(^{88}\) This was achieved “by strengthening regional financial cooperation, instead of depending merely upon support from international financial organizations, including the International Monetary Fund (IMF), and from advanced countries.”\(^{89}\)

To prevent and cope with financial crises in the region, the ASEAN sought and achieved visible results, which included the setting up of a regional emergency liquidity provision regime and fostering regional bond markets.\(^{90}\) A coordination of views and agreement among members based upon close cooperation since the 1960s contributed to the smooth promotion of financial cooperation projects in Southeast Asia. This is a prime example of consensus-building achieving desired, concrete results. Even today, several decades since its inception, ASEAN relies largely on patient consensus-building to arrive at informal understandings or loose agreements.\(^{91}\)

---


\(^{83}\) Id.


\(^{85}\) Jee-young Jung, Regional Financial Cooperation in Asia: challenges and path to development, accessed at http://www.bis.org/publ/bppdf/bispap42d.pdf.

\(^{86}\) Otto V. von Feigenblatt, Avoidance and Consensus Building in the ASEAN: The Path Towards a New ASEAN Way.

\(^{87}\) Id.

\(^{88}\) Jee-young Jung, Regional Financial Cooperation in Asia: challenges and path to development, accessed at http://www.bis.org/publ/bppdf/bispap42d.pdf.

\(^{89}\) Id.

\(^{90}\) Id.

\(^{91}\) Rodolfo C. Severino, The ASEAN Way and the Rule of Law, Address by Rodolfo C. Severino, Secretary-General of the Association of Southeast Asian Nations,
1.6.2.2. Eschewal of excessive institutionalization and enforceable commitments

Historical circumstances and culture can provide at least a partial explanation for ASEAN’s avoidance of legally binding and enforceable agreements.92

In the 1960s, Southeast Asia was plagued with conflicts. One conflict was between Indonesia and Malaysia: Indonesia was against the formation of the Federation of Malaya and the former British colonies in Southeast Asia, namely Singapore, British North Borneo (Sabah) and Sarawak, since the Indonesia saw this move as a neo-colonialist plot and a hurdle to the unification of the Malay archipelago.93 Other conflicts involved a territorial dispute over Borneo, between the Philippines and Malaysia; Singapore’s secession from Malaysia; the problem of secession in Mindanao in the southern Philippines; the military coup of 1962 in Burma; and most important of all, the war in Indochina (Vietnam, Laos, and Cambodia).94 In addition to all these was the Vietnam War; in fact, one motive for the formation of ASEAN was to counteract Communist expansion in the region.95 Considering the tense relations among the five original member countries, the initial objective of ASEAN was building trust among its Member States to repel the Communist threat and keep Southeast Asia free of considerable power rivalries.96

This history of animosity and suspiciousness towards each other, coupled with the desire of the first set of ASEAN leaders to see beyond those tensions in order to attain and maintain peace in the region partly explains the ASEAN way: “By not forcing its incredibly diverse and mutually suspicious members into legally binding standards, ASEAN has done the remarkable job of moving its members from animosity to the close cooperative relationship that they enjoy today.”97 In addition, the first ASEAN leaders believed that strict structures, laws, and treaties “would have prematurely imposed obligations upon members who were just beginning to relate to one another

at the International Law Conference on ASEAN Legal Systems and Regional Integration, 3 September 2001.

92 Rodolfo C. Severino, The ASEAN Way and the Rule of Law, Address by Rodolfo C. Severino, Secretary-General of the Association of Southeast Asian Nations, at the International Law Conference on ASEAN Legal Systems and Regional Integration, 3 September 2001.
95 Walter Woon, Dispute Settlement, the ASEAN Way.
96 Id.
97 Rodolfo C. Severino, The ASEAN Way and the Rule of Law, Address by Rodolfo C. Severino, Secretary-General of the Association of Southeast Asian Nations, at the International Law Conference on ASEAN Legal Systems and Regional Integration, 3 September 2001.
and learn to cooperate.”98 This mode of interaction involving informal efforts, striving for consensus, and relying on confidence-building and demonstrations of goodwill, instead of sanction-based enforcement of commitments is a large factor in the close cooperation and preservation of peace among the Association’s Member States.

Another reason for this aversion to enforceable agreements is due to the fact that at the time ASEAN was formed, the Founding Member States (Indonesia, Malaysia, the Philippines, Singapore, and Thailand) were hesitant to give the Association strong powers over the members, preferring to preserve a high level of individual sovereignty.99 This hesitation can be attributed to a shared history of being liberated colonies that “fought to win the right to express and develop [their] national identities.”100

Despite this avoidance of legally binding and enforceable agreements, ASEAN has had success in various endeavors, which can be categorized into three groups: peace-keeping and geo-political stability, economic cooperation, and socio-cultural cooperation. These would be discussed in an in-depth manner in Chapter Three.

1.6.2.3. Non-confrontation

One aspect of non-confrontation is the sensitive handling of disagreements, which is another feature of the ASEAN way.101 Even though ASEAN leaders debate and disagree on certain issues behind closed doors, they do not publicize these disagreements, especially when dealing with non-ASEAN entities.102 Moreover, as observed by Amitav Acharya, members of the Association go to great lengths “not to isolate or embarrass any individual ASEAN member in international fora. Even when an ASEAN member has advanced a position which is not acceptable to other members, the latter will refrain from acting in ways that may make the latter ‘lose face’ internationally.”103

---

99 Id. at 14.
103 Id.
Another facet of non-confrontation is avoidance, which refers to “conflict management procedures leading to the filtering out of certain kinds of disputes.”

This procedure can involve the immediate avoidance of a certain issue from discussion in ASEAN to other more subtle methods of avoidance such as the channeling of certain issues to powerless secondary committees and the subsequent delay and final ignorance of its findings. Among the benefits of avoidance are the maintenance of group cohesion and the projection of a unified front in the face of the external environment. Thus, avoidance has served the purpose of avoiding certain difficult internal conflicts such as those over territory and political persecution of opponents in favor of maintaining the unity of ASEAN and permitting the discussion of other issues while disagreeing on many important ones. This leads to improved communication between parties which may be in conflict over one issue while cooperating on many others. Cooperation on regional concerns such as terrorism and development can take place between members with serious disputes partly because of ASEAN’s avoidance defense mechanism.

Indeed, collaboration on matters affecting the Southeast Asian region such as terrorism and development can occur, even between and among Member States with serious disputes, partly because of ASEAN’s avoidance mechanism.

Being non-confrontational, or constructive engagement, “implies that states with differences and conflicts of interests are, nonetheless, committed to consultations and will follow agreed-upon norms and rules.” Since constructive engagement requires the meeting of previous adversaries or possible antagonists, informality makes consultations proceed with more ease. This non-legal approach “goes to the heart of the ASEAN process; the Association was founded with a Declaration of the principle of self-restraint that would guide relations among members.” This goes hand-in-hand with the Asian preference for a non-institutional method – one that also avoids

---

106 Id.
108 Id. at 122.
contentious issues and puts emphasis on social trust rather than the rule of law when negotiating.  

Taken together, these characteristics would reveal a manner of interaction that places an emphasis on ensuring that fellow Member States will not be publicly shamed even though it has broken a prevailing norm, and avoiding controversial issues so that less-contentious matters may proceed.

The ASEAN way of building consensus among Member States, avoiding excessive institutionalization and legally binding enforceable commitments, and non-confrontation is entrenched in the ASEAN Charter and other ASEAN instruments. ASEAN leaders, in drafting the Association’s Charter, rejected suggestions for sanctions in case of breaches of the Charter; the leadership likewise rejected the idea of establishing a mechanism to monitor compliance with ASEAN agreements. For these reasons, the Association has no compliance or enforcement mechanisms, and a failure to implement carries no sanctions.

Truly, the ASEAN way fits Abbott and Snidal’s previously-discussed definition of soft law. To reiterate, legalization in international relations consists of a spectrum of three factors: (i) precision of rules; (ii) obligation; and (iii) delegation to a third-party decision-maker. Soft law begins once legal arrangements are weakened along one or more of these factors. Shaffer and Pollack explain that if an agreement is not binding, or is vague so that the agreement leaves almost complete discretion to the parties as to its implementation, or an agreement does not delegate any authority to monitor its implementation or to interpret and enforce it, then the agreement is soft.

ASEAN instruments are soft because, at the very least, the Member States do not delegate a third-party institution that could enforce and demand compliance with them. In addition, as will be shown later, the provisions of its legal instruments or Agreements tend to be imprecise, so as to give the Member States great leeway in implementing them locally. Furthermore, Member States are not obliged to comply with ASEAN instruments in the strict sense of the word; indeed, ASEAN has no mechanism to compel compliance with its Agreements, and no authority to issue and enforce sanctions in the event of breach and non-compliance. ASEAN instruments then, are on the weak end of

110 Peter Malanczuk, Association of Southeast Asian Nations, Max Planck Encyclopedia of Public International Law.
Abbott and Snidal’s spectrum of factors that is used to determine whether a law is hard or soft.

However, despite, or perhaps because of, the softness of ASEAN’s various instruments, a significant number of them have achieved their stated policy goals. Nevertheless, some of these soft law instruments have failed to completely achieve their objectives. In order to see not only the effectiveness of, but also the challenges that ASEAN will likely face in resorting to soft law instruments to achieve policy objectives, the next chapter will review significant ASEAN soft law instruments, their implementation, and their outcomes.

1.7. Chapter Conclusion

ASEAN’s plans for economic integration include the promotion of information security and data protection. Specific measures proposed by the Association to promote information security and data protection include the implementation of up-to-date national data protection laws and regulations in all ten Member States, and working towards a harmonized and comprehensive data protection framework in the Southeast Asian region. It is envisioned that these data protection laws and regulations, and the harmonized regional framework, are aligned with international standards.

A crucial step in ASEAN’s efforts to promote the specific, component goal of data protection is considering the effects of its general, overarching goal of economic integration. The measures necessary to achieve economic integration, and being economically integrated, will lead to increased transborder data flows due to an increase in cross-border, intra-regional transactions and information exchange. An increase in transborder data flows will lead to various risks and challenges that need to be addressed. Hence, an important aspect of promoting data protection nationally, in the ten Member States, and regionally, in Southeast Asia, is addressing the risks and challenges associated with a surge in transborder data flows.

Due to ASEAN’s strong soft law tradition, it is timely to undertake an examination of soft law as a possible tool in promoting data protection, and in addressing the data protection risks and challenges that will be faced by the region, due to an increase in transborder data flows resulting from economic integration.
2. What lessons could be learned from the use of soft law in the ASEAN region?

Chapter Three Outline:

3.1. Chapter Abstract
3.2. Review of significant implemented ASEAN soft law instruments and their results
   3.2.1. Peace-keeping and geo-political stability
      3.2.1.1. ASEAN Convention on Counter Terrorism
      3.2.1.2. ASEAN-China Cooperative Operations in Response to Dangerous Drugs
   3.2.2. Economic Cooperation
      3.2.2.1. ASEAN Trade in Goods Agreement
      3.2.2.2. ASEAN Comprehensive Investment Agreement
      3.2.2.3. ASEAN Framework Agreement on Services
   3.2.3. Socio-cultural Cooperation
      3.2.3.1. ASEAN Agreement on Disaster Management and Emergency Response
      3.2.3.2. ASEAN Agreement on Transboundary Haze Pollution
   3.2.4. Other harmonization, cooperation, and standard-setting efforts
      3.2.4.1. e-ASEAN Framework Agreement
      3.2.4.2. ASEAN Framework on Intellectual Property Cooperation
3.3. Lessons learned from the implementation of these ASEAN soft law instruments
   3.3.1. Types of measures which are likely to achieve ASEAN policy objectives
   3.3.2. Challenges to be expected when ASEAN resorts to the use of soft law instruments in order to achieve policy objectives
3.4. Chapter Conclusion

2.1. Chapter Abstract

Considering that the main question being asked by this dissertation is “what are the ideal features and characteristics of an ASEAN data protection soft law?” it is useful to undertake a review of some of the significant pieces of ASEAN soft law. The objective of this chapter is to identify the lessons, both positive and negative, that can be learned from ASEAN soft laws - which are embodied in instruments such as Agreements, Conventions, and Declarations – and their implementation. In doing this, one can better formulate recommendations as to which soft law features and characteristics are ideal for an ASEAN data protection soft law, because they are more likely to achieve policy goals. At the same time, one may also point out the likely challenges of using soft law to achieve certain policy objectives in the Southeast Asian region.

ASEAN legal literature is rich with discussions, analyses, and critiques of the Association’s soft law instruments and their implementation. This chapter looks into these discussions by reviewing various ASEAN Agreements, Conventions, and Declarations, specifically: each instrument’s major objectives; the measures prescribed by these instruments to be enacted in order
to achieve its objectives; the positive outcomes of these measures; and the shortcomings of, or difficulties encountered in implementing, these instruments. The chapter then concludes with a discussion of the lessons that can be drawn from ASEAN’s soft law instruments and their implementation, particularly: first, which types of measures are likely to achieve various policy goals; and second, what challenges are to be expected when ASEAN seeks to achieve a policy goal by resorting to Agreements, Conventions, and Declarations.

2.2. Review of significant implemented ASEAN Agreements and their results

As discussed in the previous chapter, the goal of ASEAN to promote information security and data protection in the region involves ensuring that:

(a) all Member States have legislation in line with international best practices and regulations in e-commerce activities;\(^{114}\) (b) all Member States adopt best practices and guidelines in data protection to support regional e-commerce activities;\(^{115}\) (c) the region has a harmonized legal infrastructure for e-commerce;\(^{116}\) and (d) there is a “coherent and comprehensive framework for personal data protection”\(^{117}\) for Southeast Asia. In addition, considering the risks and challenges that will arise from increased transborder data flows due to ASEAN’s economic integration, another goal in promoting information security and data protection in the region is: (e) creating measures to address these risks and challenges.

Hence, in this chapter, the focus will be on major ASEAN Agreements, Conventions, or Declarations that have led to the following: (a) Member States enacting national legislation to carry out the stated objectives of an Agreement, Convention, or Declaration; (b) Member States taking active steps, such as promulgating rules and regulations, to adopt best practices and guidelines in order to advance an objective of an Agreement, Convention, or Declaration; (c) a harmonized legal infrastructure or framework covering a specific area of concern that was put in place in the Southeast Asian region; or (d) implementation of concrete measures in order to address risks and challenges affecting the region.

The ASEAN Agreements, Conventions, and Declarations that will be covered by this chapter will be discussed under four headings: Peace-keeping and geopolitical stability; Economic cooperation; Socio-cultural cooperation; and Other harmonization, cooperation, and standard-setting efforts.

\(^{114}\) B.6. Strategic Schedule for ASEAN Economic Community, accessed at http://www.customs.go.th/wps/wcm/connect/807a2d74-19ba-4cc4-a058-e7dbcf6b0dd4/AEC+Strategic+Schd.pdf?MOD=AJPERES&CACHEID=807a2d74-19ba-4cc4-a058-e7dbcf6b0dd4

\(^{115}\) Id.

\(^{116}\) Id.

\(^{117}\) ASEAN Economic Community Blueprint 2025 p. 24.
2.2.1. Peace-keeping and geo-political stability

2.2.1.1. The ASEAN Convention on Counter Terrorism

All ten Member States ratified the ASEAN Convention on Counter Terrorism\(^\text{118}\) (ACCT) in 2013. Its objective is to serve as a framework for regional cooperation to counter, prevent, and suppress terrorism within the region, and to deepen cooperation among law enforcement agencies and relevant authorities of the Member States in countering terrorism.\(^\text{119}\) This convention led to the creation of a regional body responsible for overseeing collective responses to transnational crime, the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) and its operational arm, the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC), tasked to develop the necessary programs to implement it.\(^\text{120}\)

Concrete steps were set out in the ACCT, most of which were law-enforcement measures designed to strengthen regional capacity to deal with terrorism.\(^\text{121}\) These involved regional cooperation in eight areas of combating transnational crime: terrorism, illicit drug trafficking, trafficking in persons, money laundering, sea piracy, arms smuggling, international economic crime and cyber crime. The result was the establishment of a network among the Member States’ front-line law enforcement agencies in combating terrorism and enhancing intelligence exchange.\(^\text{122}\) Trainings in psychological operation and warfare for law enforcement officials, intelligence-gathering, bomb detection, post-blast investigation, airport security and travel document security, immigration matters, and cross-border controls were undertaken in all Member States because of the implementation of the provisions of the ACCT.\(^\text{123}\)

ASEAN sought to integrate the ACCT with other international conventions on terrorism.\(^\text{124}\) Hence, Article II of the ACCT defined “terrorist offense” to include any of the offenses within the scope of and as defined in any of the listed fourteen counter-terrorism treaties.\(^\text{125}\) In addition to wanting to

\(^{118}\) Available at http://agreement.asean.org/search/by_pillar/1/2.html.
\(^{119}\) Article 1, ASEAN Convention on Counter Terrorism.
\(^{120}\) Tatik S. Hafidz, A Long Row to Hoe: A Critical Assessment of ASEAN Cooperation on Counter-Terrorism, Kyoto Review of Southeast Asia Issue 11 (December 2009).
\(^{121}\) Id.
\(^{123}\) Id.
\(^{125}\) ASEAN Convention on Counter Terrorism: Article II Criminal Acts of Terrorism

For the purposes of this Convention, ‘offence’ means any of the offences within the scope of and as defined in any of the treaties listed as follows:
integrate the ACCT with other relevant international instruments, Abdul Razak Ahmad pointed out that “ASEAN’s lack of experience in legislating terrorism-related laws forced it to integrate existing treaties on counter-terrorism into its own Convention.” This incorporation of provisions from other international treaties serves two purposes: first is to consolidate terrorism-related laws and ensure that it is comprehensive; second is to comply with other international initiatives.

Such a move would not only complement the other international initiatives but would help create a parallel regime in combating terrorism. ASEAN’s move in adopting such an approach is also strategic because each treaty refers to one particular type of crime. The move would help criminalise a specific action without having to define or label it as an act of terrorism. Defining terrorism is never easy and in most circumstances, it

b. Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, concluded at Montreal on 23 September 1971;
e. Convention on the Physical Protection of Nuclear Material, adopted in Vienna on 26 October 1979;
h. Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on 10 March 1988;
l. Amendment to the Convention on the Physical Protection of Nuclear Material, done at Vienna on 8 July 2005;
m. Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, done at London on 14 October 2005; and

127 Id. citing Abdul Razak Ahmad’s interview with Senior Officials, Malaysian Attorney Generals Chamber (Putrajaya, 22 December 2010).
would not be possible to cover the extensive spectrum of terrorist crimes. In this way, the approach used by ACCT 2007 in terms of definition would help ensure that the wide range of terrorist crimes would be adequately covered by the Convention.\footnote{Abdul Razak Ahmad, The ASEAN Convention on Counter Terrorism 2007, 14 Asia-Pac J. on Hum. Rts. & L. 104-105 (2013).}

However, despite this broad definition of terrorism in the ACCT, there is a variance in the definition of terrorism among the national counter-terrorism laws of the ASEAN Member States.

The ACCT also provides that the party in whose territory, in which the offender or alleged offender is present, shall take the appropriate measures under its domestic laws to prosecute or extradite such a person.\footnote{ACCT Article VIII (3).} This prosecution or extradition is to be pursued once the Member State in whose territory the offender or alleged offender is present is satisfied with the outcome of an investigation, conducted based on the information provided and shared by another Member State.\footnote{ACCT Article VIII (2).} In all cases, any person who is taken into custody or regarding whom any other measures are taken or proceedings are carried out pursuant to the ACCT shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the laws of the Member State in the territory of which that person is present and applicable provisions of international law, including international human rights law.\footnote{ACCT Article VIII (1).}

The ACCT further provides that the Party in the territory of which the alleged offender is present shall, in cases of terrorist offenses, if it does not extradite that person, be obliged, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case without undue delay to its competent authorities for the purpose of prosecution; those authorities shall take their decision in the same manner as in the case of any other offense of a grave nature under the domestic laws of that Party.\footnote{ACCT Article XIII (1).} In addition, the ACCT states that when a Party which makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it has no extradition treaty, the requested Party may, consider the ACCT as a legal basis for extradition in respect of the offences covered in Article II of the Convention.

An important question arises in light of the provisions of the ACCT on extradition and prosecution: What if a party refuses to extradite a suspected terrorist? This issue was not addressed in the ACCT and, without an enforceable treaty obligation mandating extradition, or without an institution that has the authority to enforce the provisions of the ACCT, these provisions are, at best, recommendatory.
There is, however, an enforceable treaty specifically dealing with prosecuting crimes. The ASEAN Treaty on Mutual Assistance in Criminal Matters states that Parties are to render to one another the widest possible measure of mutual legal assistance in criminal matters, namely investigations, prosecutions and resulting proceedings.\(^\text{133}\) The assistance contemplated covers evidentiary matters, service of judicial documents, searches and seizures, production of documents, identifying and tracing instrumentalities of a crime, freezing, recovery, forfeiture or confiscation of property, and location and identification of witnesses and suspects.\(^\text{134}\) This Treaty specifically excludes matters of extradition and transfer of proceedings.\(^\text{135}\)

Another issue to consider in reviewing the ACCT is that given the potential human rights abuses that could occur because of the counter-terrorism measures in the ACCT, and possible legal proceedings challenging these measures, the Convention itself does not provide a mechanism for the resolution of such disputes.\(^\text{136}\) “It must be borne in mind that the region is composed of diverse legal systems and legal traditions in addition to the vast difference in the level of civic development. Human rights standards also vary a great deal from one Member State to another.”\(^\text{137}\) Indeed, a region-wide mechanism to address human rights violations is currently inexistent among ASEAN Member States. Although there is an ASEAN Inter-Governmental Commission on Human Rights, its mandate is very limited, and it does not have accessible enforcement mechanisms.\(^\text{138}\)

It has also been observed that the ACCT “is predictably silent on the issue of state-sponsored terrorism.”\(^\text{139}\) Indeed, there are no provisions in the ACCT that contemplate a scenario wherein the Member State itself is the offending party. Due to ASEAN’s adherence to the principle of non-interference, it is unsurprising that the framers of the ACCT did not intend to address this controversial aspect of terrorism.\(^\text{140}\)

### 2.2.1.2. ASEAN-China Cooperative Operations in Response to Dangerous Drugs (ACCORD)

ASEAN has endeavored to address the narcotics problem in the region by 2015. This led to the **ASEAN-China Cooperative Operations in Response to Dangerous Drugs (ACCORD)**. ACCORD has led to the reduction of the

---


\(^{134}\) Article I (2), Treaty on Mutual Assistance in Criminal Matters.

\(^{135}\) Article II (1), Treaty on Mutual Assistance in Criminal Matters.


\(^{137}\) Id.

\(^{138}\) Id.

\(^{139}\) Id. at 104.

\(^{140}\) Id.
production of natural drugs such as opium and cannabis, especially in the Golden Triangle area (an area bordering Myanmar, Laos, and Thailand), as well as synthetic drugs such as amphetamine-type stimulants and ecstasy. The poppy cultivation area in the region reduced by 85%, from 157,900 hectares in 1998 to 24,160 hectares in 2007. Since its inception, law enforcement units from China, the Philippines, Malaysia, Indonesia, Thailand, Singapore, and Myanmar have collectively investigated and prosecuted high-profile drug cases through a cooperative mechanism. These efforts have also led to the discovery of large transborder drug rings from within the ASEAN, and extending outwards to Canada, Japan, and the United States. Training to enhance the capacity of enforcement personnel in dealing with various aspects of drug production and trafficking have been held in collaboration with China and Australia.

ACCORD, however, is not without its shortcomings. It calls for detailed plans, formal law enforcement arrangements, review procedures, and verification standards, but provisions for these have yet to be enacted. In addition, the high turnover of law enforcement officers trained for specific tasks and locations leads to a loss of skills and knowledge, and with them goes the capacity-building investment.

Another challenge is that there are wide differences in the operational capacity of enforcement agencies. In some cases, drug authorities are well-funded and staffed, while the same is not true for their counterparts in neighboring Member States. These disparities are critical because it is unlikely that regional drug control efforts will be effective if not all concerned law enforcement units across the region, and their capacity to perform their responsibilities, are up to standard. To illustrate, if the capacities of border patrols on one side of a border do not match with those on the other side of the same border, intelligence and information gathering will be detrimentally affected, due to incomplete data coming from the side with fewer resources. “This results in a net loss to cross-border efforts since both units of investigators overlook important pieces of information.”

---

142 Zou Keyuan, China-ASEAN Relations and International Law, p. 163.
143 Id.
144 Id. at 69.
145 Sheng Lijun, China-ASEAN Cooperation against Illicit Drugs from the Golden Triangle, 30 (2) ASIAN PERSPECTIVE, pp. 97-126, 118 (2006).
147 Id. at 70.
148 Id.
Furthermore, relevant domestic laws and expectations for law enforcement are incompatible between and among countries party to ACCORD, and these lead to other difficulties.\footnote{Id. at 69.} For example:

Some countries in the region have asset forfeiture legislation while others do not and this complicates cross border cooperation in terms of prosecuting criminals;

Mutual Legal Assistance agreements have been signed by all ASEAN Governments but national regulations are not harmonized to allow for effective legal cooperation actions such as extradition and controlled deliveries; and

Forensic requirements are not the same for enforcement authorities – in some countries drug authorities are required to determine seized drug profiles while in other countries this action is only done on an ad-hoc basis. This challenges the ability of correct identification of substances which is an important aspect of drug investigations.\footnote{Id.}

2.2.1.3. The ASEAN Declaration Against Trafficking in Persons Particularly Women and Children and the ASEAN Convention Against Trafficking in Persons, Especially Women and Children.

In the ASEAN Declaration Against Trafficking in Persons Particularly Women and Children, ASEAN leaders committed to undertake concerted efforts to effectively address trafficking in persons, particularly women and children, by establishing a regional network to prevent and combat trafficking in persons in the ASEAN region; adopting measures to protect the integrity of travel and identity documents; sharing information on migratory flows, strengthening border controls, and enacting necessary national legislation; ensuring victims are treated humanely and provided with assistance, including prompt repatriation to their respective countries of origin; undertaking coercive measures against trafficking and offering the widest possible assistance to fellow Member States to punish such activities; and strengthening regional and international cooperation to prevent and combat trafficking in persons.\footnote{ASEAN Declaration Against Trafficking in Persons Particularly Women and Children, accessed at http://www.asean.org/communities/asean-political-security-community/item/asean-declaration-against-trafficking-in-persons-particularly-women-and-children-3} This Declaration led to formal bilateral commitments aimed at ensuring cross-
border law enforcement cooperation and the protection and support of victims when returned to their home countries.\textsuperscript{154}

One challenge is the variance in the level of response among the Member States. Some countries have very advanced measures to combat trafficking, while others are lagging behind.\textsuperscript{155} Despite such differences, a commissioned research shows that all Member States are working towards the broad objectives they have agreed to with their ASEAN neighbors.\textsuperscript{156} A major step forward is the introduction of relevant national policies, laws, and law enforcement initiatives that combat trafficking in all Member States.\textsuperscript{157} “However, in most countries in the region, there are still major deficiencies in existing laws. Legislation in most countries does not fully comply with current international standards, as set out in the UN Trafficking Protocol.”\textsuperscript{158} Another hurdle is the lack of training and awareness among prosecutors and judges.\textsuperscript{159} To address this, several ASEAN countries have engaged prosecutors and judges in training on trafficking issues.\textsuperscript{160}

A development of note is the establishment of specialist trafficking units in several ASEAN countries. Nine Member States have fully functional specialist trafficking units, and their heads meet every three months to share information regarding cases, and coordinate their work.\textsuperscript{161} These units have also developed and adopted standard operating procedures to facilitate information-sharing on specific cases, and participate in training programs.\textsuperscript{162} A commissioned study\textsuperscript{163} laid out the advantages to having specialist units:

- Specialist teams secure better results in identifying and prosecuting traffickers. This sends out a message to potential traffickers that they will be caught. It also signals to victims that there are people who can and will help them.

- Specialist units can work to reduce or prevent the corruption that is often associated with trafficking. By making specialist units exclusively responsible for handing trafficking cases, it is easier to monitor the response, and to secure that investigations are being conducted lawfully and ethically.

\textsuperscript{154} Human Trafficking: Exploring the International Nature, Concerns, and Complexities, edited by John Winterdyk, Benjamin Perrin, Philip Reichel
\textsuperscript{p. 242.}
\textsuperscript{156} Id.
\textsuperscript{157} Id.
\textsuperscript{158} Id. at 7.
\textsuperscript{159} Id. at 9.
\textsuperscript{160} Id.
\textsuperscript{161} Id. at 8.
\textsuperscript{162} Id.
\textsuperscript{163} Id. at 9.
• Provided that specialist units are properly set up, investigators in the units quickly become skilled in investigating a number of complex crimes: rape, assault, organised crime, financial investigations, and international liaison. This creates a pool of multi-skilled officials who can eventually be deployed across the wider police force.

• By responding to trafficking through specialist units, a clear picture begins to emerge more quickly about the scale and nature of the problem. This allows law enforcement to develop appropriate responses.

An ASEAN report outlined the key elements of a strong and comprehensive legal framework for combatting human trafficking, which include the full and effective criminalization of trafficking in persons and of related offences. This is recognized as the central element of a strong and comprehensive legal framework, providing the basis for efforts aimed at ending impunity for offenders. ASEAN Practitioner Guidelines make it explicit that: “All forms of trafficking in persons and related crimes should be specifically criminalised in accordance with applicable international standards”

The report states that effective criminalization can be achieved through the passing of a special anti-trafficking law or amendment to existing laws, most typically in Member States’ Penal Codes. “When amending their laws, States are not necessarily obliged to reproduce the fairly complex international legal definition as set out in the UN Trafficking Protocol and elsewhere. However, certain core features of the international definition would need to be included to satisfy the obligation of criminalisation.”

In addition, a strong legal framework will go beyond the crime of trafficking to ensure that trafficking-related offenses are also separately and fully criminalized. “A strong legal framework will also provide for penalties that take account of and are proportionate to the gravity of the offense.” Ensuring that there is access to remedies was also identified as a key element in an effective legal framework for combatting human trafficking.

Another element is that the legal framework should establish the widest possible jurisdiction over trafficking and trafficking related crimes. The objective is to “reduce or eliminate safe havens for traffickers by ensuring that

---

165 Id.
166 Id.
167 Id. at 8.
168 Id.
all parts of the crime can be punished wherever they took place.” The report explains:

The reduction or elimination of safe havens for traffickers and their assets further requires legislative support for mutual legal assistance, a formal process that enables investigative and judicial cooperation across borders to identify, locate, seize and transfer suspects, evidence and even proceeds of crime. Extradition powers in relation to trafficking and trafficking-related crimes should be specifically included in the national legal framework and within the terms of extradition treaties to which States are party.

Despite the progress made, anti-trafficking efforts in the Southeast Asian region “are being held back by a lack of relevant, reliable data on trafficking.” Recognizing this problem, in 2005, ASEAN member countries commissioned the International Organization for Migration to conduct a research project to identify best practices in data collection on trafficking, and to prepare a report on data collection by government agencies in four ASEAN member countries (Cambodia, Indonesia, the Philippines and Thailand). The project discusses lessons learned from the country studies, and suggests practical solutions that are potentially relevant to all ASEAN member countries wanting to improve their data on trafficking. It also presents recommendations that can be adopted at the agency level, at the national level, and also at the ASEAN level.

November 2015 saw the signing of the ASEAN Convention Against Trafficking in Persons, Especially Women and Children. Its objectives are to prevent and combat trafficking in persons, and to ensure effective punishment; protect victims, and promote cooperation among the Parties signatory to the convention to meet its objectives. The Convention, as opposed to the Declaration, provides specific steps to be undertaken by the Parties in furtherance of the goal of combatting human trafficking. Although its effects are yet to be seen, a review of the Convention can shed light on the types of provisions to which ASEAN Member States are willing to agree, when the subject pertains to offenses of a cross-border nature.

---

169 Id. at 9.
170 Id.
172 Id.
173 Id.
174 Id.
175 http://www.asean.org/images/2015/November/actip/ACTIP.PDF
176 Article 1 (1), ASEAN Convention Against Trafficking in Persons, Especially Women and Children.
Each Party is expected to adopt legislative measures necessary to establish the criminal conduct set forth in the Convention as criminal offences in their countries. This Convention also settled jurisdictional matters. For instance, each Party shall establish jurisdiction if an offense covered by the Convention is committed within its territory, or when an offense is committed by or against a national of that party.\textsuperscript{177}

Cross-border cooperation must be undertaken by the Parties to prevent and detect trafficking; the measures specified by the Convention include maintaining direct lines of communication; intelligence and information exchange; the development and use of databases; effective border controls; and the controlled issuance of travel documents.\textsuperscript{178} Bilateral and multilateral arrangements between and among Member States to prevent and combat trafficking are also proposed by the Convention.\textsuperscript{179}

The Convention provides for Law Enforcement measures as well. These include skill- and knowledge-building for law enforcement authorities; detection, determent, and punishment of trafficking-related corruption and money-laundering; ensuring that the legal systems of each Member State is equipped to handle trafficking cases; adopting measures to facilitate coordination of the policies and actions of government agencies; and providing training for relevant officials to aid them in preventing, investigating, and prosecuting trafficking.\textsuperscript{180} The same Convention also expects Parties to enable the confiscation and seizure of the proceeds of the offense, and the property, equipment, and other instrumentalities used to commit the offense.\textsuperscript{181}

This Convention mandates that the Parties should afford one another the widest measure of mutual legal assistance in criminal investigations or proceedings.\textsuperscript{182} Another remarkable feature of this Convention are its provisions on extradition. This Convention establishes the offenses specified as trafficking offenses to be extraditable offenses, if there is an extradition treaty between concerned Parties.\textsuperscript{183} In addition, if a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it has no extradition treaty, the Convention may be considered as the basis for extradition.\textsuperscript{184}

As for law enforcement cooperation, the Convention provides that Parties are to cooperate with each other in conducting inquiries with respect to

\textsuperscript{177} Article 10 (1) and (2), ASEAN Convention Against Trafficking in Persons, Especially Women and Children.
\textsuperscript{178} Id. Article 13.
\textsuperscript{179} Id. Article 12(b).
\textsuperscript{180} Id. Article 16.
\textsuperscript{181} Id. Article 17.
\textsuperscript{182} Id. Article 18.
\textsuperscript{183} Id. Article 19(i).
\textsuperscript{184} Id. Article 19(2).
the identity, whereabouts, and activities of suspected offenders, and providing items for evidentiary purposes.\textsuperscript{185}

Notably, the Convention has a monitoring mechanism, which states that the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) shall be responsible for promoting, monitoring, reviewing, and reporting to the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) on the effective implementation of this Convention.\textsuperscript{186} The ASEAN Secretariat shall provide support for supervising and coordinating the implementation of the Convention.\textsuperscript{187}

2.2.2. Economic Cooperation

2.2.2.1. ASEAN Trade in Goods Agreement

The objective of the \textit{ASEAN Trade in Goods Agreement} (ATIGA) is the free flow of goods in ASEAN in order to help establish a single market and production base for the deeper economic integration of the region.\textsuperscript{188} A single market for goods will enable the development of production networks within Southeast Asia and enhance the region’s ability to serve as a global production center.\textsuperscript{189} Some of the significant features of this Agreement are:

\textit{Comprehensive coverage}: this single Agreement covers various trade-related rules and regulations, including tariff liberalization, non-tariff barrier liberalization, rules of origin, trade facilitation, customs procedures, standards and conformance, and Sanitary and Phytosanitary (SPS) measures.\textsuperscript{190}

\textit{Consolidated and streamlined rights and obligations}: “to have an agreement that is more user-friendly for traders, the ATIGA consolidates all of ASEAN’s existing initiatives, obligations and commitments made with regard to intra-ASEAN trade-in-goods into one comprehensive document.”\textsuperscript{191}

\textit{Set deadlines}: the ATIGA provides for specific measures to achieve its goal of free flow of goods within ASEAN. Some of these measures are reduction or elimination of import duties on all products traded between Member States;\textsuperscript{192} elimination of tariff rate quotas on the importation of any goods originating in other Member States or on the exportation of any goods destined for the territory of the other Member States;\textsuperscript{193} and elimination of other non-
Each of these measures has a set deadline, mutually agreed upon by all Member States, which encourages swift compliance.

_Provision for the issuance of legal enactments:_ Each Member State shall, after the entry into force of the ATIGA, issue a legal enactment in accordance with its laws and regulations to give effect to the implementation of the tariff liberalization schedules committed under Article 19. The “ASEAN-6” countries (the more economically-prosperous states) composed of Brunei Darussalam, Indonesia, Malaysia, the Philippines, Singapore, and Thailand, have a deadline of 90 days from the date the ATIGA entered into force to comply with this requirement, while the “CLMV” bloc, (the less economically prosperous and historically conflict-ravaged, neighbors) composed of Cambodia, Laos, Myanmar, and Viet Nam, were given 6 months to comply.

_Tools for implementation and a review mechanism:_ A comprehensive work program, a framework, and a guidebook on ASEAN trade facilitation will be developed as integral parts of the ATIGA. The ATIGA implementation would be reviewed after its first year, and thereafter every two years.

_Trade repository and complaint-filing:_ To enhance transparency, the ATIGA called for the creation of the ASEAN Trade Repository, an online database of trade and customs legislation and procedures. This repository contains trade and customs laws and procedures of all Member States, and is accessible through the Internet. The ASEAN Trade Repository website also contains a notable feature – the ASEAN Solutions for Investments, Services and Trade (ASSIST), which is a “non-binding and consultative mechanism for the expedited and effective solution of operational problems encountered by ASEAN-based enterprises on cross-border issues related to the implementation of ASEAN economic agreements.” It is designed to be an internet-based and business-friendly facility for receiving, processing, and responding to complaints submitted by ASEAN enterprises. Through this system, an ASEAN-based enterprise may submit a complaint on the ASSIST website; the Central Administrator (the ASEAN Secretariat) reviews the complaint and forwards it to a national focal point, who reviews the complaint and may accept or reject it; if the complaint is accepted, the responsible government agency in that country will search for a solution; and the ASEAN-based enterprise may accept the proposed solution or reject it and seek other dispute resolution avenues.

---

194 Id. Art. 42.
195 Id. Art. 21 (1) (a).
196 Id. Art. 95.
197 Life After the Charter, ASEAN Studies Centre, Institute of Southeast Asian Studies, p. 14
198 See www.atr.asean.org
Dispute settlement: The Agreement explicitly states that the ASEAN Protocol on Enhanced Dispute Settlement Mechanism shall apply in relation to any dispute arising from, or any difference between Member States concerning the interpretation or application of this Agreement.\textsuperscript{201}

Institutional arrangements: Under the ATIGA, the ASEAN Economic Ministers (AEM) shall establish an ASEAN Free Trade Area (AFTA) Council composed of one ministerial-level nominee from each Member State and the Secretary-General of ASEAN. The AFTA Council shall also be supported by the Senior Economic Officials’ Meeting (SEOM). In the fulfillment of its functions, the SEOM may establish bodies to assist them, such as the Coordinating Committee on the implementation of ATIGA (CCA). The SEOM, assisted by the CCA, shall ensure the effective implementation of this Agreement.\textsuperscript{202}

Because of the implementation of the measures in ATIGA, Brunei, Indonesia, Malaysia, Philippines, Singapore, and Thailand have eliminated intra-ASEAN import duties on 99.65 percent of their tariff lines; Cambodia, Lao PDR, Myanmar, and Viet Nam have reduced their import duties to 0-5 percent on 98.86 percent of their tariff lines.\textsuperscript{203} The effect of the trade measures in ATIGA, according to the World Bank, is that “trade costs in ASEAN have dropped by as much as 15\% over the past decade. ... ASEAN trade costs are now comparable to those in NAFTA. The World Bank further suggests that the reduction in trade costs has contributed to the increase in ASEAN’s trade.”\textsuperscript{204} At present, efforts are geared towards addressing non-tariff measures that could have non-tariff barrier effects on the region’s trade and business activities.\textsuperscript{205}

Although the ASEAN, through ATIGA, has done well on tariff elimination, and credibly on trade facilitation,\textsuperscript{206} the Agreement is not without weaknesses. It has been observed that “[i]n the negotiation of this agreement, no prior public consultations were made. Public consultations, characterized by lack of transparency, were conducted only after the negotiation has been

\textsuperscript{201} ASEAN Trade in Goods Agreement, Art. 89.
\textsuperscript{202} Id. Art. 90.
concluded." Another difficulty encountered by the ASEAN leadership in implementing the ATIGA is “a public relations problem that has arisen not from the nature of free trade but from the way ASEAN member states have packaged it. Citizens feel disenfranchised and overlooked by the AEC.” There is, indeed, a rising backlash of nationalism against liberalization under the ASEAN’s free trade efforts, and a possible solution is effective communication of ASEAN’s plans of facilitating the freer flow of goods in the region with stakeholders, and actively building popular support for its economic plans.

Another area needing improvement is implementation. ATIGA devotes a chapter to trade facilitation, reflecting features such as the “single window” (single submission and synchronous processing of all information required for border clearance), risk management and authorized economic operators or trusted traders, advanced rulings, and post-entry audit. “While implementation of each of these varies from state to state, ASEAN rules are clear and the working groups provide support.” ASEAN would benefit from active monitoring of implementation, and it has been suggested that an independent policy implementation center be established for this purpose. A way for businesses to assess implementation of ATIGA’s provisions would aid them in decision-making.

2.2.2.2. ASEAN Comprehensive Investment Agreement

The objective of the ASEAN Comprehensive Investment Agreement (ACIA) is to create a free and open investment regime in ASEAN in order to achieve the goal of economic integration through the progressive liberalization of the investment regimes of the Member States; provision of enhanced protection to investors and their investments; improvement of transparency and predictability of investment rules, regulations, and procedures conducive to investment; the joint promotion of the region as an integrated investment area; and cooperation to create favorable conditions for investment by investors of a Member State in the territory of the other Member States.

The ACIA prescribes a set of benefits to be granted to investors, and these include: National treatment – all ASEAN investors are given treatment

---

208 Daniel Wu, Malaysia’s ASEAN Chairmanship Priorities All In Order, East Asia Forum, accessed at http://www.eastasiaforum.org/2015/02/12/malaysias-asean-chairmanship-priorities-all-in-order/.
209 Id.
211 Id.
212 Life After the Charter, ASEAN Studies Centre, Institute of Southeast Asian Studies, p. 18
213 ASEAN Comprehensive Investment Agreement, Art. 1.
equal to that afforded to domestic investors; *Most-favored nation treatment*—preferential treatment granted by any ASEAN member under any existing or future agreement must be extended to all other members; *Performance requirements*—investors shall not be required to meet export performance requirements; *Senior management*—ASEAN members cannot mandate that senior management must be made up of any particular nationality; *Movement of persons*—key personnel must be allowed entry and presence by the ASEAN member government; and *Dispute resolution*—the ACIA establishes the right of states and private investors to invoke dispute resolution.\(^\text{214}\)

Some of the advantages provided by the ACIA are: having a single investment agreement that clearly demonstrates the interaction of its provisions; it grants immediate benefits to ASEAN and ASEAN-based foreign investors due to its shorter deadline of 2015, as opposed to the *ASEAN Investment Area* (AIA) which provided for a deadline of 2020; and clear and transparent procedures for obtaining specific approval in writing, and comprehensive and clearer definitions in line with international investment agreements, both of which were absent in previous ASEAN Agreements, such as the AIA and the *ASEAN Investment Guarantee Agreement* (IGA). Indeed, these benefits boost investors’ confidence to invest in Southeast Asia.

However, one of the main challenges is with regard to the implementation of the ACIA itself:

One must understand that the process of harmonization does not end with the completion of the texts as the same has to be incorporated into the domestic laws. The ACIA contains provisions which may be expensive to implement and administer and for some Member States may require the enactment of new legislations and regulations or revision of existing ones which will create substantial burden to these Member States, particularly for those countries whose practice differs significantly from international standards.\(^\text{215}\)

It has been concluded that the effective implementation of the ACIA will largely depend on ASEAN Member States’ willingness and commitment to pursue structural and regulatory reforms in line with the ACIA provisions.\(^\text{216}\) In addition, regulatory reforms that further simplify procedures, licensing, and

\(^\text{216}\) Id.
other regulatory requirements would result in a more favorable investment environment.\(^{217}\)

### 2.2.2.3. ASEAN Framework Agreement on Services

The objectives of the Member States under the *ASEAN Framework Agreement on Services* (AFAS) are to enhance cooperation in services among Member States in order to improve production capacity and distribution of services within and outside ASEAN; to eliminate restrictions to trade in services among Member States; and to liberalize trade in services with the aim of realizing a free trade area in services.\(^{218}\)

The measures prescribed in the AFAS to achieve these goals include establishing or improving infrastructural facilities; joint production, marketing and purchasing arrangements; research and development; and exchange of information.\(^{219}\) Loftier goals consist of liberalizing trade in services in a substantial number of sectors within a reasonable time-frame by eliminating substantially all existing discriminatory measures and market access limitations amongst Member States, and prohibiting new or more discriminatory measures and market access limitations.\(^{220}\) Mutual recognition of work requirements, licenses, or certifications granted in one Member State, for the purpose of licensing or certification of service suppliers in another, which can be accomplished through Mutual Recognition Arrangements, is another suggested measure in the AFAS.\(^{221}\)

The difficulties encountered by ASEAN with regard to AFAS “relate both to the process itself and as well as ensuring compliance and implementation.”\(^{222}\) With regard to the process, it has been observed that establishing AFAS as a series of negotiating rounds resulted in delays and implementation on an incremental basis.\(^{223}\) It has been suggested that it may have been better to have a single undertaking, which would have resulted in a consolidated result on an ASEAN-wide basis.\(^{224}\) As for the challenges with respect to compliance and implementation, these could be attributed to the limited effect of monitoring and sanctioning.\(^{225}\) Stronger monitoring and

---

\(^{217}\) Id.

\(^{218}\) Id. Art. 2 (2).

\(^{219}\) Id. Art. 3.

\(^{220}\) Id. Art. 5.

\(^{221}\) Id. Art. 5.

\(^{222}\) Stefano Inama and Edmund W. Sim, *The Foundation of the ASEAN Economic Community*, p. 30 (2015).

\(^{223}\) Id. at 127.

\(^{224}\) Id.

\(^{225}\) Id. at 128.
sanctioning mechanisms were the recommended solutions to ensure that the measures prescribed by the AFAS could be implemented.  

2.2.3. Socio-cultural Cooperation

2.2.3.1. ASEAN Agreement on Disaster Management and Emergency Response

The goal of the ASEAN Agreement on Disaster Management and Emergency Response (AADMER) is to “provide effective mechanisms to achieve substantial reduction of disaster losses in lives and in the social, economic and environmental assets of the Parties, and to jointly respond to disaster emergencies through concerted national efforts and intensified regional and international co-operation.” It is a regional framework for cooperation, coordination, technical assistance, and resource mobilization in all aspects of disaster management.

Its implementation is laid out in the two-phase AADMER Work Programme, and the ASEAN Committee on Disaster Management (ACDM) is the driving force behind the Agreement’s implementation. Phase 1 was kicked-started by the establishment of the ASEAN Coordinating Centre for Humanitarian Assistance on disaster management (AHA Centre), which has, as its governing board, the ACDM. The ASEAN Secretariat provides policy and strategic coordination support, and assists in the monitoring and evaluation of the Work Programme. The ACDM reports directly to the ASEAN ministers in charge of disaster management, who also serve as “Conference of the Parties” (COP). COP provides the overall oversight and policy guidance.

The AADMER places emphasis on the involvement of all stakeholders including local communities, non-governmental organizations and private enterprises in addressing disaster risks. In addition, the Agreement requires each member-country to cooperate in developing and implementing measures to reduce disaster losses. This entails identification of disaster risks, monitoring, assessment and putting in place early warning systems, standby arrangements for disaster relief and emergency response, exchange of

---

226 Id.
230 Id.
231 Id.
232 Id.
233 Id.
234 Article 3(6), ASEAN Agreement on Disaster Management and Emergency Response.
235 Article 4(a), ASEAN Agreement on Disaster Management and Emergency Response.
information and technology, and the provision of mutual assistance.\textsuperscript{236} Under the AADMER, Member-countries are expected to take legislative, administrative, and other measures necessary to implement their obligations under the Agreement.\textsuperscript{237}

The AADMER has led to concrete results, including the establishment of a trained, fully-functional ASEAN Emergency Rapid Assessment Team, a third of whom have been deployed to exercises and actual disasters; a Standard Operating Procedure for Joint Disaster Relief and Emergency Response Operations involving civil-military coordination which has been tested and validated in exercises and actual disasters; and a real-time disaster monitoring and decision support system which has been tested and used in exercises and real disasters.\textsuperscript{238} Moreover, the AADMER helped ensure that all ASEAN Member States have national disaster management legislation.

However, challenges and gaps remain. Some of these include the significant time and resources needed to facilitate cross-sectoral coordination; strengthening the institutional capacity of national disaster management organizations; multiple, possibly overlapping mechanisms and institutions within the ASEAN concerned with humanitarian disaster management which lack coordination; and funding gaps.\textsuperscript{239}

\subsection*{2.2.3.2. Agreement on Transboundary Haze Pollution}

The objective of the Agreement on Transboundary Haze Pollution is to “prevent and monitor transboundary haze pollution as a result of land and/or forest fires which should be mitigated, through concerted national efforts and intensified regional and international co-operation.” All 10 Member States have ratified this Agreement. The Agreement requires the Parties to the Agreement to:

(i) cooperate in developing and implementing measures to prevent, monitor, and mitigate transboundary haze pollution by controlling sources of land and/or forest fires, development of monitoring, assessment and early warning systems, exchange of information and technology, and the provision of mutual assistance;

(ii) respond promptly to a request for relevant information sought by a State or States that are or may be affected by such transboundary haze pollution, with a view to

\textsuperscript{236} Article 4(a), ASEAN Agreement on Disaster Management and Emergency Response.\textsuperscript{237} Id. Article 4(d).\textsuperscript{238} ASEAN Agreement on Disaster Management and Emergency Response Phase 1 Accomplishment Report, accessed at http://www.ahacentre.org/download-file/default-file_admeer-iREmV3Qpofnwe4g4.pdf.\textsuperscript{239} Id.
minimising the consequence of the transboundary haze pollution; and

(iii) take legal, administrative and/or other measures to implement their obligations under the Agreement.240

“The Agreement establishes an ASEAN Coordinating Centre for Transboundary Haze Pollution Control to facilitate cooperation and coordination in managing the impact of land and forest fires in particular haze pollution arising from such fires.”241

The motivation behind this Agreement was a series of environmental crises in the region involving dangerous levels of haze resulting from the deliberate use of fire to clear forests and land. Indonesia is the largest source of the haze, which spreads to neighboring Malaysia, Singapore, Brunei and Thailand.242

The Agreement’s minimal achievements involve the sharing of resources to help combat the haze. Singapore has consistently offered assistance packages to Indonesia to help fight the fires - in August 2005, Indonesia accepted Singapore’s offer of high-resolution satellite pictures, one C130 aircraft for cloud seeding operations, and a contingent of fire fighters.243 The Ministerial Steering Committee (MSC) on Transboundary Haze Pollution comprising Brunei, Indonesia, Malaysia, Singapore and Thailand “agreed to explore the sharing of digital geo-reference concession maps and leverage on satellite and mapping technologies to enhance hotspot monitoring.”244

However, this Agreement has been subject to heavy criticism due to its failure to curb the worsening problem of transboundary haze originating from Indonesian forest fires. One observed weakness is the Agreement’s failure to contain specific prescriptions on preventive measures.245 Another deficiency is the lack of a strong dispute resolution mechanism and a provision for compensation for victim states or their citizens for losses incurred due to the haze.246 In addition, there is no provision for a minimum level of monitoring competence and procedures.247 Although state parties are mandated to regularly communicate data on fires and haze to the ASEAN Center, “this

---

240 Article 4, ASEAN Agreement on Transboundary Haze Pollution.
241 http://haze.asean.org/asean-agreement-on-transboundary-haze-pollution/
244 Id.
246 Id. at 664.
247 Id. at 666.
reporting requirement is limited in its effect because the ASEAN Center is not bound to do anything more beyond analyzing the received data and providing to state parties an assessment of the risks to human health and the environment. It has been suggested that there should be a procedure for the ASEAN Center to prescribe remedial measures to be immediately undertaken by state parties, and that the Center be given the authority to require additional information should the initial data be deemed inadequate.

On the national level - specifically in Indonesia, the major source of the haze - the challenges that contribute to the worsening haze problem could be traced to several factors. One is that “the institutions which existed for environmental and natural resource governance were fractured and weak.” Indeed, there existed two separate agencies tasked with environmental management efforts. In addition, inter-agency cooperation was minimal, and each agency seemed to be operating independently of the others. This lack of cooperation and confusion as to each agency’s role accounted for much of Indonesia's failure to deal with the fires of the late 90’s.

Another challenge, in addition to institutional overlap, was the confusing state of laws and regulations issued by the different agencies. “The difficulty resided in the fact that the legislative and executive bodies at both central and regional levels typically issued legal instruments at their own discretion, creating webs of often contradictory laws and regulations.”

2.2.4. Other harmonization, cooperation, and standard-setting efforts

2.2.4.1. e-ASEAN Framework Agreement

The objectives of the e-ASEAN Framework Agreement are to promote cooperation to develop and strengthen the competitiveness of the ICT sector in ASEAN; to promote cooperation to reduce the digital divide within the region; and promote the liberalization of trade in ICT products, ICT services and investments to support the e-ASEAN initiative. To achieve this, the Agreement states that Member States shall adopt electronic commerce regulatory and legislative frameworks that create trust and confidence for consumers and facilitate the transformation of businesses towards the

---

248 Id.
249 Id. at 666-667.
250 Id.
251 Id. at 672.
252 Id.
253 Id.
254 Id. at 675.
255 Id. citing Krystof Obidzinski & Christopher Barr, The Effects of Decentralization on Forests and Forest Industries in Berau District, East Kalimantan 13-14 (Ctr. for Int'l Forestry Research, Case Study No. 9, 2003)
development of e-ASEAN.\textsuperscript{257} To this end, Member States shall put in place national laws and policies relating to electronic commerce transactions based on international norms; facilitate the establishment of mutual recognition of digital signature frameworks; facilitate secure regional electronic transactions; and adopt measures to protect intellectual property rights arising from e-commerce; and encourage the use of alternative dispute resolution mechanisms for online transactions.\textsuperscript{258}

To help achieve these goals, the ASEAN-Australia Development Cooperation Program (AADCP) Harmonization of E-Commerce Legal Infrastructure in ASEAN Project was undertaken “to assist in the implementation of modern, best-practice and compatible laws - enabling ASEAN Member Countries to obtain the maximum benefit from the growth of e-commerce, both individually and as a region.”\textsuperscript{259} This project had three phases:

The focus of Phase 1 was the harmonization of e-commerce legal infrastructure. This phase was conducted between 2004 and 2005, and included the establishment of a broad, high-level harmonized legal, regulatory and institutional infrastructure for e-commerce. Phase 2, which was conducted in 2006, examined the potential establishment of a harmonized legal, regulatory and institutional infrastructure for electronic contracting and online dispute resolution (ODR). Phase 3, which was conducted in 2007, examined the possible establishment of a harmonized legal, regulatory and institutional infrastructure for the mutual recognition of digital signatures, so as to facilitate cross-border trade.\textsuperscript{260}

Each phase built on the accomplishments of previous phases, and the result of each phase became more meticulous and technical in nature as the project progressed.\textsuperscript{261}

Harmonization projects such as these are “designed to align individual country laws to remove unwanted gaps, overlaps and duplication.”\textsuperscript{262} Furthermore, e-commerce harmonization projects have, as a goal, the increase in legal certainty for parties that transact with more than one member country

\textsuperscript{257} Article 5, e-ASEAN Framework Agreement.
\textsuperscript{258} Id.
\textsuperscript{261} Id.
\textsuperscript{262} Harmonisation of E-Commerce Legal Infrastructure in ASEAN.
– for instance, multinational enterprises that are attempting to expand their business in a new region.263

There are two categories of harmonization projects – soft harmonization (based on training and capacity-building) and hard harmonization (based on model or uniform laws).264 “Most e-commerce legal harmonization projects are soft harmonization projects, in that there is no intention or requirement for countries to adopt the same (or even model) laws and regulatory systems.”265 The project merely involves training and capacity development activities, with the goal of ensuring a common (or harmonized) understanding of e-commerce legal requirements.266

ASEAN chose to pursue hard harmonization for its project dedicated to creating a regional e-commerce legal framework, which is based on implementation guidelines rather than simple capacity-building.267 Under this hard harmonization option, e-Commerce Project Guidelines were developed that build on the common objectives and principles for an e-commerce legal infrastructure.268 The guidelines include more prescriptive information on implementation steps, and a timeline.269 They were developed by an Australian private consulting firm, in collaboration with project participants and technical experts from ASEAN member countries.270

As a result of these efforts, ASEAN became the first region in the developing world to adopt a harmonized e-commerce legal framework consistent across jurisdictions.271 This project assisted Member States in implementing consistent e-commerce laws and meeting ASEAN implementation deadlines.272 The success of the project can also be seen in the improvement of the coverage of e-commerce enabling laws in the region: in 2004, only 4 Member States had enabling e-commerce laws – this number rose to 8 in 2008, and Laos was the last country to pass an e-commerce law.273 Cambodia now has a draft e-commerce law.274

264 Id.
265 Id.
266 Id.
267 Id.
268 Id.
269 Id.
270 Id.
271 Harmonisation of E-Commerce Legal Infrastructure in ASEAN.
272 Id.
273 Id.
The project’s most important achievements include:

i. Significant progress in regional understanding, drafting and reviewing domestic e-commerce laws to achieve harmonization;

ii. Increased activity in the region developing legal and technical policy;

iii. Development of a regional community of experts,

iv. Fostering and mentoring key individuals in the regional community of experts ... ; and

v. Encouragement of intra-ASEAN networking, information and informal technical support.\textsuperscript{275}

In addition, the project ensured that international best practices were adopted in the drafting of the harmonized e-commerce laws. “E-commerce infrastructure, given its globalized nature, must conform to international standards and practices. The project has ensured that all harmonization activities have involved major research of international initiatives, and that, wherever possible, international model laws and standards are implemented.”\textsuperscript{276} Implementation Checklists were also created for each phase of the project to support ongoing monitoring of implementation progress.\textsuperscript{277}

A commissioned study made several recommendations as to how the objectives of the e-ASEAN Framework Agreement can be further achieved. These include:

a. Establishing a regional dispute resolution facility to handle various types of online disputes, particularly consumer-related.\textsuperscript{278} This would build confidence in online transactions, and relieve pressure on the existing court system.\textsuperscript{279}

b. Monitoring harmonization of e-commerce laws in ASEAN member countries, since formal, regular reporting “would help to bring up-to-date information to the attention of all stakeholders, and could help to motivate member countries to meet the targets.”\textsuperscript{280} It was suggested that the ASEAN be tasked to handle the coordination

\textsuperscript{275} Harmonisation of E-Commerce Legal Infrastructure in ASEAN.
\textsuperscript{276} Id.
\textsuperscript{277} Id.
\textsuperscript{279} Id.
\textsuperscript{280} Id.
intended to harmonize regional and national legal frameworks. To this end, focal points in each country will gather the relevant data for information sharing.  

c. Workshops and training programs for law and policy makers to facilitate capacity-building. 

d. Relying on the UNCTAD for the following: Advisory services for the preparation of national e-commerce laws; on-site regional and national training courses or briefings; and documenting and disseminating proven best practices amongst networks of partners.

Several key challenges to e-commerce legal harmonization were identified in the surveys used in the commissioned study. Some of the main challenges are:

a. **Differences in legal approach:** Omnibus laws have been developed in certain ASEAN countries, while other Member States chose to have specific laws, which makes it difficult for companies to identify and compare legal requirements across the ASEAN countries.

b. **Absence of independent, well-resourced regulators:** Various areas of law require the attention of a specific, focused regulator, and this is absent in some ASEAN Member States. The commissioned study concluded, “[a] regulator with adequate funding and secondary rule-making powers is especially important in the new technology field, characterized by rapid changes. A well-resourced, flexible regulator can usually address emerging issues through developing guidelines or using test cases – and this process is much faster than waiting for parliament to update legislation.”

c. **Lack of skills and training:** “Some member countries face a lack of skills and training, especially in drafting, interpreting and enforcing laws.” Moreover, staff turnover is a factor to be considered, which further necessitates additional training.

d. **Limited funding:** This difficulty was particularly pronounced in the case of the CLMV countries. Funding is generally required from the initial scoping and policy formulation stage right through to implementation and follow-up work. Appropriate resources will

---

281 Id. 
282 Id. 
283 Id. 
285 Id. 
286 Id. 
287 Id. 
288 Id. 
289 Id.
need to be allocated by member country Governments to implement e-commerce legal infrastructure.”

Some Member States indicated that they lack the necessary resources and funds to enhance existing legal infrastructure.

2.2.4.2. ASEAN Framework on Intellectual Property Cooperation

The objectives of the ASEAN Framework Agreement on Intellectual Property Cooperation are strengthening cooperation in the field of intellectual property with a view to contributing to the promotion and growth of regional and global trade liberalization; promoting cooperation in the field of intellectual property among government agencies as well as among the private sectors and professional bodies of ASEAN; contributing to the promotion of technological innovation and the transfer and dissemination of technology; promoting the region-wide protection of patent; exploring the possibility of setting up an ASEAN trademark system; and most importantly, creating intellectual property ASEAN standards and practices consistent with international standards.

Various intellectual property rights initiatives were commenced and undertaken in order to achieve these goals. These include the Hanoi Plan of Action (HPA) and the ASEAN IPR Action Plan 2011-2015. The HPA, which was in place from 1999 to 2004, dealt with three IPR areas: protection, facilitation, and cooperation. It contained provisions regarding the strengthening of civil and administrative procedures and remedies for IP infringement, and technical cooperation relating to patent search and examination, computerization, and human resource development for the implementation of the TRIPS Agreement.

Measures geared towards intellectual property policy exchange among ASEAN member states were also created, including:

Exchange of information on: (a) well-known marks towards exploring the possibility of establishing a regional trademark system; (b) current IPR administrative systems with a view towards simplifying and standardizing them in the region;

Review of IP laws to ensure compliance with the TRIPS Agreement; and

---

291 Id.
Setting up of ASEAN electronic database on patents, designs, trademarks, geographical indications, copyright, and layout design of integrated circuits.\textsuperscript{295}

To accomplish the objective of establishing regional trademark and patent systems, “the HPA provided for the implementation of an ASEAN common form for trademark and patent applications in order to streamline the procedure.”\textsuperscript{296} Other measures included: promoting the accession of ASEAN member states to international IP treaties; encouraging IP awareness through training programs; and enhancing IP enforcement and protection, through information dissemination regarding ASEAN IP administration, registration, and infringement; facilitating interaction among government agencies; and encouraging bilateral/multilateral arrangements on mutual protection and joint cooperation in IPR enforcement.\textsuperscript{297}

Regardless of these plans, the establishment of the ASEAN regional trademark and patent filing systems were delayed. Some of the cited reasons for the delay, according to Weerawit Weeraworawit, include “sectarian oppositions and lack of political will, as well as inertia arising from international IP developments, such as the increasing importance of international IP registration systems that achieve the same objectives, e.g. the Madrid Protocol (for the international registration of marks) and the Patent Cooperation Treaty (PCT).”\textsuperscript{298} This led ASEAN to instead focus on the standardization of certain IP procedures and processes.\textsuperscript{299}

The 2011-2015 Intellectual Property Rights (IPR) Action Plan is built on earlier Action Plans, and seeks to further advance regional IP integration.\textsuperscript{300} This Plan deferred its previous goal of pursuing a fully harmonized regional IP system with one set of IP laws, and instead adopted a more flexible IP cooperation model.\textsuperscript{301} This approach, as mentioned by Elizabeth Siew-Kuan Ng, “enables its members to move forward collectively, but at varying paces in accordance with their developmental level and capacity... [and] emphasizes the

\textsuperscript{295} Elizabeth Siew-Kuan Ng, ASEAN IP Harmonization: Striking the Delicate Balance, 25 Pace Int’l L. Rev. 141 (2013) citing the ASEAN Hanoi Plan of Action, Art. 2.7.2 D & E, 2.7.2 F, and 2.7.2 G.
\textsuperscript{296} Elizabeth Siew-Kuan Ng, ASEAN IP Harmonization: Striking the Delicate Balance, 25 Pace Int’l L. Rev. 141 (2013).
\textsuperscript{297} Id. citing the ASEAN Hanoi Plan of Action, Art. 2.7.3.
\textsuperscript{299} Elizabeth Siew-Kuan Ng, ASEAN IP Harmonization: Striking the Delicate Balance, 25 Pace Int’l L. Rev. 142 (2013)
\textsuperscript{300} Id. at 146.
\textsuperscript{301} Id.
intensification of cooperation in joint focused programs and activities with measurable outputs in selected areas.\textsuperscript{302}

This Action Plan’s goals include creating an IP system that takes into account the varying levels of development of Member States and differences in the institutional capacity of national IP offices; developing national or regional legal and policy infrastructures that address evolving demands of the IP landscape; and encouraging active regional participation in the international IP community through the accession of Member States to three major international treaties (The Madrid Protocol; the ague Agreement; and the Patent Cooperation Treaty).

The Plan has led to concrete on-going projects such as the reduction of trademark registration backlogs, an ASEAN-wide patent search and examination system, accession by ASEAN members to various international IP treaties (such as the Patent Cooperation Treaty, Madrid Protocol, and the Berne Convention), the establishment of an IP Portal containing necessary intellectual property rights information for businesses and the general public, and the completion of the ASEAN Common Form for Trademark.

Scholars have identified some of the possible reasons for the slow and halting progress of ASEAN’s plans for regional intellectual property rights harmonization. One is that “ASEAN members’ diverse cultural traditions may influence their perception of IP and impact cooperation efforts.”\textsuperscript{303}

As one commentator has noted, some cultures “emphasize commonality” and hold the traditional belief that creative works and inventions are “community property” to be shared freely. The idea that IP is “private property” that must be protected by law may be a new and foreign concept, which may contribute to inertia in its national implementation.\textsuperscript{304}

Another challenge may be that local lawyers oppose the establishment of an ASEAN trademark and patent system “for fear of possible threats to their livelihood.”\textsuperscript{305} On the contrary, however, it is likely that this system will lead to a larger number of applications for trademarks, patents, and industrial design.\textsuperscript{306} Yet another hurdle is the lack of urgency for the implementation of a

\textsuperscript{302} Id.
\textsuperscript{303} Elizabeth Siew-Kuan Ng, ASEAN IP Harmonization: Striking the Delicate Balance, 25 Pace Int’l L. Rev. 132 (2013).
\textsuperscript{304} Id. citing Dongwook Chun, Patent Law Harmonization in the Age of Globalization: The Necessity and Strategy for a Pragmatic Outcome, 93 J. PAT. & TRADEMARK OFF. SOC’Y 127, 131-32 (2011) (stating that “[t]he Chinese believed for centuries that inventions and creative works belonged to the community or the government and should be freely shared”).
\textsuperscript{305} Weerawit Weeraworawit, The Harmonisation of Intellectual Property Rights in ASEAN, in Intellectual Property Harmonisation Within ASEAN and APEC 214 (Christopher Antons et al. eds., 2004).
\textsuperscript{306} Id.
region-wide patent and trademark system, and the lack of political will among ASEAN governments because such a system will compel Member States to change their IP laws, rules, and regulations.  

2.3. Lessons learned from the implementation of these ASEAN Soft Law instruments

2.3.1. Types of measures which are likely to achieve ASEAN policy objectives

A review of significant pieces of ASEAN soft law instruments, and literature that analyzes and critiques their implementation, will reveal that there are certain types of measures that, if executed, are likely to help achieve the Association’s policy objectives, as laid out in various Agreements, Conventions, and Declarations. Identifying these measures will help form the basis of the recommendations as to the ideal features and characteristics of a data protection soft law framework for the ASEAN region, which will be discussed in Chapter 6. These measures are the following:

2.3.1.1. Undertaking a harmonization project

ASEAN’s experience with the ASEAN-Australia Development Cooperation Program (AADCP) Harmonization of E-Commerce Legal Infrastructure in ASEAN Project led to the impressive feat of having the Southeast Asian region be recognized as the first region in the developing world to adopt a harmonized e-commerce legal framework consistent across jurisdictions. The hard harmonization model that was chosen by ASEAN for its e-commerce legal infrastructure project offers five benefits:

First, the guidelines are an inclusive instrument, which ensures the participation of less developed ASEAN member countries. They also contain implementation steps that ensure greater consistency across ASEAN member countries. In addition, the guidelines include a timetable, which helps to ensure an orderly, phased development of e-commerce legal infrastructure in ASEAN. Moreover, they leave less room for interpretation and reduce inconsistencies. Finally, they remain a flexible instrument that can be reviewed and updated (for example, every three years).

Indeed, this model produced tangible, positive results. The project resulted in achieving policy objectives, such as implementing consistent e-commerce laws across the Southeast Asian region, ensuring that these laws comply with

---

307 Id. at 215.
Pursuing a harmonization project for data protection will be helpful in coping with some of the challenges that are being faced by the Member States as the Association undertakes regional law enforcement efforts. Examples of these challenges are the following: due to a lack of legal harmonization efforts, some countries in the region have laws providing for certain penalties, such as confiscation and seizure, while others do not, and this complicates cross border cooperation in terms of prosecuting offenders; national regulations are not harmonized to allow for effective legal cooperation actions such as extradition; and investigative procedures are not uniform, which leads to insufficiency of information needed to pursue a case.

In addition, a harmonization project will help Member States navigate cultural differences that sometimes lead to variances or gaps in their laws. In the same way that cultural differences influenced the different countries’ perception of intellectual property and thus affected harmonization efforts in that field, it is likely that Member States’ varying opinions on the concept of privacy will have an impact on the creation of a harmonized data protection legal framework for Southeast Asia.

As ASEAN begins to pursue its plans of having a harmonized and comprehensive legal framework for data protection, it should strongly consider embarking on a hard harmonization project similar to that it undertook when it harmonized the region’s e-commerce legal infrastructure. The success of the e-commerce project is testament to the benefits that could arise, should the Association again resort to a team composed of a consulting firm, technical experts, and legal practitioners whose focus will be creating and implementing the steps necessary to achieve a harmonized legal framework for data protection, suited to Southeast Asia.

Any ASEAN harmonization project would also benefit from taking into consideration the lessons learned from the experiences of the Association with implementing its other soft law instruments. Some of those lessons are discussed in the rest of this sub-chapter, which talks about the types of measures which are likely to achieve ASEAN policy objectives, and the next sub-chapter, which presents and examines some of the challenges to be expected when ASEAN resorts to the use of soft law instruments in order to achieve policy objectives.

2.3.1.2. Establishing information networks

The first type of measure involves efforts geared towards establishing information networks. These networks, according to Anne-Marie Slaughter, “bring together regulators, judges, or legislators to exchange information and to collect and distill best practices. This information exchange can also take place
through technical assistance and training programs provided by one country’s officials to another.”

Indeed, going through discussions on the implementation of the Agreements, Declarations, and Conventions tackled in this chapter, one would observe that mechanisms for intelligence-exchange, information-sharing, capacity-building, training for government officials, judges, legislators, and other personnel, avenues for technical cooperation, and the establishment of information databases are commonplace.

Intelligence-exchange has been credited for aiding in the detection and apprehension of offenders and the instrumentalities of their offenses, as was the case in the ASEAN-China Cooperative Operations in Response to Dangerous Drugs and the ASEAN Convention on Counter-Terrorism. Information-sharing has led to better coordination in monitoring human trafficking cases, improved recovery efforts after natural calamities, and has contributed to the creation and review of e-commerce legislation to achieve harmonization across the region.

Capacity-building and training activities improved the ability of law enforcement to deal with the various aspects of drug production and trafficking. It has also improved criminal intelligence-gathering, investigation, security, and cross-border controls in the region. Training and capacity-building has also been instrumental in equipping judges and prosecutors to ensure that they can handle cases involving newly-enacted laws, regulations, and policies.

Technical cooperation has been instrumental in making the ASEAN the first region in the developing world to adopt a harmonized e-commerce legal framework, consistent across the 10 Member States. It has also improved disaster-readiness and post-calamity recovery in the region. The creation of databases has made information on ASEAN trade and customs laws and procedures accessible. Online databases have also brought Southeast Asian intellectual property rights information easily accessible to businesses and the general public.

2.3.1.3. Enforcement networks

The second type of measure, to which success in achieving ASEAN policy objectives has been partly attributed, is resorting to building enforcement networks. Enforcement networks are focused primarily on “enhancing cooperation among national regulators to enforce existing national laws and rules. As the subjects they regulate—from criminals to corporations—

---

309 Anne-Marie Slaughter, A New World Order, p. 19.
move across borders, they must expand their regulatory reach by initiating contact with their foreign counterparts.\textsuperscript{310}

Collective efforts among law enforcement units of the Member States have led to the discovery of international drug trafficking rings, and have also led to the apprehension and prosecution of narcotics producers and traffickers. Cross-border law enforcement arrangements that have been set up will also assist in enforcing human trafficking laws in the region and will help ensure the safe return of victims to their home countries.

The fact that an enforceable treaty obligation, in the form of the ASEAN Treaty on Mutual Assistance in Criminal Matters, is in force will help ensure that the Member States will render to one another the widest possible measure of mutual legal assistance in criminal matters, namely investigations, prosecutions and resulting proceedings. As previously mentioned, the assistance contemplated covers evidentiary matters, service of judicial documents, searches and seizures, production of documents, identifying and tracing instrumentalities of a crime, freezing, recovery, forfeiture or confiscation of property, and location and identification of witnesses and suspects. It is worth noting that the ASEAN, in its efforts to implement measures in its soft law instruments, can refer and resort to preexisting enforceable treaties, to pursue policy goals in its various Agreements and Declarations.

2.3.1.4. Provisions that integrate existing treaties and international model laws into its own soft law instruments

It would serve ASEAN well to learn from the experiences of its counterparts from the rest of the world, and to attempt to reconcile the provisions of its soft law instruments with the treaty provisions of other international organizations. It has previously done this by integrating provisions of existing treaties into its own Agreements and Conventions. For instance, in defining “terrorist offense,” ASEAN included offenses defined as such by 14 other counter-terrorism treaties. In doing so, it was able to consolidate laws on the same subject matter and was able to comply with other international initiatives. Similar efforts were undertaken when the Association drafted its Comprehensive Investment Agreement, thus producing comprehensive and clear definitions that are deemed in line with other international investment agreements.

In its harmonization efforts on e-commerce, ASEAN and its partners ensured that they conducted research on similar international initiatives, and that whenever possible, model laws and standards were incorporated into the resulting soft law instruments, and in draft national laws.

\textsuperscript{310} Id. at 63.
2.3.1.5. Provisions that call for the introduction of relevant national legislation and policies, accompanied by a monitoring mechanism to oversee local implementation

ASEAN Agreements on disaster management, tariff liberalization, and e-commerce have provisions calling on Member States to enact relevant national laws and policies, in order for the region to collectively achieve the policy objectives laid out in the Agreements. The Member States, in enacting appropriate legislation, were able to harmonize their laws, making them compatible with other pieces of legislation on the same subject matter in the Southeast Asian region, and this also aligned individual country laws to remove unwanted gaps, overlaps, and duplication. Furthermore, with the assistance of subject-matter experts who were tasked to assist in the harmonization of legal infrastructures, as was the case in the ASEAN-Australia Development Cooperation Program Harmonization of E-Commerce Legal Infrastructure in ASEAN Project, modern, best practices were adopted in the drafting of the Member States’ e-commerce laws.

In line with a previously-mentioned study on the key elements of a strong and comprehensive legal framework to address human trafficking, specific measures that could be included in the Member States’ local laws would be criminalizing the conduct sought to be curbed, criminalizing related offenses, and providing specific remedies and penalties.

It has been recommended that to further ensure that Member States implement the necessary national laws, monitoring mechanisms should be established. Currently, the ASEAN Secretariat provides support and coordinates efforts in implementing Agreements. There are instances where ministerial-level officials, such as the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) were given the responsibility of promoting, monitoring, reviewing, and reporting on the effective implementation of certain soft law instruments, such as those dealing with human trafficking. The establishment of an independent policy implementation center tasked with monitoring compliance with provisions of Agreements, Conventions, and Declarations has been suggested. Reporting and monitoring schemes would help provide updated information to the relevant government agencies and institutions, both regional and local, and could help to motivate member countries to meet specified targets.

2.3.1.6. Establishing specialist units

In tackling offenses of a cross-border nature, ASEAN has largely benefitted from setting up specialist units. For instance, in pursuing human trafficking cases, Member States set up specialist trafficking units, whose heads meet regularly to share information and coordinate tasks. As previously mentioned, the benefits of having specialist units include: better results in identifying and prosecuting offenders; investigators in the units quickly
become skilled in investigating complex offenses (such as breaches of data protection laws), which creates a pool of multi-skilled officials who can eventually be deployed to other enforcement units; it encourages the use of customized, standard investigative practices and procedures; and establishing these units will provide a focal point for investigations at the local, regional, and global level. In addition, establishing specialized units that will, over time, build up knowledge and expertise as an organization, can help remedy a situation that has been observed in the implementation of some Agreements on a local level – that of loss of skills and knowledge due to a high turnover of officers.

2.3.1.7. Establishing the widest possible jurisdiction over offenses

Yet another lesson that could be drawn from ASEAN’s experience with using soft law to combat human trafficking is that of establishing the widest possible jurisdiction over offenses, in order to reduce or eliminate safe havens for offenders. The rules that could be applied in this regard, as culled from an ASEAN report, are the following:

(a) A State is required to establish jurisdiction over offences when the offence is committed in the territory of that State or on board a vessel flying its flag or on an aircraft registered under its laws (the territoriality principle).
(b) A State may exercise jurisdiction over offences when committed outside the territorial jurisdiction of that State against one of its nationals (the principle of passive personality).
(c) A State may exercise jurisdiction over offences when committed outside the territorial jurisdiction of that State by one of its nationals (the principle of nationality).
(d) A State may exercise jurisdiction over offences when such are committed outside the territorial jurisdiction of that State but are linked to serious crimes and money laundering planned to be conducted in the territory of that State.
(e) A State must establish jurisdiction over offences when the offender is present in the territory of the State and the State does not extradite the offender on grounds of nationality (the principle of “extradite or prosecute”).

Indeed, having intra-regional rules on jurisdiction, especially on a subject matter that would have cross-border implications, such as data protection, would better facilitate law enforcement.

311 Progress Report on Criminal Justice Responses to Trafficking in Persons in the ASEAN Region p. 9.
2.3.1.8. Enacting a clear and simplified comprehensive Agreement that consolidates related instruments and policies

The success of the tariff liberalization efforts in the Southeast Asian region has been partly attributed to the form of the Agreement itself. The ATIGA, together with its Annexes, is comprehensive, since it contains all the pertinent and necessary rules and regulations, which makes compliance easier. It also consolidated and streamlined the rights and obligations of parties, contained in existing initiatives, into one document. A single Agreement that clearly demonstrates the interaction of its provisions, as is the case in the ACIA, also makes compliance simpler and less complicated.

2.3.1.9. Building a mechanism for complaint-filing and dispute resolution

In implementing the ATIGA, ASEAN employed a system wherein an ASEAN-based enterprise may submit a complaint online through the ASEAN Solutions for Investments, Services and Trade (ASSIST) website. As previously explained, the ASEAN Secretariat reviews the complaint and forwards it to the proper government agency for resolution; the ASEAN-based enterprise may accept the proposed solution, or reject it and seek other dispute resolution avenues.

In addition, ASEAN Agreements, such as the ACIA, explicitly provide for the procedure to be followed in the event of an investment dispute. The process involves resorting to consultation and negotiation; if the dispute has not been resolved, the disputing investor may submit a claim to the courts or administrative tribunals, or to one of several arbitration institutions, such as the Regional Centre for Arbitration at Kuala Lumpur.

Having an easily-accessible mechanism through which enterprises could file their complaints and have those complaints resolved by the proper government agency, and a detailed process through which disputes may be settled, help boost investor confidence.

2.3.2. Challenges to be expected when ASEAN resorts to the use of soft law instruments in order to achieve policy objectives

The Association’s experience with the use of soft law will show that certain measures, such as those outlined in the immediately preceding subchapter, will likely yield positive results and help achieve stated policy objectives. Nevertheless, significant challenges must be addressed, and possible pitfalls must be avoided, when the ASEAN embarks on a project dedicated to creating a regional soft law legal framework for data protection.

a) Human rights concerns and offenses committed by the Member States: Analyses of the ASEAN counter-terrorism Agreement, the ACCT,
have mentioned the Agreement’s lack of a mechanism to address human rights disputes that could arise in implementing the instrument. Reviews of the same Agreement also critique the absence of provisions addressing offenses that could be committed by the Member States themselves, against their own citizens. These reports imply that in Agreements that implicate civil and political rights because their implementation calls for surveillance and investigations, there are usually no safeguards, remedies, or procedures that could be resorted to, in order to address claims of human rights abuses; neither are there such measures to address offenses that could potentially be committed by government instrumentalities.

To further understand the human rights situation in Southeast Asia and how it will affect any regional undertaking involving data protection, one must consider the status of privacy as a human right across the ASEAN region. Only six ASEAN Member States’ constitutions mention the right to privacy.\(^{312}\) Furthermore, the extent to which the right is protected is not uniform across these States, and protections against searches of the home, residence, or property, the individual’s person, undue exploitation of personal data, and protections of honor, dignity and reputation, correspondence and other communications, and the right to family life are neither consistently protected, procedurally or substantively.\(^{313}\)

However, the *ASEAN Human Rights Declaration* (ADHR) explicitly recognizes the right to privacy. Article 21 states: “Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person’s honour and reputation. Every person has the right to the protection of the law against such interference or attacks.” Inclusion of this provision in the ADHR confirms the need for the ASEAN to ensure that as it works towards promoting data protection across the region, economic considerations must be balanced against privacy rights.

Recognizing the commonly-prescribed measure of mandating the enactment of local laws to achieve regional policy goals, it has been suggested that in order to “reflect recent developments in soft law surrounding the right to privacy and ASEAN’s own institutional planning documents, there must be a clearer formulation of Member


\(^{313}\) Id.
States’ obligation to ‘adopt legislative and other measures’ to protect personal and confidential information against interception, collection and misuse by both state and private actors.”

The challenge then, for the ASEAN as it creates a regional soft law framework for data protection, is to ensure that there are provisions that call on all Member States to recognize privacy as a human right, and that the Association is able to guide the Member States as they draft or revise their laws to ensure that their legislative issuances effectively protect against privacy violations committed by both private and state actors.

b) **Measures which may be expensive to implement and administer:** A critique of the ACIA involves the difficulty encountered by some Member States in implementing the said Agreement’s provisions because of lack of resources. The enactment of new laws and regulations, or even the revision of existing ones, entail significant expense. More onerous is the implementation and administration of new laws, especially if this necessitates the creation of new government agencies.

The ASEAN, in proposing data protection measures for the region, will have to contend with the fact that the inability of Member States to comply with a potential soft law framework could be attributed to the significant expense involved in such an undertaking. A possible remedy lies in cooperative efforts that will allow countries with less resources to seek assistance from their ASEAN neighbors for matters such as drafting legislation, gaining technical expertise, receiving training, and sharing in the output of research efforts.

c) **Lack of public consultation and public support:** In the discussions surrounding the economic Agreements on trade liberalization, a criticism was that on a national level, not all concerned sectors were consulted during the drafting of the instrument. As a result, some affected sectors felt that their concerns were not sufficiently addressed, leading to public backlash against the Association’s trade liberalization efforts. The opposition against certain tariff measures was also partly attributed to the absence of outreach efforts to gather public support for ASEAN’s new economic policies.

---

The Association will have to ensure that the business sector, human rights advocates, academics, various professional organizations, and technical experts, among others, will have to be directly engaged when it drafts a soft law framework for data protection, as the input of these sectors will be highly valuable in ensuring that interests of various stakeholders are well-represented in the drafting process. Engaging these sectors will also help bolster public support for ASEAN’s efforts to promote data protection in the region.

**d)** *Institutions with overlapping functions:* In ASEAN’s experience of using soft law instruments to help cope with natural disasters, the Association had to contend with various regional and government institutions with overlapping functions. Their lack of coordination has been cited as a challenge in providing better disaster management response. There are more than 20 sectors in ASEAN that should be engaged in the implementation of the AADMER work program, and it is indeed a large task for existing institutions to engage and coordinate all sectors.\(^{35}\)

The Association, in pursuing its goal of promoting data protection in the region, should then anticipate the significant task of coordinating the plans and actions of multiple institutions, which could include existing and yet-to-be-established national privacy enforcement authorities, consumer protection agencies, and law enforcement bodies.

**e)** *Confusing state of laws and regulations:* In addressing the transboundary haze problem, the ASEAN, in particular the Member State identified as the largest producer of the haze, Indonesia, faced the difficulty of having to deal with multiple laws and regulations on the same subject matter, issued by various legislative and executive bodies. These legal instruments were often contradictory, thus creating confusion among those tasked to enforce them and those who sought remedies.

The ASEAN will have to undertake the challenge of gathering all pieces of national legislation and regulations that touch upon data protection, and analyze how they are implemented, who enforces them, and if there exists any contradictions among these enactments. For Member States with significant legislative and regulatory gaps,

---

the Association will have to ensure that in drafting the necessary data protection laws and regulations, inconsistencies among relevant laws will be avoided and institutional overlaps reduced or eradicated altogether.

Considering that: a) only Malaysia, Singapore, and the Philippines among the Member States have comprehensive data protection laws; b) that in these countries, there are also other statutes that deal with data protection; and c) that in the seven remaining Member States, they have, in varying degrees of number and development, laws and regulations concerned with data protection, coupled with the absence of a comprehensive data protection law, efforts to ensure that laws on the matter are consistent and that the government agencies tasked to enforce them are properly identified, are necessary.

f) Failure to provide specific prescriptions on remedial measures: Another lesson to be learned from ASEAN’s work in addressing the transboundary haze problem is to ensure that monitoring efforts prescribed in Agreements should not end at merely gathering data and evaluating whether its provisions are followed by the Member States. Critics have described that reporting requirements that aid in the monitoring of obligations are limited in their effects because the monitoring body – the ASEAN Center – is not bound to do anything more beyond analyzing data and providing risk assessments to the state parties. It has been recommended that for monitoring to be more fruitful, the monitoring body should prescribe remedial measures as well.

In the event that an ASEAN data protection soft law framework will prescribe the monitoring of obligations, the Association should strongly consider giving the monitoring agency the authority to prescribe remedial measures, should it observe shortcomings on the part of the reporting Member State. Ideally, the entity that could make assessments is an office within the Association itself, charged with monitoring compliance with its data protection efforts. This could be an ASEAN Data Protection Office (which will be further elaborated upon in the succeeding chapter), or an office whose main task is monitoring compliance with all ASEAN soft law instruments.

g) Wide differences in the operational capacity of enforcement agencies: As illustrated in the analysis of the implementation of the ACCORD, disparities in the operational capacity of enforcement authorities are critical because it is unlikely that law enforcement efforts will be effective if not all concerned law enforcement units across the region, and their capacity to perform their responsibilities, are up to standard.
ASEAN should look into ways as to how it could prevent a net loss to cross-border efforts due to inadequate information resulting from the insufficiency of data and intelligence gathered by an agency in a Member State with fewer resources. In creating a soft law framework for data protection, ASEAN should provide for means to help build the capacity of the proper government agencies, such as data protection authorities, to investigate possible breaches of data protection laws, and other related offenses, especially those with cross-border implications.

h) Insufficient funding: The regional e-commerce project showed that a lack of funding and resources on the part of some Member States, especially those from the CLMV bloc, can hamper the progress of harmonization projects. Thus, these Member States may need some form of external assistance to implement prescribed measures. It should thus be noted that several ASEAN member countries have benefited from external assistance, including training programs and advisory services provided by various United Nations organizations, such as UNCITRAL and UNCTAD.

i) Absence of independent, well-resourced regulators: A key challenge identified by those who conducted the harmonization project of ASEAN’s e-commerce legal infrastructure was the absence of independent, capable regulators. The existence of a regulatory agency is justified by the expertise necessary to administer laws concerning a complex, technical, and relatively new field, the need for specialized knowledge to be able to issue and implement appropriate and effective rules and regulations with expediency, and the necessity of having an independent agency due to its powers to investigate and monitor other government instrumentalities.

In drafting its own data protection soft law framework, the ASEAN should strongly consider prescribing the establishment of an independent data protection authority for each Member State.

2.4. Chapter Conclusion

A review of ASEAN soft laws and their implementation will show that particular measures are likely to achieve stated policy objectives. If the policy objective involves the Member States having legislation in line with international best practices and regulations and having a harmonized legal infrastructure or a comprehensive framework for a certain area of concern, such as data protection, one measure likely to be effective is undertaking a multi-phase hard harmonization project.
This harmonization project should take the following measures into consideration when it formulates the specific steps needed to be undertaken to create a harmonized legal framework: drafting a clear and simplified comprehensive Agreement that consolidates related instruments and policies; integrating appropriate and relevant provisions of related treaties and international model laws into this Agreement; ensuring that stakeholders are engaged and consulted in the drafting process; building regional information and enforcement networks; calling for the enactment of relevant national laws and regulations, which are administered by independent regulators and specialist units; ensuring that these national laws recognize as offenses the conduct sought to be curbed, that appropriate remedies and penalties are in place, and that related offenses are similarly addressed; creating a mechanism that will monitor compliance with Member States’ obligations; ensuring that the widest possible jurisdiction for offenses is recognized; establishing an easily-accessible online mechanism for complaint filing; providing for specific dispute resolution remedies; and authorizing the monitoring body to prescribe remedial measures.

A harmonization project that seeks to create a harmonized and comprehensive legal framework for data protection in the ASEAN region should recognize and address the following challenges: possible human rights violations and privacy violations committed by the Member States themselves; insufficient funding that could hinder the complete implementation of the necessary measures in certain ASEAN countries; and differences in operational capacity among the relevant government agencies.
3. International Data Protection Soft Law: What is it, and what are the lessons to be learned from its implementation by the APEC and OECD?

Chapter Four Outline
4.1 Chapter Abstract
4.2 International Data Protection Soft Law
   4.2.1 What is International Data Protection Soft Law?
       4.2.1.1 Definitions
           4.2.1.1.1 Privacy and / versus Data Protection
           4.2.1.1.2 Data Protection Law
           4.2.1.1.3 Data Protection Soft Law Framework
   4.2.2 The emergence of International Data Protection Soft Law Frameworks
4.3 Examination of the use of Soft Law in International Data Protection: Lessons learned from the OECD Privacy Guidelines and the APEC Privacy Framework
   4.3.1 The OECD Privacy Guidelines and the APEC Privacy Framework
       4.3.1.1 The OECD Privacy Guidelines
       4.3.1.2 The APEC Privacy Framework
   4.3.2 What are the advantages and disadvantages of the following features and characteristics of the APEC Privacy Framework and the OECD Privacy Guidelines? What are the successes of and challenges involved in the implementation of these features and characteristics?
       4.3.2.1 National / domestic implementation strategies
           4.3.2.1.1 Review of domestic frameworks
           4.3.2.1.2 Establishing Data Protection Authorities
           4.3.2.1.3 Promotion of legislative approaches
           4.3.2.1.4 Promotion of self-regulation
           4.3.2.1.5 Encouraging the establishment of privacy management programs
           4.3.2.1.6 Professionalizing the privacy practice / instituting data protection and privacy law credential programs
           4.3.2.1.7 Encouraging the deployment of privacy-enhancing technologies
           4.3.2.1.8 Having Member States report on their domestic implementation of the framework’s recommendations
       4.3.2.2 International implementation strategies
           4.3.2.2.1 OECD’s Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy
           4.3.2.2.2 APEC Cross Border Privacy Rules System and the APEC Cross Border Privacy Enforcement Arrangement
               4.3.2.2.2.1 The advantages and successes of the APEC CBPR and CPEA System
               4.3.2.2.2.2 The disadvantages and weaknesses of and challenges involved in implementing the APEC CBPR System

4.4 Chapter Conclusion
3.1. Chapter Abstract

The goal of this dissertation is to propose a set of ideal features and characteristics for an ASEAN data protection soft law framework. In order to produce a set of these ideal features and characteristics, the previous chapter presents the lessons that could be learned from ASEAN soft laws. These lessons reveal those ASEAN soft law features and characteristics that could be adapted for the purpose of promoting data protection in the region because of their likely success in attaining specific policy goals. This chapter, on the other hand, offers the lessons that could be gleaned from two existing data protection soft law frameworks – the OECD Privacy Guidelines and the APEC Privacy Framework.

Learning from the successes and weaknesses of, and the challenges involved in implementing the OECD Privacy Guidelines and APEC Privacy Framework would help in discovering the types of features and characteristics a data protection soft law framework should ideally possess so that it could better achieve its stated policy goals. This exercise also exposes some of the challenges encountered in the implementation of these frameworks. Being aware of these challenges could help the ASEAN address and avoid the weaknesses in the two frameworks being discussed.

However, before a study on the topic could be embarked upon, one must first provide a definition of “data protection soft law framework.” Subchapter 4.2 provides a definition of this term in the form of a set of elements. It is hoped that this definition could enhance and improve discussions in this dissertation, and in future studies on similar and relevant subjects. The same subchapter also provides the reasons as to why it is highly likely that a data protection soft law framework will emerge in Southeast Asia.

Subchapter 4.3 then proceeds to inform readers about the general features of the OECD Privacy Guidelines and the APEC Privacy Framework. It describes some of their salient features and characteristics, particularly those that could be adapted by the ASEAN when it decides to create its own data protection soft law framework for the Southeast Asian region. These specific measures are briefly explained, and then their benefits discussed. Save for the first feature, each measure’s drawbacks, weaknesses, or the challenges involved in implementing it are presented. This is followed by proposals on how to address these drawbacks, weaknesses, or challenges.

The following chapter will then take the results of the discussions in this chapter and the previous chapter, and come up with a recommendation in the form of a set of features and characteristics that would be ideal for an ASEAN data protection soft law framework.
3.2. International Data Protection Soft Law
3.2.1. What is International Data Protection Soft Law?

3.2.1.1. Privacy and / versus Data Protection

A survey of literature on the subject will likely lead one to conclude that there is no single, ultimate definition of the term “privacy.” For Daniel Solove,316 privacy is “a concept in disarray.” It is a “sweeping concept, encompassing (among other things) freedom of thought, control over one’s body, solitude in one’s home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogations.”317 The following definitions illustrate the diversity in opinion with regard to the definition of privacy.

In Privacy and Freedom,318 Alan Westin described privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” Westin elaborated, explaining that privacy is:

[t]he voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.319

Westin illustrated four states of privacy: (1) solitude; (2) intimacy; (3) anonymity; and (4) reserve.320 The first is a separation from the group and freedom from the observation of other persons, said to be the most complete state of privacy.321 In the second state, the individual is a “part of a small unit that claims and is allowed to exercise corporate seclusion so that it may achieve a close, relaxed, and frank relationship between two or more individuals.”322 The third state of privacy occurs “when the individual is in public places or performing public acts but still seeks, and finds freedom from identification and surveillance.”323 It also encompasses the situation of publishing ideas anonymously.324 The last state is “the creation of a psychological barrier against unwarranted intrusion; this occurs when the individual’s need to limit communication about himself is protected by the willing discretion of those surrounding him.”325

317 Id.
319 Id.
320 Id at 43.
321 Id.
322 Id.
323 Id.
324 Id.
325 Id at 43.
For Ruth Gavison, privacy relates to “accessibility to others; the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others’ attention.” On the other hand, for Charles Fried, privacy is not merely “an absence of information about what is in the minds of others.” For him, it is the “control over knowledge about oneself.”

As for the right to privacy, Samuel Warren and Louis Brandeis defined it as the individual’s “right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.” In their groundbreaking article, The Right to Privacy, Warren and Brandeis asserted that one cannot be compelled to express these thoughts and sentiments (except when upon the witness-stand); and even if an individual has chosen to express these thoughts, “he generally retains the power to fix the limits of the publicity which shall be given them.”

One particular article, however, was able to distill the different conceptions of privacy into six categories. In Conceptualizing Privacy, Solove submitted the general concepts that encompass the recurrent views on what privacy means:

(i) the right to be let alone-Samuel Warren and Louis Brandeis’s famous formulation for the right to privacy; (2) limited access to the self-the ability to shield oneself from unwanted access by others; (3) secrecy-the concealment of certain matters from others; (4) control over personal information-the ability to exercise control over information about oneself; (5) personhood-the protection of one’s personality, individuality, and dignity; and (6) intimacy-control over, or limited access to, one’s intimate relationships or aspects of life.

Indeed, as Graham Greenleaf has mentioned, “[p]hilosophical arguments about how ‘privacy’ should best be conceptualized and defined, and the resulting arguments about the extent to which aspects of such a concept of privacy should be protected by law, can take many directions.” One can write an entirely separate dissertation just on the concept of “privacy.” However, such discussions are outside the scope of this work, because the concept of “data
protection,” which is the main subject of this dissertation, is now “relatively well defined as a set of ‘data protection principles’, which include an internationally accepted set of minimum principles plus additional principles which are evolving continually through national laws and international agreements.”

For Colin Bennett, data protection pertains to the group of policies designed to regulate the collection, storage, use, and transmission of personal information. Explaining the divergence in appellation, Bennett states: “[Data protection] is more technical and esoteric and means little to the average citizen. For this reason, most English-speaking nations have retained the word “privacy” to add popular appeal to statutes that essentially perform the same functions as European data protection laws.” For Bennett, data protection is a more precise term, and it distinguishes the policy problem from the broad social value (privacy) that has such a fertile tradition and significance in the liberal democratic heritage. Data protection is largely similar to the concept of “information privacy,” the classic definition of which is given by Westin, and is worth reiterating: “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

Outside Europe, the term “data protection” is frequently used to designate activities that Americans would designate as “privacy” centric. In Southeast Asia, for example, the laws of Malaysia and Singapore use “data protection” in the titles of their statutes on this matter. This could likely be attributed to the fact that “the major influence on the data privacy laws outside Europe, including in Asia, will be shown to be ‘European standards’.”

3.2.1.1.1. Data Protection Law

Data protection law, according to Paul Schwartz, “refers to the legal structures that attempt to regulate knowledge and concealment of an individual’s personal information.” It addresses the ways in which personal information is gathered, registered, stored, exploited, and disseminated. For

---

333 Id.
335 Id. at 14.
336 Id.
337 Id.
341 Graham Greenleaf, Asian Data Privacy Laws: Trade & Human Rights Perspectives
Graham Greenleaf, data protection laws “essentially comprise a set of enforceable data privacy principles based on the ‘life cycle’ of personal data (collection, accuracy, security, use, disclosure, access, deletion, etc.) coupled with an enforcement structure backed by legal measures requiring compliance.” Enforcement is commonly assigned to a Data Protection Authority (DPA), Privacy Enforcement Authority (PEA) or Privacy Commissioner, but often involves other enforcement authorities as well.

Data protection laws typically apply “only to data that relates to, and permits identification of, individual physical/natural persons (hereinafter also termed simply ‘individuals’).” However, in rare cases, its rules also apply to data about corporations and other legal or juristic persons. A more precise way to think about the data to which these laws apply is to understand the concept of personally identifiable information (PII) as a continuum. Schwartz and Solove’s “PII 2.0” model “places information on a continuum that begins with no risk of identification at one end, and ends with identified individuals at the other.” Schwartz and Solove divided this spectrum into three categories, “each with its own regulatory regime: under the PII 2.0 model, information can be about an (1) identified, (2) identifiable, or (3) non-identifiable person. [These] three categories divide up this spectrum and provide different regimes of regulation for each.” Since these categories do not have hard boundaries, they defined them in terms of standards.

As for the first category, “[i]nformation refers to an identified person when it singles out a specific individual from others. Put differently, a person has been identified when her identity is ascertained.” In the second category, which is in the middle of the risk continuum, information pertains to an identifiable individual when “specific identification, while possible, is not a significantly probable event.” In this case, “an individual is identifiable when there is some non-remote possibility of future identification.” Schwartz and Solove assert that the risk level for such information is low to moderate, hence this type of information “should be treated differently from an important subcategory of nominally identifiable information, in which linkage to a specific person has not yet been made, but where such a connection is more

---

342 Id at 5 (2014).
343 Id at 5-6.
344 Id at 5.
346 Id.
348 Id.
349 Id.
350 Id.
351 Id.
likely.”\textsuperscript{352} In the third category of PII, which is at the other end of the risk continuum, nonidentifiable information cannot be said to be relatable to a person, considering the means likely to be used for identification; in this instance, the risk of identification is remote.\textsuperscript{353}

Lee Bygrave provides for more distinguishing features of data protection law. One is that data protection law is largely statutory. Although both case law and various forms of soft law, such as guidelines, recommendations, and codes of conduct, are encompassed within data protection law, the fundamental rules are usually expressed in legislation.\textsuperscript{354} Another is that data protection statutes commonly take the form of “framework” laws.\textsuperscript{355} Instead of prescribing detailed rules on data processing, data protection legislation “tends to set down rather diffusely formulated, general rules for such processing, and provide for the subsequent development of more detailed rules as the need arises.”\textsuperscript{356} This demonstrates a desire for the necessary regulatory flexibility because of the complex and evolving nature of technology, in addition to the uncertainty over the nature of the interests to be protected.\textsuperscript{357}

### 3.2.1.1.2. International Data Protection Soft Law Framework

Synthesizing relevant discussions in this chapter and previous ones, one can present a definition of “international data protection soft law framework” in the form of a set of elements. These elements are:

i. A legal structure that attempts to regulate the ways in which personal information is gathered, registered, stored, used, and disseminated;

ii. The legal structure encompasses both the conduct of states with and among each other, and the conduct of private parties involved in cross-border transactions, in relation to the gathering, registering, storing, use, and dissemination of personal information;

iii. The legal structures lack one, two, or all of the following: (i) precision of rules; (ii) enforceable obligations; and/or (iii) delegation of authority to a third-party decision-maker to monitor, interpret, or enforce implementation; and

iv. The legal structures tend to set down diffusely formulated, general rules for gathering, registering, storing, using, and disseminating personal information, and provide for the

\textsuperscript{352} Id.
\textsuperscript{353} Id.
\textsuperscript{354} Lee Bygrave, Data Privacy Law: An International Perspective, p. 3 (2014).
\textsuperscript{355} Id.
\textsuperscript{356} Id.
subsequent development of more detailed rules as the need arises.
This definition is intended to encompass those legal structures that provide for broad, general rules that influence, in a non-binding and unenforceable manner, the ways in which personal data is processed, both within national borders, and when the data crosses those borders.

3.2.2. The emergence of international data protection soft law

Lee Bygrave asserts that there are “three categories of factors behind the emergence of data protection law: (i) technological and organizational developments in the processing of personal data; (ii) fears about these developments; and (iii) other legal rules.”

Data protection laws, which have been in existence since the 1960’s, “emerged on the political agendas of advanced industrial states as a result of the development and application of computers.” With this development came the “greater dissemination, use, and re-use of personal data across organizational boundaries and, secondly, replacement or augmentation of manual control mechanisms by automated mechanisms.” Related to these trends are the dangers associated with the use of data for purposes other than the purposes for which it was originally gathered; the likelihood of misinterpreting and misapplying data; the dissemination of invalid or misleading data; the automatic processing of organizational decision-making processes; and individuals being evaluated or acted upon on the basis of data about them that is inaccurate, or of poor quality.

In relation to these dangers, a complex set of fears arose with regard to the implications for the personal privacy of citizens, and the policy area known as data protection emerged. “By the end of the 1980’s the protection of personal data had taken on a momentum of its own and is a separate and significant issue of public policy.” In addition to a growing distrust of technology were economic concerns; one fear is that the emerging data protections laws will unduly hamper the transborder flow of data. This fear came about because of the new European data protection laws that restricted the flow of personal data to states that do not provide a level of data protection similar to the “exporting” country. Hence, the principal international codes were all introduced partly to minimize the harmful effect that such restrictions

359 Id.
361 Id.
362 Id.
364 Id.
would have on international commerce and freedom of expression. Yet another anxiety relates to the possibility that, without data protection laws, individuals will lack confidence to participate in commerce, as consumers. The enactment of data protection laws can thus be partly attributed to efforts to boost public trust in the way organizations process personal data.

The third factor for the emergence of data protection laws is rooted in the fact that data protection legislation would not have been enacted if not for the inability of pre-existing laws to deal with the problems resulting from the earlier mentioned two categories of factors. This is understandable, considering the novelty of issues that arose in relation to emerging technologies capable of accomplishing tasks not previously possible.

It is submitted that the reason why international data protection laws (and international data protection soft law frameworks) arose and will continue to arise is because of the factors presented above, combined with the need for the problems related to those factors to be addressed on a regional or global scale.

It has been theorized by Colin Bennett that technological development in this area had a leveling impact on diverse social structures, cultural traditions, and public policies. The result is that various states will be pressured to respond to these technological developments in similar ways – a policy convergence, simply put. However, this technological determinism is only one explanation for policy convergence in data protection. The second possible explanation for the similar (though not necessarily identical) response among states as they try to address data protection concerns is emulation – policy makers imitate or adapt the efforts of other countries because the incentives to copy or draw lessons from the pioneers of data protection are strong. When solutions beyond the existing arsenal of national policy and regulations are required, and a state has no experiences from which to learn, there is a natural tendency to seek answers from the experiences of other countries – to see how these other states have addressed novel policy questions, to share ideas, and to bring foreign insights into local decision-making.

The third likely reason for policy convergence in data protection, according to Bennett, is elite networking, where “the convergence results from

---

365 Id.
366 Id.
367 Id.
368 Id at 11.
370 See Id.
371 Id.
372 Id.
373 Id at 4-5.
the shared beliefs of a relatively coherent and enduring network of elites bound by expertise on an issue and a common concern for its resolution.”

In this case, policy convergence is the result of a consensus among members of a transnational “policy community” or “issue network.”

The fourth reason is harmonization, wherein the harmonization of policy by intergovernmental institutions is encouraged by interdependence and a need to lessen inconsistencies and incompatibilities. There comes a point where states realize that certain problems cannot be resolved on a national level, and that in situations where the subject of the policy issue concerns something of a transnational nature, such as data protection, solutions that cross national borders become necessary.

Bennett’s fifth explanation for policy convergence in the data protection sphere is the one he termed penetration. This is based on the assumption that policy action within one jurisdiction, whether a state or an international organization, “may carry certain costs that are then exported to those which have not yet responded.” In this type of penetrative process, foreign officials affect policy-making by providing advice, and by sending a strong message that the concerned country has no other option but to follow a dominant trend.

Considering the following:

i. the widespread use of technology that allows the automated processing of personal data within and across national borders in Southeast Asia;

ii. the privacy and security concerns surrounding these technologies and processes;

iii. the need to bolster consumer trust to foster commerce, especially e-commerce within the region;

iv. the practice of Southeast Asian policy makers of adapting the national policies and learning from the experiences of other countries with regard to novel policy issues; and

v. the existence of a network of policy experts within Southeast Asia who have stated, through the Association’s ASEAN Economic Community plans and Blueprints, the necessity of creating a comprehensive and harmonized framework for e-commerce and, in particular, data protection;

it is highly likely, if not inevitable, that a policy convergence on data protection will occur among the ASEAN Member States. ASEAN’s deeply entrenched practice of avoiding legally binding and enforceable commitments, as

---

374 Id at 5.
375 Id.
376 Id.
377 Id.
378 Id at 4-5.
379 Examples would include the policy areas of e-commerce and intellectual property rights, as explained in the previous chapter.
explained in Chapter 2, increases the likelihood that the data protection legal structure that will emerge in the region will be one that can be characterized as soft law. Furthermore, considering the need for the necessary regulatory flexibility because of the complex and evolving nature of the technology involved in processing personal data, it is similarly likely that the resulting legal structure for the region will take the form of a framework, which will set diffusely formulated and general rules, instead of a set of highly detailed and specific provisions.

To be able to give recommendations as to what the ideal features and characteristics a potential data protection soft law framework for the ASEAN region should have, this dissertation will look at the lessons that could be learned from existing international data protection soft law frameworks. These would be the OECD Privacy Guidelines (OECD Guidelines) and the APEC Privacy Framework (APEC Framework).

3.3. Examination of the use of Soft Law in International Data Protection: Lessons learned from the OECD Privacy Guidelines and the APEC Privacy Framework

3.3.1. The OECD Privacy Guidelines and the APEC Privacy Framework

3.3.1.1. The OECD Privacy Guidelines

The Organisation for European Economic Co-operation (OEEC) was established in 1948 to run the US-financed Marshall Plan for the post-World War II reconstruction of Europe. Focusing on the necessity of economic interdependence, it ushered in a new era of cooperation in the European continent. Encouraged by its success and the possibility of bringing its work to the rest of the globe, Canada and the US joined OEEC members in signing the new OECD Convention on December 14, 1960. The Organisation for Economic Co-operation and Development (OECD) was officially founded on September 30, 1961, when the Convention entered into force.

Today, 34 OECD member countries regularly consult with each other to identify problems, discuss and analyze them, and promote policies to solve them. Collectively, the OECD brings together countries that account for 80% of world trade and investment, giving it a significant role in addressing global economic challenges.

OECD “uses its wealth of information on a broad range of topics to help governments foster prosperity and fight poverty through economic growth and

381 Id.
382 Id.
383 Id.
384 Id.
385 Id.
financial stability.” Its work is based on monitoring events in member and non-member countries, and includes regular projections of short and medium-term economic developments. The OECD Secretariat collects and analyzes data; various committees then discuss policy regarding this information; the Council makes decisions; and then governments implement the Organization’s recommendations.

Discussions at the committee-level sometimes evolve into negotiations where OECD countries agree on rules to facilitate international cooperation. The result of these negotiations could be formal agreements among countries, for example on combating bribery, on arrangements for export credits, or on the treatment of capital movements. They may create standards and models, such as those for the use of bilateral treaties on taxation, or recommendations, for example on cross-border co-operation in enforcing laws against spam. They may also result in guidelines, for instance on corporate governance or environmental practices. Another one of these resulting guidelines is the OECD Privacy Guidelines.

The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Data, which were released in 1980, were the first internationally agreed-upon set of privacy principles. Recognizing the importance of information, including personal information, in the global economy, and the developing concerns about the impact on the rights of individuals arising from the automated processing of personal information, spurred the creation of these Guidelines. Another reason for the creation of these Guidelines were fears that varying national regulations, that would have considerable impact on interconnecting communications technology, would produce grave inefficiencies and economic costs. In addition, the OECD foresaw the possible global economic risk of placing undue restrictions on the flow of information.

The goals of the OECD Guidelines are:

a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;

---

386 What We Do and How, accessed at http://www.oecd.org/about/whatwedoandhow/.
387 Id.
388 Id.
389 Id.
390 Id.
391 Id.
392 Id.
393 Thirty Years After: The OECD Privacy Guidelines, p.3.
394 Id.
395 Id at 8.
396 Id. at 10.
b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;

c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and

d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows.\textsuperscript{397}

These Guidelines focus on two essential basic values: the protection of privacy and individual liberties, and the advancement of free flows of personal data.\textsuperscript{398}

The Guidelines consist of five parts. Part One contains the necessary definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards.\textsuperscript{399} Part Two, which is the core of the Guidelines, presents eight basic principles relating to the protection of privacy and individual liberties at the national level.\textsuperscript{400} These principles are Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.

Part Three sets out principles of international application, which are chiefly concerned with relationships between Member countries.\textsuperscript{401} Part Four presents, in general terms, various means of implementing the Guidelines’ basic principles, and specifies that these principles should be applied in a non-discriminatory manner.\textsuperscript{402} Part Five discusses matters of mutual assistance among Member countries, primarily through the exchange of information, and by avoiding incompatible national procedures for the protection of personal data.\textsuperscript{403} It concludes by referring to legal issues that may arise when flows of personal data involve several Member countries.\textsuperscript{404}

The Guidelines are not legally binding on OECD member states. However, its accompanying OECD Council Recommendation states that account should be taken of them when member countries develop domestic legislation.

\textsuperscript{398} Id.
\textsuperscript{399} Id. at par. 23.
\textsuperscript{400} Id.
\textsuperscript{401} Id.
\textsuperscript{402} Id. at par. 24.
\textsuperscript{403} Id.
\textsuperscript{404} Id.
on privacy and data protection.\footnote{Lee Andrew Bygrave, Data Privacy Law: An International Perspective, p. 43 (2014), citing Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980; (C(80)58/FINAL).} The Recommendation also emphasized that member countries should "endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder data flows of personal data."\footnote{Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980; (C(80)58/FINAL).}

The Guidelines were revised in 2013. The fundamental changes introduced by the revised Guidelines relate to implementation and enforcement mechanisms,\footnote{Lee Andrew Bygrave, Data Privacy Law: An International Perspective, p. 44 (2014).} specifically focusing on an approach grounded in risk management, and improving interoperability. New concepts were also introduced in the 2013 revisions, and these pertain to national privacy strategies which place importance on coordination at the highest levels of government; privacy management programs at an organizational level; and data security breach notifications.\footnote{2013 OECD Privacy Guidelines, accessed at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.} However, despite the revisions, the Guidelines are still non-binding. The eight core principles and, to a large extent, their rationale, remain unchanged.

3.3.1.2. The APEC Privacy Framework

The Asia Pacific Economic Cooperation (APEC) arose from an informal meeting of government trade officials,\footnote{Carla Bulford, Between East and West: The APEC Privacy Framework and the Balance of International Data Flows, 3:3 I/S: A JOURNAL OF LAW AND POLICY 706, 707 (2007-08) (citation omitted).} and it represents 21 Member Economies, 6 of which are ASEAN Member States.\footnote{Australia, Brunei Darussalam, Canada, Chile, People’s Republic of China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, The Russian Federation, Singapore, Taipei, Thailand, the United States of America, and Viet Nam.} Collectively, these Economies account for more than a third of the world’s population, over 50% of the world’s GDP, and more than 41% of world trade.\footnote{Johanna G. Tan, A Comparative Study of the APEC Privacy Framework – A New Voice in the Data Protection Dialogue?, Asian Journal of Comparative Law: Vol. 3: Iss. 1, Article 7, 15 (2008).} The APEC notably represents “the most economically dynamic region in the world, having generated nearly 70% of global economic growth in its first 10 years.\footnote{Id.} Its activities are confined to economic concerns, specifically Trade and Investment Liberalization, Business Facilitation, and Economic and Technical Cooperation.\footnote{Id.} The APEC facilitates communication among its member economies about trade and investment in the Pacific Rim,\footnote{Id.} and in doing so, it
ensures that all economies have an “equal say” and decisions are made by consensus.415

This entity is atypical in being an organization of sovereign states because it does not have a constitution, and undertakes commitments on a voluntary basis.416 “APEC ‘agreements’ such as the APEC Privacy Framework do not have any legal status, and are best seen as agreed aspirations, supported by consensus-based commitments to cooperate.”417

Varying domestic privacy laws among the member economies, and economies at different stages and levels of legislative recognition of privacy led the APEC to decide that a regional agreement creating a minimum privacy standard would be the ideal mechanism for facilitating the free flow of data among the member economies (and thus promoting electronic commerce).418 The result was the principles-based APEC Framework, which was written by APEC’s Electronic Commerce Steering Group (ECSG), and adopted in 2004.

It is the result of five years of negotiation among the APEC member economies, with the goal of protecting personal data within the region.419 It is a framework that recognizes “the importance of the development of effective privacy protections that avoid barriers to information flows” and is intended to provide clear guidance to businesses in the APEC region on common privacy issues.420 It is considered “the most significant international privacy instrument since the EU Directive of the mid-1990s.”421

The APEC Framework’s goals are:

vi. to develop appropriate privacy protections for personal information;

vii. to prevent the creation of unnecessary barriers to information flows;

417 Id.
viii. to enable multinational businesses to implement uniform approaches to the collection, use, and processing of data; and

ix. to facilitate both domestic and international efforts to promote and enforce information privacy protections.\textsuperscript{422}

It has four major parts: a Preamble, a section outlining the Framework’s Scope, the Privacy Principles, and a section on Implementation, which is divided into two parts: Part A, which is the Guidance for Domestic Implementation, and Part B, the Guidance for International Implementation.

In its Preamble, the APEC Framework claims to be consistent with the core values of the OECD Guidelines.\textsuperscript{423} It also sets a tone which is prevalent throughout the APEC Framework - that of balancing information privacy with business needs, while giving due recognition to diversities that exist among its member economies.\textsuperscript{424} The Framework’s Scope, on the other hand, aims to clarify the extent of the coverage of the Principles and provides useful definitions. For instance, it defines “Personal information” as “any information about an identified or identifiable individual.” \textsuperscript{425} Its corresponding Commentary section clarifies that the Framework “applies to personal information, which is information that can be used to identify an individual. It also includes information that would not meet this criteria alone, but when put together with other information would identify an individual.”

The central feature of the Framework are its nine Privacy Principles: Preventing Harm, Notice, Collection Limitation, Use of Personal Information Choice, Integrity of Personal Information, Security Safeguards, Access & Correction, and Accountability. Its final part, which deals with implementation, provides guidance to Member Economies on implementing the APEC Privacy Framework. Part A recommends measures Member Economies should consider in implementing the Framework domestically, while Part B provides APEC-wide arrangements for the implementation of the Framework’s cross-border elements.\textsuperscript{426}

The APEC Framework’s non-prescriptive nature could be attributed to the fact that the APEC operates through a system of voluntary compliance, and that its Member Economies are not obligated to transpose the policies

\textsuperscript{422} Carla Bulford, Between East and West: The APEC Privacy Framework and the Balance of International Data Flows, 33 I/S: A JOURNAL OF LAW AND POLICY 706, 709 (2007-08)
\textsuperscript{423} APEC Privacy Framework, Preamble, p.3 http://publications.apec.org/publication-detail.php?pub_id=390 (last accessed on March 16, 2015)
\textsuperscript{425} APEC Privacy Framework, Scope, p. 5.
\textsuperscript{426} Id. at, Implementation, p. 30.
embodied in the APEC Framework into their domestic legislation. Unlike other privacy frameworks, the APEC Framework does not impose treaty obligations on its member economies; consistent with APEC’s approach of relying on non-binding commitments, open dialogue and consensus, the APEC Framework is merely advisory, and accordingly has few legal requirements or restrictions.427

In fact, there are several options for implementing the Framework, including legislative, administrative, industry self-regulatory, or a combination of these.428 It is meant to be effectuated “in a flexible manner that can accommodate various methods of implementation” and it assumes that ways of giving effect to the framework may differ among member economies.429

Considering that seven of the original APEC member economies are also members of the OECD, it is not surprising that the APEC Framework is largely based on the original OECD Guidelines.430 Notable similarities include the following:

The APEC privacy principles address personal information about living individuals, and exclude both publicly available information and information connected with domestic affairs. The principles apply to persons or organisations in both public and private sectors who control the collection, holding, processing or use of personal information. Organisations that act as agents for others are excluded from compliance.431

However, while the APEC Framework is based on the OECD Guidelines, its principles are not identical to those of the OECD’s.432 For instance, it does not have the OECD Guidelines of ‘purpose specification’ and ‘openness,’ although facets of these can be seen within the APEC Framework’s nine principles.433 The APEC principles also allow a wider scope of exceptions, and have slightly more robust guidelines on notice.434

429 Id. at 31.
431 Id.
432 Id.
433 Id.
434 Id.
3.3.2. What are the advantages and disadvantages of the following features and characteristics of the APEC Privacy Framework and the OECD Privacy Guidelines? What are the successes of and challenges involved in the implementation of these features and characteristics?

Keeping in mind this dissertation’s objective, which is providing recommendations as to which features and characteristics are ideal for a potential ASEAN data protection soft law framework, this sub-chapter will look at certain features and characteristics present in the APEC Framework and the OECD Guidelines. Each feature or characteristic will be presented, and their successes, and the challenges encountered with regard to their implementation, will be described. Should the ASEAN embark on its plans of creating a harmonized legal infrastructure for data protection, it would be beneficial to learn from the lessons presented by APEC’s and OECD’s experience with their respective data protection soft law frameworks.

3.3.2.1. National / domestic implementation strategies

3.3.2.1.1. Review of domestic frameworks

In the OECD *Recommendation of the Council on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy* (OECD Recommendation), one of the recommended measures is for countries to “review as needed, and where appropriate adjust, their domestic frameworks to ensure their effectiveness for cross-border co-operation in the enforcement of Laws Protecting Privacy.” In fact, the first step in improving cross-border privacy enforcement for some countries has been to review existing domestic frameworks to determine whether it has sufficient authority to co-operate.

For example, the US FTC continually evaluates its ability to cooperate with international counterparts; for instance, in a previous Report to Congress, it reported on its experiences with the *U.S. SAFE WEB Act*, which provided the FTC expanded authority to cooperate with international authorities on enforcement matters. Another example is the Parliament of New Zealand enacting the *Privacy Cross-border Information Amendment Act*. This empowers the Privacy Commissioner to refer a complaint to an overseas PEA – a term modelled after the OECD Recommendation. This allows the New Zealand Privacy Commissioner to work with other PEAs to help New Zealanders protect

---

437 Id.
their information wherever it is held, ensuring that New Zealand can take full advantage of the mechanisms provided by the APEC Cross-border Privacy Enforcement Arrangement (CPEA) and the OECD Global Privacy Enforcement Network (GPEN).  

Although the OECD recommended a review of domestic frameworks to improve cross-border cooperation among its member countries (which presupposes an existing framework), this type of undertaking is also a practical first step for the ASEAN, when it begins to create a data protection soft law framework for the region. This will allow the ASEAN to:

a) take stock of the existing data protection laws, regulations, and enforcement mechanisms of the 10 Member States;
b) evaluate their advantages and disadvantages, in order to inform the policy-making choices that will be made by the ASEAN in creating a regional framework;
c) find out the gaps in legislation, so that these could be addressed; and
d) if existing laws are found to be adequate, recommend that the other ASEAN Member States model their draft data protections laws after those of Singapore, Malaysia, and / or the Philippines, the ASEAN Member States with existing comprehensive data protection laws.

A periodic review of domestic frameworks is also ideal when a regional framework has already been established, to help ensure that the Member States are implementing and enforcing the necessary local legislation to carry out the ASEAN's data protection goals.

3.3.2.1.2. Establishing Data Protection Authorities / Privacy Enforcement Authorities / Privacy Commissions

The revised OECD Guidelines make explicit the need to establish and maintain PEAs. In the context of the OECD revised Guidelines, a PEA refers not only to those public entities whose primary task is to enforce national privacy laws, but may also extend to regulators with a consumer protection goal, provided they have the authority to conduct investigations or bring proceedings in the context of enforcing data protection legislation.  

A new provision in the revised OECD Guidelines calls on Member countries to establish and maintain PEAs with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions

---

440 Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, p. 28 (2013).
on an “objective, impartial and consistent basis.” It also refers to the need for PEAs to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy.

The need for PEAs is rooted in the necessity of having a government entity primarily responsible for deterring and sanctioning violations of data protection laws, conducting effective investigations, including obtaining access to relevant information relating to possible violations, and prescribing corrective action to be taken against data controllers engaged in violations. In addition, having a government agency with sufficient expertise and resources will expedite rule-making and standard-setting, improve information dissemination, facilitate audit and inspections, enable more efficient cross-border cooperation, and ensure that the agency providing technical assistance to public and private entities possesses the necessary proficiency.

The benefits of having PEAs / DPAs are clear. However, for these authorities to effectively function, their cross-border capabilities must also be maximized. This is due to the increasing volume of cross-border data flows, and the violations that need to be addressed in relation to these flows. Ensuring this is not without its difficulties. A report examining the PEAs / DPAs and the mechanisms that have been established to protect privacy mentions that almost all OECD PEAs / DPAs can act against a domestic data controller in behalf of a foreign individual, but many are limited in or unsure about their authority to protect their own citizens from privacy violations by a foreign controller. A majority express that they would benefit from improved powers to exchange information and perform investigations, either jointly with or at the request of a foreign authority. The same OECD report also avers that “efforts by authorities in the cross-border context are sometimes limited by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints.”

A data protection soft law framework for the ASEAN region should, as is the case with the OECD Guidelines, make explicit the necessity of having PEAs / DPAs in every Member State. Considering the resources that would have to be dedicated to set up a separate agency, Member States should be considered as having followed this recommendation if they designate a government agency,

---

441 Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, Par. 19(c), (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79].
442 Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, p. 28 (2013).
443 Id. at 29.
445 Id.
446 Id.
such as a consumer protection office, that could undertake the necessary responsibilities with regard to data protection.

The establishment of PEAs / DPAs in all ten ASEAN Member States will help ensure that there will be a government entity who will enforce data protection laws, issue the necessary rules and regulations, provide technical assistance, and act as a focal point in cross-border cooperation and enforcement.

However, for these PEAs / DPAs to be truly effective, the laws creating them should not only grant them the usual regulatory functions, such as rule-making and enforcement; it should also bestow upon these entities the necessary powers and authority to cooperate effectively and efficiently with PEAs and DPAs from other countries. With regard to cross-border concerns, PEAs / DPAs should be authorized to engage in information exchange and joint investigations with their foreign counterparts. An ASEAN data protection soft law framework should likewise provide the mechanism through which remedies and penalties could be enforced against an offender in another Member State. This framework should also aim at reducing the inconsistencies in the national data protection regimes of the Member States, in order to further ease cross-border enforcement.

One way to reduce inconsistencies among the national data protection regimes of the Member States is to embark on a hard harmonization project, similar to that undertaken by the ASEAN for its e-commerce legal framework. As mentioned in the previous chapter, hard harmonization projects involve prescriptive information on implementation steps and a timeline. The tools for these projects are geared towards ensuring an orderly, phased development of legal infrastructure harmonization; additionally, they leave less room for interpretation and are intended to reduce inconsistencies. On the other hand, in soft harmonization projects, there is no intention or requirement for countries to adopt the same, or even model laws and regulatory systems. All that is undertaken are training and capacity development activities, aimed at ensuring a common (or harmonized) understanding of legal requirements.

Hard harmonization projects would provide a venue through which the Member States could proactively align their national data protection statutes, in order to facilitate cross-border enforcement of data protection laws. Such a project could also aim to fill in legislative gaps and reduce variances in policy, with the goal of ensuring that enforcement agencies could refer matters to one another, undertake joint investigations, and enforce remedies against offenders located in another Member State’s jurisdiction.

448 Id.
449 Id.
A mechanism allowing cross-border cooperation among Southeast Asian law enforcement agencies exists, and it is embodied in the ASEAN Treaty on Mutual Assistance in Criminal Matters, which provides that Parties must render to one another the widest possible measure of mutual legal assistance in criminal matters, namely investigations, prosecutions and resulting proceedings. The assistance contemplated covers evidentiary matters, service of judicial documents, searches and seizures, production of documents, identifying and tracing instrumentalities of a crime, freezing, recovery, forfeiture or confiscation of property, and location and identification of witnesses and suspects.

This Treaty could be resorted to by ASEAN PEAs / DPAs should the relevant data protection violation constitute a criminal offense. Alternatively, it could stand as a model arrangement for an instrument specifically made for enforcement of data protection laws, should it be found unworkable for that purpose.

3.3.2.1.3. Promotion of legislative approaches

Both the OECD Guidelines and the APEC Framework recommend legislative measures to give effect to their provisions. This recommendation indeed resulted in numerous pieces of data protection legislation across the globe. The Guidelines have been quite influential in countries that had not passed legislation by 1980. In fact, the OECD Guidelines influenced the development of national data protection laws and model codes among the OECD member countries.

For instance, the Australian Privacy Act of 1988 contains 11 Information Privacy Principles, based directly on the Guidelines. The New Zealand Privacy Act, passed in 1993, contains 12 principles, the first four of which all relate to collection, expounding on the OECD’s Collection Limitation and Purpose Specification Principles. Canada’s 2001 private sector legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), requires organizations to comply with ten principles specified in a Model Code, which was incorporated directly into the Act. This Model Code was developed by a committee that used the OECD Guidelines as a starting point. Japan’s Act on the Protection of Personal Information, which came into force in 2005, applies to

---

452 OECD Guidelines, par. 19 (a) and APEC Privacy Framework, Part IV, A. II (31).
453 The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, in the OECD Privacy Framework, p. 77.
454 Id. at 11.
455 Id. at 77.
456 Id.
457 Id.
the collection, use and disclosure of personal data in private businesses that process the personal data of more than 5,000 individuals; this Act also incorporates the OECD privacy principles.\textsuperscript{458} Korea’s \textit{Act on the Promotion of Information and Communications Network Utilization and Data Protection Act} went into effect in 2001. The law was generally patterned after the privacy principles in the OECD Guidelines; it initially applied only to providers of information and communications networks, but later included 14 additional types of businesses.\textsuperscript{459} In 2010, Mexico followed suit and became yet another OECD country to implement the Guidelines through national legislation.\textsuperscript{460} In the same year, Turkey amended its Constitution and gave its citizens additional rights to protect their personal data, addressing issues of consent, use limitation, access and correction.\textsuperscript{461}

It is quite apparent that a regional data protection soft law framework that contains data protection principles, and strategies for implementation, especially one that contains an explicit recommendation to enact legislation, has a great potential to influence the passing of national data protection laws. With more countries that enact data protection laws, more organizations, both public and private, that collect personal data, are obligated to handle this data in accordance with the privacy or data protection principles upon which the legislation is based.

However, with the increasing number of national data protection laws come a few challenges. These challenges include the fact that differences among the laws make compliance demanding for entities with activities in multiple countries; the variance in the manner of their enforcement makes investigations, prosecutions, and pursuing remedies difficult for government agencies and those seeking redress; and the fact that some countries have restrictions on the cross-border transfers of data, while others do not, may unduly restrict the free flow of data which could hamper commerce. The difficulties lie in the fact that data protection can no longer be confined within a nation’s borders, due to the increasing cross-border flows of data. Thus, the issues that arise with regard to cross-border flows of data need to be addressed, but this proves to be challenging due to the differences in national data protection laws.

Yet another challenge is that resorting to legislation in order to promote data protection has inherent weaknesses. These include the fact that because the law is largely reactive, that is, new laws are commonly passed after long periods of deliberation and in response to significant development or change, it

\textsuperscript{458} The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, in The OECD Privacy Framework, p. 77.
\textsuperscript{459} Id. at 78.
\textsuperscript{460} Id.
\textsuperscript{461} Id.
will usually lag behind technology.\footnote{Benjamin J. Goold, Building it In: The Role of Privacy-Enhancing Technologies in the Regulation of Surveillance and Data Collection, in New Directions in Surveillance Privacy, edited by Benjamin J. Goold and Daniel Nyland, p. 19 (2013).} Even if it is assumed that governments intend to have regulatory frameworks in pace with technological advances, new technologies that implicate privacy and data protection concerns continually emerge at such rapid rates, that even the most diligent lawmakers will not be able to keep up.\footnote{Id.}

Another problem with depending on legislation is that imposing legal sanctions is costly and time-consuming; simply providing individuals with a cause of action, for instance, for breach of privacy, is not particularly effective.\footnote{Id at 22.} Litigating potential privacy or data breach cases in order to seek redress involves having to go through the court system, and especially in Southeast Asia, with a majority of these jurisdictions having constantly clogged dockets, this is an unsurprisingly slow process, which will entail significant costs on the part of plaintiffs.

In addition, implementing, administering, and enforcing data protection laws is resource-intensive. Creating rules and regulations to complement legislation is a lengthy process that depends on a body of experts and the participation of various stakeholders; proper regulatory oversight necessitates the deployment of sufficient resources and staff, among other things; and receiving and processing complaints, and ensuring that remedial measures are enforced is a similarly costly endeavor.

Should the ASEAN pursue the creation of a regional data protection soft law framework as a strategy to achieve its goal of having a comprehensive and harmonized legal infrastructure for e-commerce, which has, as one of its components, the promotion of data protection, it should consider the following strategies as possible ways to address the abovementioned challenges:

a) To address the differences among national data protection laws, the ASEAN should pursue a hard harmonization project in order to minimize and narrow the gaps among the Member States’ laws on the subject. The fact that seven out of the ten Member States do not yet have a comprehensive national data protection law is an advantage at this point, since the ASEAN, through a hard harmonization project similar to the one it undertook for e-commerce,\footnote{See Chapter 3 of this dissertation, Section 3.2.4.1 “e-ASEAN Framework Agreement.”} could heavily influence how data protection bills will be drafted in those jurisdictions.

b) Absolute uniformity among the region’s national data protection laws and in the manner of their enforcement is
highly unlikely, considering, among other things, the Member States’ varying legal traditions, governmental structure, and existing procedural or remedial laws. Even a hard harmonization project is not likely to achieve absolute uniformity, although it could minimize gaps and variances. In order to ease cross-border enforcement in light of the differences in procedural laws, the ASEAN should create a mechanism through which enforcement agencies in the Member States could cooperate with each other for purposes of investigating offenses, information-sharing, prosecuting violations, and enforcing remedies. An arrangement similar to that of APEC’s CPEA is a possible model. Through the CPEA, PEAs/DPAs could refer matters, request assistance, notify counterparts in the event of a suspected breach, and coordinate for purposes of investigations and enforcement.\footnote{APEC Cooperation Arrangement For Cross-Border Privacy Enforcement, Section 9, accessed at \url{http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf}.}

Another way to facilitate cross-border enforcement of data protection laws would be to have a mechanism similar to that specified in the aforementioned ASEAN Treaty on Mutual Assistance in Criminal Matters which has, as its goal, ensuring that law enforcement agencies in ASEAN Member States could provide each other mutual legal assistance in investigating and prosecuting various offenses.

c) There is a possibility that there could arise, among the ASEAN Member States, a difference in default regulatory position\footnote{According to Christopher Kuner, in Transborder Data Flows and Data Privacy Law pp. 76-77 (2013): The laws and instruments regulating transborder data flows also differ in the ‘default position’ that they take. Many ... require that personal data may not flow outside the jurisdiction unless a legal basis for the transfer is present, which in some cases requires regulatory authorization. Some others ... generally permit data flows, but give regulators the power to block or limit them in certain circumstances, and require parties exporting personal data to remain accountable or responsible for them once they have crossed national borders.} as regards the cross-border flows of data. Some states could follow a restrictive default position, and others may abide by a more permissive default position. This can unduly hamper or slow down the cross-border transfers of data necessary for certain types of commerce. This is inconsistent with ASEAN’s interests, since it is likely that the ASEAN will advocate for freer cross-border flows of data because of its goal of becoming a single market and production base. To mitigate this, the ASEAN, in its hard harmonization project for data protection, should reach a consensus as to the default regulatory position for the region.
It is submitted that the ideal default regulatory position within the Southeast Asian region is one that allows cross-border flows of data. The model should be one wherein regulations do not require a separate legal basis for cross-border data flows, or routinely subject them to prior regulatory approval or registration. However, data flows should be in accordance with legal requirements applicable to data processing, and regulators should have the authority to suspend them or subject them to conditions in appropriate circumstances.

While the processing of personal data in another country may carry risks, such as when the receiving party fails to provide sufficient security, or when the government is given unhampered access to the data, these hazards are not generally dependent on whether data crosses national borders; poor data security or free access to data by the state can also occur if data are processed locally. Consequently, cross-border data flows should not normally require a distinct legal basis, authorization, or other regulatory the authority to suspend data flows, or subject them to conditions, if necessitated by the risks of specific data transfers. A requirement to notify regulators about certain types of data transfers that are particularly sensitive, such as transfers of sensitive medical or financial information, could also be provided.

While the transfer of personal data to another country deprives them of the protection of national laws, thus making redress for violations more challenging, substantial data protection risks in the form of local data breaches or undue government intrusion, may similarly exist in the home country despite the application of national law. Indeed, as noted by Christopher Kuner, “the risks of data processing in other countries are sometimes exaggerated, while those concerning processing within national borders may be underplayed.” Add to this the fact that so much data flows across borders over the Internet, and it leads one to conclude

---

469 Id.
470 Id.
471 Id.
472 Id.
473 Id at 167.
that it may no longer be necessary to create distinctions between local data flows from cross-border data flows.\textsuperscript{474}

A way to treat national and cross-border data flows equally is to apply the same requirements for these two types of data flows. For instance, if the processing of sensitive medical information necessitates prior approval under national law, then the same requirement should also apply if the same type of information is processed abroad. As Kuner mentioned, “... an extra legal basis or authorization should not be required solely because the data are to be transferred across borders, absent some extra risk factor.”\textsuperscript{475}

Since the ASEAN aims to facilitate freer and easier commerce within the region, requirements such as across-the-board prior regulatory approvals for all types of data transfers should be discouraged. A better solution is encouraging the use of model codes and contracts, arrangements similar to the APEC CBPR, targeted audits, giving regulators stronger enforcement powers, and providing a mechanism through which these regulators can coordinate and cooperate for purposes of investigations, prosecutions, and enforcement of remedies.

Such a model dispenses with the unnecessary distinction between locally and internationally-processed data, encourages and eases cross-border flows of data to generate more commerce among ASEAN Member States, and still provides sufficient protection to data that crosses national borders.

d) Merely depending on legislation as a way to promote data protection is not sufficient. Solutions and measures that could compensate for the weaknesses of legislation – specifically its inability to constantly keep up with technological advances, the costliness and time-consuming nature of pursuing lawsuits, and the expense and resource-intensive nature of enforcement – must likewise be considered. These measures include supporting self-regulation and promoting the use of privacy-enhancing technologies. The following sub-sections will show the benefits of self-regulation, the use of privacy-enhancing technologies, and other strategies and how these complement data protection legislation.

\textsuperscript{474} Id.
\textsuperscript{475} Id.
3.3.2.1.4. Promotion of self-regulation

In addition to encouraging the adoption of appropriate legislation, the OECD Guidelines recommend that member countries encourage and support self-regulation.\textsuperscript{476} Paragraph 19(b) of the OECD Guidelines concerning self-regulation is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action.\textsuperscript{477} The OECD Guidelines have served as a basis for many private sector privacy policies, self-regulatory policies and model codes, and some companies and trade associations have endorsed the Guidelines.\textsuperscript{478} It should also be noted that the APEC Framework provides that self-regulation, by itself or in combination with legislative or administrative methods, could be used to give effect to its provisions.\textsuperscript{479}

Self-regulation is “a regulatory process whereby an industry-level organization (such as a trade association or a professional society), as opposed to a governmental- or firm-level, organization sets and enforces rules and standards relating to the conduct of firms in the industry.”\textsuperscript{480} Industries have resorted to self-regulation in reaction to both the lack of government regulation and the threat of excessive government regulation.\textsuperscript{481}

Self-regulation provides certain benefits. Rulemaking, monitoring, enforcement, and remediation processes can be faster using self-regulation rather than government regulation, which means that consumers are protected sooner.\textsuperscript{482} It has also been asserted that self-regulatory organizations (SROs) can be more effective than government agencies at rulemaking, because when businesses gather to develop rules, those involved are likely to have a higher degree of technical and industry expertise than a government regulator.\textsuperscript{483} On the part of government, regulatory processes, such as rulemaking, monitoring, and enforcement, can be costly and resource-intensive.\textsuperscript{484} SROs can perform these functions, instead of having a government regulator be at the frontlines; this means that complaints can be investigated sooner and disputes addressed faster. According to Daniel Castro, “[t]his benefits government agencies by

\textsuperscript{477} Id.
\textsuperscript{478} The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines, in the OECD Privacy Framework, p. 79.
\textsuperscript{479} APEC Privacy Framework, Part IV (A) (II) (31).
\textsuperscript{482} Id.
\textsuperscript{483} Id at 6.
\textsuperscript{484} Id at 7.
reducing regulatory overload and allowing them to focus their efforts on more productive activities, such as taking action against bad actors that refuse to follow the rules.\footnote{485}{Id.}

Self-regulation also benefits the economy by fostering a more flexible regulatory environment than is usually found with government regulation.\footnote{486}{Id at 6.} Self-regulation involves industry experts reviewing current activities, identifying best practices, and developing these into industry guidelines.\footnote{487}{Id.} Additionally, the guidelines evolve over time in response to feedback from industry leaders.\footnote{488}{Id.} This more flexible regulatory environment may allow firms to operate more efficiently and minimizes compliance costs.\footnote{489}{Id.} Even government regulators themselves have argued that “self-regulation can protect privacy in a more flexible and cost-effective manner than direct regulation without impeding the rapid pace of innovation in Internet-related businesses.”\footnote{490}{Id.}

However, self-regulation has been heavily criticized, especially in terms of not being able to protect consumer privacy. First, it is argued that industry will put their own profits ahead of the public interest; hence, self-regulatory standards will inevitably prove too lenient.\footnote{491}{Dennis D. Hirsch, The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? 34 Seattle U. L. Rev. 439, 458, citing Colin J. Bennett & Charles D. Raab, The Governance Of Privacy: Policy Instruments In Global Perspective 134 (2003).} Second, it is doubtful whether industry representatives, who do not hold governmental power to fine or otherwise penalize violators, possess sufficient authority or incentive to enforce industry standards against their peers.\footnote{492}{Dennis D. Hirsch, The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? 34 Seattle U. L. Rev. 439, 458, citing Bert-Jaap Koops, Miriam Lips, Sjaak Nouwt, Corien Prins & Maurice Schellekens, Should Self-Regulation be the Starting Point?, in Starting Point For ITC Regulation: Deconstructing Prevalent Policy One-Liners 109, 149 (Bert-Jaap Koops, Corien Prins, Maurice Schellekens & Miriam Lips eds., 2006).} Third, it is asserted that self-regulatory processes lack transparency, as opposed to traditional rulemaking, and consequently, public interest will not be adequately represented.\footnote{493}{Id.} Finally, critics worry that without sanctions for non-participants, many businesses will stand by as their competitors institute expensive, self-regulatory standards,
then free ride on the industry’s improved reputation for being privacy-protective.494

It is clear that although self-regulation has its benefits, its disadvantages could not be ignored. Should the ASEAN similarly encourage the use of self-regulation as a tool to promote data protection in the Southeast Asian region, it should ensure that self-regulation is merely a complementary strategy to legislation. Self-regulation, due to its inherent weaknesses, should not replace the enactment of appropriate legislation. However, the benefits of industry participation in the creation of rules affecting their businesses should also be considered. A possible solution is resorting to co-regulation.

Co-regulatory approaches encompass “initiatives in which government and industry share responsibility for drafting and enforcing regulatory standards.”495 Such an approach could involve government and industry trade associations negotiating regulatory goals, collaborating on the drafting of standards, and working cooperatively to enforce the standards against companies that violate them.496

This type of system could co-exist with data protection legislation. For instance, an ASEAN Member State could pass, as recommended by an ASEAN data protection soft law framework, a comprehensive national data protection law. Considering the various sectors and industries that will be affected by such a law, it is foreseeable that this type of statute could not embrace all the necessary data protection rules for all industries, especially those that are highly specialized. The varying levels of sensitivity of the types of information that industries handle, in addition to other factors that make a certain sector’s data processing operations distinct from others, further necessitate specialized rules for specific types of entities. Hence, to complement a national data protection law, government and industry representatives could come together to draft industry-specific rules or legislation.

Both government and industry trade associations could collaborate on setting policy goals and drafting rules or legislation. Furthermore, trade associations could assist government in enforcing these rules and laws by being on the frontlines of receiving complaints and processing remediation. They can then refer to government regulators those matters that need to be escalated, or those issues that could not be resolved at their level. This type of co-regulatory

arrangement ensures that there is industry participation from policy goal-setting to enforcement.

This provides a way through which industry experts could contribute to the creation of rules that will affect their industries. At the same time, government participation will help ensure that these rules are not too lenient or unduly beneficial to business at the expense of the public. As opined by Ira Rubinstein, “firms tend to be more committed to rules that they had a hand in shaping, resulting in increased compliance rates.”

Enforcement will then be improved in two ways: first, industry trade associations will help lessen the burden of government regulators by filtering out those disputes that could be resolved at their level; second, the compulsion to comply with the rules will be stronger, since government is presumably able to impose stiffer fines and penalties against violators. Indeed, co-regulatory arrangements, which unite a self-regulatory mechanism with some type of government intervention, are more robust and effective than self-regulation alone.

This type of arrangement is already being commenced in at least one ASEAN Member State. The Philippines passed its National Data Privacy Act in 2012, and the National Privacy Commission was finally constituted in March 2016. Understanding the complexities involved in regulating the data being processed by the health and medical industries, efforts are now underway to bring together government and industry representatives who will collaboratively draft industry-specific rules and regulations for the processing of data by health and medical firms. These rules and regulations are meant to supplement the country’s comprehensive Data Privacy Act.

3.3.2.1.5. Encouraging the establishment of privacy management programs

The new Part Three of the OECD Guidelines on “Implementation Accountability” introduces the concept of a privacy management program and articulates its essential elements. With the growing amount of personal data that exists, is processed, and is transferred, the risks of data breaches also increase. This emphasizes the need for data controllers, both in the public

---

and private sectors, to implement effective internal mechanisms to protect individuals' personal data.\textsuperscript{501} Data breaches will have a negative effect both on data subjects and controllers; thus, minimizing risks, building and maintaining a good reputation, and ensuring the trust of citizens and consumers is highly important for data controllers in all sectors.\textsuperscript{502} Data controllers must then resort to measures aimed at good data protection governance, while minimizing the legal, economic, and reputational risks they are likely to encounter because of poor practices.\textsuperscript{503} Accountability-based mechanisms aim at delivering these goals, and one such mechanism is the establishment of privacy management programs.

Generally speaking, privacy management frameworks or programs include the policies, procedures, and systems that organizations employ to ensure that personal data is properly protected, risks are managed, and privacy legislation is complied with.\textsuperscript{504} A comprehensive privacy management program provides an effective way for data controllers to communicate to regulators and data subjects that they are compliant. It is also a tool for the companies themselves to find out if they are fully compliant, which gives them an opportunity to remedy their shortcomings. Such a program also helps foster a culture of privacy throughout an organization.\textsuperscript{505} When an organization communicates that privacy is vital to its operations and, in turn, implements a robust privacy management program, that organization will receive enhanced trust from their stakeholders.\textsuperscript{506} “An organization that has a strong privacy management program may enjoy an enhanced reputation that gives it a competitive edge.”\textsuperscript{507} In the longer term, a privacy management program that is appropriate to the organization’s needs will save money and make good business sense.\textsuperscript{508}

Conversely, without strong privacy protection, the levels of trust that data controllers receive may suffer. For instance, privacy breaches are costly for organizations, both in terms of having to remedy their situation and their reputation.\textsuperscript{509} Breaches may also prove expensive for the affected data subjects. An appropriately designed and implemented privacy management program

\textsuperscript{501} Id.
\textsuperscript{502} Id.
\textsuperscript{503} Id.
\textsuperscript{504} The Evolving Privacy Landscape: 30 Years After The OECD Privacy Guidelines, in the OECD Privacy Framework, p. 105.
\textsuperscript{506} Id.
\textsuperscript{507} Id.
\textsuperscript{508} Id.
\textsuperscript{509} Office of the Privacy Commissioner for Personal Data, Hong Kong, Privacy Management Programme: A Best Practice Guide (February 2014).
may help minimize the risk of such breaches, maximize the organization’s ability to identify and address such incidents, and minimize their damage.\textsuperscript{510}

For the reasons provided above, the ASEAN should, in its data protection soft law framework, encourage both public and private data controllers to establish and implement privacy management programs. However, encouraging data controllers to implement a privacy management program is not without its challenges. One challenge is that data controllers might view this endeavor as costly and time- and resource-consuming. Another is that they may not see its value.

The ASEAN should consider an approach employed by the privacy regulators in Canada, Hong Kong, France, Australia and Colombia. These countries have issued “Accountability Guides” or “Privacy Governance Frameworks” intended to assist private sector (and in some instances, also public sector) entities setting up processes and procedures to ensure privacy compliance.\textsuperscript{511} These Guides, if widely publicized and disseminated, could serve the purpose of educating data controllers about privacy management programs and communicating their value. More importantly, since it is a free resource, it is a non-costly way for data controllers to begin establishing their privacy management programs.

The Canadian, Hong Kong, and Colombian Guides all endorse privacy management programs as the proper tool to ensure privacy compliance.\textsuperscript{512} According to the Guides, the two key elements of a comprehensive privacy management program are organizational commitment and program controls.\textsuperscript{513} The guides of these countries outline the necessary features of a privacy management program (such as the appointment of a data protection officer, having internal reporting mechanisms, etc.) and the steps to be undertaken to have a functioning program (like conducting a personal data inventory, setting data protection policies and notices, conducting periodic risk-assessments, adopting a privacy-by-design approach, etc.) In addition, the guides mention that privacy management programs must be continuously assessed and revised.\textsuperscript{514}

The Australian and French privacy regulators likewise issued guidance on the matter, but unlike the Canadian, Hong Kong, and Colombian regulators, they do not explicitly refer to, or promote the implementation of, privacy management programs.\textsuperscript{515} However, the French Standard largely resembles the

\textsuperscript{510} Id.
\textsuperscript{512} Id.
\textsuperscript{513} Id.
\textsuperscript{514} Id.
\textsuperscript{515} Id.
Guides of the three previously mentioned countries.\textsuperscript{516} For example, it includes recommending having adequate internal and external privacy policies, appointing a properly trained data protection officer, training staff on privacy issues, undertaking privacy risk assessments, and the like.\textsuperscript{517} Notably, companies that demonstrate compliance with the 25 requirements of the French Standard will be able to obtain an accountability seal certifying their compliance.\textsuperscript{518}

On the other hand, the Australian Guide provides four steps for organizations to take to ensure they practice good privacy governance and meet their compliance obligations. Generally, these are: embedding a culture of privacy that enables compliance; establishing robust and effective privacy practices, procedures and systems; evaluating privacy processes to ensure continued effectiveness; and enhancing responses to privacy issues, for example, by changing practices in response to evaluation results, considering external assessments, and monitoring and addressing new risks and threats.\textsuperscript{519}

The ASEAN could issue a Guide similar to those described above that is appropriate to the Southeast Asian region. Such a guide should be an essential element of an ASEAN data protection soft law framework. If widely distributed among ASEAN public and private data controllers, it not only communicates the necessity and benefits of having a privacy management program, it is also a cost-efficient way for these data controllers to begin establishing privacy management programs within their respective offices and companies. Considering its proposed regional nature, it will also help standardize the region’s privacy management programs, if widely implemented.

The ASEAN should also consider adopting the French Standard’s system of issuing privacy seals to those entities that have been deemed to meet all requirements. Receiving such a seal boosts confidence in the services and products provided by an organization.\textsuperscript{520} In addition to giving an incentive for successfully complying with all the requirements of an Accountability Guide, the process of gaining a privacy seal also provides an ethical and legal framework for these entities, demonstrates the willingness of the organization to innovate and process personal data responsibly, and helps prepare organizations comply with a regional data protection soft law framework by introducing the notion of accountability.\textsuperscript{521}

\textsuperscript{515} Id.
\textsuperscript{516} A CNIL privacy seal on Privacy Governance Procedures, accessed at https://www.cnil.fr/fr/node/15803.
\textsuperscript{517} Id.
\textsuperscript{518} A CNIL privacy seal on Privacy Governance Procedures.
\textsuperscript{519} Theo Ling, Privacy Accountability: National Regulators’ Accountability Guidance.
\textsuperscript{520} A CNIL privacy seal on Privacy Governance Procedures.
\textsuperscript{521} Id.
3.3.2.1.6. Professionalizing the privacy practice / instituting data protection and privacy law credential programs

Privacy professionals play an increasingly important role in the implementation and administration of privacy management programs. Hence, Paragraph 19(g) of the OECD Guidelines explicitly encourages Member countries to consider adopting measures to support the development of the skills necessary to manage privacy programs. In line with this recommendation, several OECD Member countries have already undertaken initiatives to define the competencies of privacy professionals. Credential programs in data protection and privacy, as well as specialized education and professional development services likewise contribute to the development of the necessary skills.

In some countries, there is a legislative basis to support or encourage the role of the privacy professional. For instance, Germany’s Federal Data Protection Act provides specific requirements for data protection officials in organizations; Canada’s federal private sector legislation, PIPEDA, requires an organization to assign an individual(s) to be accountable for its personal data processing activities; New Zealand’s Privacy Act requires every public or private agency to appoint a privacy officer; and the EU Directive makes reference to a personal data protection official.

Of note is the Canadian Access and Privacy Association Professional Standards and Certification Project (PSCP). It has a stated goal of “establishing Information Access and Protection of Privacy (IAPP) specialists as a recognized profession in Canada.” The project will attain this objective by developing professional standards, establishing a certification model, and by recognizing a governance group capable of implementing the program. From this project came the Canadian Institute of Access and Privacy Professionals (CIAPP) Certification initiative.

The International Association of Privacy Professionals (IAPP) also has a certification initiative. The IAPP was founded in 2000 to define, promote and improve the privacy profession globally. It provides three types of credential

---

523 Id.
524 Id.
525 The Evolving Privacy Landscape: 30 Years After The OECD Privacy Guidelines, in The OECD Privacy Framework, p. 108.
526 Id.
528 Id.
programs, as well as educational and professional development services, and hosts yearly conferences on privacy.

In creating a regional data protection soft law framework for Southeast Asia, the ASEAN should likewise establish privacy specialists as professionals in their own right. The ASEAN could also develop professional standards, establish a certification program (perhaps through the IAPP), and organize a governing body that will be in charge of administering an association for ASEAN privacy professionals. A project that tries to accomplish these will help ensure that there will be accredited privacy specialists certified to manage privacy management programs created in accordance with an ASEAN standard; that these professionals meet a minimum performance standard; and that a governing body will be responsible for further training and educating professionals, creating professional standards, and overseeing compliance with these standards.

Such a regional undertaking is more relevant now, considering ASEAN’s goal of further integrating and liberalizing professional services across the region. This is because a certification will help ease the movement of privacy professionals between Southeast Asian countries. A certification such as that proposed will communicate that an individual is capable of managing privacy management programs across the region. This creates a signal for various Southeast Asian organizations that a person possessing such a certification, regardless of nationality, has the necessary skills to help manage their respective privacy programs. This increases the mobility of privacy professionals within the ASEAN.

The movement of professionals within the region will bridge the surplus and shortage of professionals between countries. It is foreseeable that organizations belonging to the CLMV bloc, especially regional offices of multinational corporations, (which, of late, have been proliferating) will need the services of privacy professionals from the other ASEAN countries, because the privacy profession is not as developed in the former set of countries. The employment of foreign professionals also usually brings new technology, new management skills, and new ideas and can thus help ASEAN countries upgrade their industrial practices. Having a pool of certified privacy professionals within the region will indeed assist organizations as they search for qualified individuals to manage their privacy programs. Such a program, if publicized widely and favorably, could even encourage more individuals to consider a career in privacy and data protection law, once they see the industry’s potential. In a region where privacy and data protection law is at a very nascent stage, such a resource is even more valuable.

531 Id.
3.3.2.1.7. Encouraging the development and deployment of privacy-enhancing technologies

Technical measures also play an increasingly important role in complementing laws protecting privacy. Paragraph 19(g) of the OECD Guidelines encourages measures to foster the development and deployment of privacy-respecting and privacy-enhancing technologies (PETs). There is no one uniform definition of PETs, but generally, they “constitute a wide array of technical means for protecting users’ privacy.” The term also refers to the use of technology to help achieve compliance with data protection legislation.

According to a European Commission briefing paper, common examples of PETs include:

a) Technologies that automatically anonymize personal data after a certain lapse of time, which supports the principle that the data processed should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were originally collected;

b) Encryption tools which prevent hacking when the information is transmitted over the Internet and support the data controller’s obligation to take appropriate measures to protect personal data against unlawful processing;

c) Cookie-cutters, which prevent third parties from placing cookies on the user’s PC to make it perform certain instructions without the user being aware of them; these enhance compliance with the principle that data must be processed fairly and lawfully, and that the data subject must be informed about the processing going on; and

d) Platform for Privacy Preferences (P3P), which allows Internet users to analyze the privacy policies of websites and compare them with the user’s preferences as to the information they allow to release, which helps to ensure that data subjects’ consent to processing of their data is an informed one.

Some of the benefits of promoting the use of PETs are, firstly, restricting the ability of entities and individuals to commit acts that would be considered as violations of data protection laws and regulations. A consequence of this is a

reduction in the instances of breaches, because PETs are designed to make invasions more difficult to carry out.\textsuperscript{535} As opposed to only relying on the imposition of legal rules and sanctions, PETs do not merely focus on modifying the behavior of potential violators; instead, it recognizes that it is necessary to restrict what the technology can accomplish and make it more difficult to commit acts that would lead to violations.\textsuperscript{536}

Secondly, since PETs focus on preventing the commission of unwanted acts by limiting what technology can do, resulting in a reduction of violations, it then follows that PETs likewise reduce the need for costly oversight and complaints procedures.\textsuperscript{537} By building-in privacy in technology, the need for close, independent oversight of their day-to-day use is reduced.\textsuperscript{538} Similarly, if “designing out” unwanted or illegal behavior reduces the number of abuses, the number of genuine complaints that must be dealt with by regulators and the courts is likewise lowered.\textsuperscript{539}

Thirdly, the promotion of the use of PETs forces producers and users of technology to consider the capacity of devices and their legality as inseparable, and thus encourages them to regard privacy-enhancement as a positive aspect of the technology.\textsuperscript{540} By making it a legal requirement for various devices and technologies to have PETs built-in, manufacturers are “forced to confront these issues and negotiate them with their potential customers.”\textsuperscript{541} The expectation is that over time, these values become internalized both into the costs of these products but also in the decision-making of the consumers.\textsuperscript{542} The ultimate goal is to encourage individuals and companies to see technology and privacy as intrinsically linked.

Fourthly, the use of PETs has economic benefits. The principal benefit that could be gained by data controllers is in the form of trust-related or reputational effects.\textsuperscript{543} Indeed, the use of PETs contributes to a positive corporate image and consumer trust, which lead to customer loyalty and increased sales.\textsuperscript{544} Additionally, the security achieved through the use of PETs is a benefit to businesses, insofar as any costs incurred through data breaches

\textsuperscript{535} Privacy Enhancing Technologies, MEMO/07/159, Brussels, 2 May 2007.
\textsuperscript{536} See Benjamin J. Goold, Building it In: The Role of Privacy-Enhancing Technologies in the Regulation of Surveillance and Data Collection, in New Directions in Surveillance Privacy, edited by Benjamin J. Goold and Daniel Nyland, p. 28 (2013).
\textsuperscript{537} See Id.
\textsuperscript{538} Id.
\textsuperscript{539} Id.
\textsuperscript{540} See Id. at 29.
\textsuperscript{541} Id.
\textsuperscript{542} Id.
\textsuperscript{544} Id at 73.
could be reduced.\textsuperscript{545} Better control over data stored by an organization reduces exposure to risk of data loss or breach, with the associated risk of costly legal disputes, fines, and reputational damage.\textsuperscript{546} On a broader level, a general sense of trust and security is beneficial for the further development of online services, including e-government applications.\textsuperscript{547}

However, the ASEAN should recognize that there are challenges and difficulties involved in promoting the use of PETs. The first is that there is a general lack of awareness about PETs, and there is a scarcity of information describing exactly how to deploy PETs; these were significant reasons for their non-adoption in the EU.\textsuperscript{548} Another set of difficulties observed by European DPAs is that the fixed costs of having to employ PETs, staffing and training issues, and its perceived technological complexity limit their deployment and widespread use.\textsuperscript{549} In addition to these is a lack of political imperative to make use of PETs.\textsuperscript{550} It is also interesting to note that both EU consumer and business associations revealed that the refusal of customers to pay for PETs, and consumer acceptance of current privacy and data protection risks and arrangements, were disincentives for the deployment of PETs by businesses.

Should the ASEAN encourage the use of PETs as a complementary measure to legislation and co-regulation to promote data protection across the region, it should seek ways to address the aforementioned challenges. Possible solutions could begin with a dialogue between regulators and businesses, in order to raise awareness and educate stakeholders about the risks to and means of protecting personal information. This dialogue should inform businesses of the value and necessity of using PETs, the various types of PETs that could be deployed, and cost-effective means of deploying them. Regulators should also provide advisory services and issue guides on PETs to businesses, in order to slightly lower the costs involved in deploying them. These advisory services and regulatory guides could be a regional effort sponsored by the ASEAN, so that the Member States could pool their resources and lower costs. Regulators should also look into the possibility of requiring certain data controllers, such as those who collect and process highly sensitive personal information, to deploy PETs.

Regionally, Member States may choose to support the development of technical standards that advance privacy principles. International standardization initiatives could advance technical interoperability among

\textsuperscript{545} Id at 72.
\textsuperscript{546} Id.
\textsuperscript{547} Id at 73.
\textsuperscript{548} Id at 76.
\textsuperscript{549} Id at 75 and 76.
\textsuperscript{550} Id at 75.
PETs, which may in turn help promote wider adoption of these technologies.\textsuperscript{554} Accreditation and seal programs may further foster the adoption of technologies beneficial to privacy. Other measures include the promotion of research and development and exchange of best practices.\textsuperscript{552}

3.3.2.1.8. Having Member States report on their domestic implementation of the framework’s recommendations

The APEC Framework has its Member Economies report on the domestic implementation of the Framework through the completion of and providing periodic updates to Individual Action Plans (IAPs) on Data Privacy.\textsuperscript{553} Data Privacy IAPs were envisioned to improve the transparency of the data protection frameworks of the APEC economies, which in effect will enable other economies to be informed of the relevant stage that an economy has reached.\textsuperscript{554} This is in line with the overall objective of the APEC Framework to encourage the development of common effective privacy protections and ensure the free flow of information in the region.\textsuperscript{555}

The term “reporting and monitoring obligations” is used broadly to encompass any process or practice, whether formal or informal, that gathers and shares information about whether or to what extent an obligation has been (a) complied with, in the sense of substantive compliance, or (b) implemented, in the sense of formal compliance.\textsuperscript{556} This practice yields various positive results, although its goals are typically not punishing non-compliance (though it could reveal instances of non-compliance), but assisting states to improve and enhance compliance with treaty obligations.\textsuperscript{557}

A study conducted by Simon Chesterman\textsuperscript{558} on ASEAN monitoring and reporting obligations illustrates five purposes or results of these types of obligations. First is assessing substantive compliance, which is linked to the evaluation of success in achieving a specified outcome; second is assessing compliance, with a focus on the establishment of a national agency or enactment of local legislation, (as opposed to focusing on the effectiveness of

\textsuperscript{553} Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, P. 32 (2013).
\textsuperscript{555} Id.
\textsuperscript{556} APEC Privacy Framework, Part iv (A) (vi) (39).
\textsuperscript{558} Id.

555 Paul C. Szasz, Administrative and Expert Monitoring of International Treaties, p. 15.
the measures taken in achieving a stated purpose); **third** is providing an authoritative and clear interpretation of obligations; **fourth**, the facilitation of long-term implementation through confidence-building and information transfers; and **fifth**, which is an expression of unity among Member States with regard to a certain issue.

As regards the first purpose, monitoring and reporting obligations drive Member States to reveal and demonstrate whether and how they implemented measures to achieve certain policy goals. Measuring compliance would be easier, however, if the policy goals are highly specific and clear, as opposed to vague and general. This is a common pitfall in ASEAN Agreements, since they are intentionally vague in their objectives, often framed in the language of promotion and cooperation, rather than the attainment of clear goals.\(^{559}\)

As for the second purpose, formal compliance is most easily established when an Agreement requires objective procedural steps to be taken, such as the creation of a government agency or adoption of legislation.\(^{560}\) However, a commonly observed weakness not only in the ASEAN, but also in the APEC, is the lack of a concrete consequence in instances of non-compliance. This, however, is inevitable among organizations that, by their nature, are unable to enforce compliance with obligations through sanctions.

However, reporting and monitoring obligations, especially those with a peer review mechanism such as APEC’s Data Protection IAP, exerts peer pressure insofar as members respect one another’s views and provide forthright opinions and critique.\(^{561}\) Indeed, peer pressure should not be discounted as a way to encourage or compel substantive compliance.\(^{562}\) In addition to the respect members have for each other’s views, another factor is the public nature of the review: publicly-shared data on compliance is more likely to influence Member State behavior due to the incentives and benefits they may receive because of being recognized as compliant. For instance, complying with data protection frameworks boost a Member State’s reputation among possible investors who are interested in ensuring that the personal data they may want to have processed in another country is kept secure. Hence, in the absence of an organization’s ability to sanction non-compliance, mechanisms that have the effect of shaming or pressuring members in the event of non-compliance, or putting them in a good light should they be found compliant, could be a viable substitute for compelling compliance through the threat of punishments.


\(^{560}\) Id at 65.

\(^{561}\) Id. at 61.


The third purpose of monitoring and reporting obligations is to help clarify the obligations of Member States. When Member States publicize their manner and method of compliance, and the international organization to which they are reporting approves or does not object, other Member States are informed of what measures they could implement in order to be similarly considered as having complied, and what measures might be deemed insufficient. Also, in the event that the monitoring mechanism somehow includes adjudicatory bodies with enforcement powers, an adjudicatory body can authoritatively pronounce whether, in case of a dispute, a Member State has complied with its obligations. This then apprises other Member States as to what constitutes compliance or non-compliance.

The fourth purpose of monitoring and reporting obligations which pertains to facilitation of long-term implementation through confidence-building and facilitating information transfers is fulfilled by the act of Member States' publicly sharing their experiences in trying to achieve the international organization's stated policy goals. Other Member States can then learn from their neighbors' experiences – they can adopt those measures that yielded positive results, and they will likely avoid those that were not effective. Constantly updating a shared, public database will result into a rich resource from which other countries can learn.

The fifth purpose is minor, as compared to the others, yet in showing a united front on an issue, an international organization can help shape the perception of outsiders. The benefits of demonstrating unity with regard to a certain issue such as data protection, is merely reputational.

Despite the usefulness of monitoring and reporting obligations, specific challenges and weaknesses are present. One challenge to ensuring that monitoring and reporting obligations help achieve policy goals is the lack of specific, measurable goals. Should the ASEAN resort to monitoring and reporting obligations as one way to promote data protection in the region, it should not rely on vague, general policy goals. It should outline specific steps and measures for its Member States to follow, compliance with which will warrant recognition and certification that the Member State successfully implemented national measures to advance the goals of the ASEAN data protection soft law framework. In advancing the goals of an ASEAN data protection soft law framework, the ASEAN should avoid its common pitfall of resorting to vague standards such as “promoting” and “encouraging” greater cooperation, and the like. It must propose specific, measurable goals with a set timetable so that compliance by a Member State can be easier determined.

Another challenge to monitoring and reporting obligations is constantly keeping the reports updated. A cursory glance at the APEC Data Protection IAP
database\textsuperscript{564} would reveal that only 14 out of the 21 Member economies submitted IAP reports. Out of these 14, six last updated their reports in 2006, and the rest sent their last updates between 2009 and 2015. In the ASEAN, this feature will only be maximized if all participating countries submit reports and make regular updates. In addition to reports on compliance with basic requirements specified in an ASEAN data protection soft law framework, periodic updates containing items such as significant data protection complaints and cases, enforcement measures, new rules, regulations, and industry standards, emerging PETs, developing issues and challenges, helpful research and publications, and other pertinent developments would also be useful.

A weakness of the APEC Data Protection IAP project is that there seems to be no independent assessment as to whether the Member economies complied with the APEC Framework. The APEC makes no pronouncement regarding the progress of a Member economy in terms of implementing the suggested measures of the APEC Framework, and neither does it recommend remedial courses of action in cases of noncompliance. Should the ASEAN adopt this monitoring and reporting feature, it should go beyond collecting and publishing its Member States’ reports. It should, after considered analyses, make assessments as to the States’ levels of compliance, and suggest remedial measures in cases of noncompliance.

3.3.2.2. International implementation strategies
3.3.2.2.1. OECD’s Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy

In 2007, the OECD Council adopted a Recommendation setting forth a framework for cross-border cooperation in the enforcement of privacy laws, based on the findings of a 2006 enforcement report. The framework embodied in the Recommendation reflects a commitment by governments to improve their domestic frameworks for data protection law enforcement to better allow their authorities to cooperate with their foreign counterparts, as well as to provide mutual assistance to one another in the enforcement of data protection laws.\textsuperscript{565}

Although primary responsibility for implementation of the Recommendation rests with member country governments and their PEAs, there is also a role for the OECD to facilitate some aspects of implementation.\textsuperscript{566} In particular, some of the most significant provisions of the Recommendation relate to collective activities, including the collection of contact points, sharing

\textsuperscript{566} Id at 8.
information on outcomes, and fostering the establishment of an informal network of PEsAs.\textsuperscript{567} Other notable features include provisions for requesting assistance from foreign counterparts and fostering stakeholder dialogue.

The Global Privacy Enforcement Network (GPEN) is an inclusive cooperation network, open to any public PEA that: (1) is responsible for enforcing laws or regulations the enforcement of which has the effect of protecting personal data; and (2) has powers to conduct investigations or pursue enforcement proceedings.\textsuperscript{568} Its goal is to foster cooperation among PEsAs, and it primarily seeks to promote cooperation by: exchanging information about relevant issues, trends and experiences; encouraging training opportunities and sharing of enforcement knowhow, expertise, and good practice; promoting dialogue with organizations having a role in privacy enforcement; creating, maintaining, and supporting processes or mechanisms useful to bilateral or multilateral cooperation; and undertaking or supporting other specific activities.\textsuperscript{569}

Its notable accomplishments include the GPEN Alert - a new information-sharing system that will enable PEsAs to better coordinate efforts in protecting consumer privacy; the Network of Networks project, which facilitates communication beyond the immediate GPEN community and the exchange of knowledge, experience and best practices to leverage combined strengths; consolidating a list of enforcement contacts for APEC, Council of Europe and the OECD, with facility for addition of enforcement contacts from other networks in future; an Opportunities Board featuring employment, secondment, and training opportunities, which allows GPEN member authorities to share various opportunities with GPEN users from other DPAs; and various workshops and training programs.\textsuperscript{570}

Aside from the establishment of the GPEN and the GPEN’s programs, another noteworthy feature of the OECD’s cross-border enforcement efforts is the Request for Assistance Form. The OECD Working Party for Information Security and Privacy (WPISP) developed a Request for Assistance Form for use by PEsAs to help ensure that certain basic categories of information are provided to the authority receiving the request for assistance.\textsuperscript{571} The process of completing the Form also helps guarantee that the requesting authority has first conducted its own preliminary investigation or consideration of the matter, before seeking assistance from foreign counterparts.\textsuperscript{572} The Form has been adapted by authorities from APEC economies, and is indeed a useful step

\textsuperscript{567} Id.
\textsuperscript{568} 2015 Global Privacy Enforcement Network (GPEN) Annual Report, p. 4.
\textsuperscript{569} Id.
\textsuperscript{570} See 2014 and 2015 Global Privacy Enforcement Network (GPEN) Annual Reports.
\textsuperscript{572} Id.
towards ensuring compatible processes between OECD and APEC, particularly for PEAs from countries that are members of both organizations.\(^{573}\) 

An ASEAN data protection soft law framework could adopt these measures in order to facilitate cooperation among the PEAs, or agencies that perform the tasks usually performed by PEAs, in the region. The ASEAN, in coordination with the region’s PEAs, could similarly engage in information exchange, facilitating dialogue among stakeholders, training programs, providing avenues through which the Member States could enter into bilateral or multilateral arrangements, and more importantly, a mechanism that will allow the region’s PEAs to request assistance from each other. This could be done through the creation of a formal network of Southeast Asian PEAs. Similarly, a Request for Assistance form that helps ease the process of asking for aid in relation to cross-border enforcement of data protection laws would be beneficial for the region’s PEAs. In order to maximize the benefits that could arise from the use of this form, it should likewise be compatible with similar Forms being used by the APEC and OECD.

Nevertheless, in adapting measures similar to those specified above, the ASEAN should take note of the following challenges. One is that PEAs will find difficulty in cooperating with foreign counterparts if they are not equipped with the necessary powers and authority to do so.\(^{574}\) Another difficulty in cross-border cooperation among PEAs is the existence of legal limitations on the ability of PEAs to share information with foreign authorities, with some OECD countries reporting a legal barrier or lack of clarity on the matter.\(^{575}\) An additional problem is the general lack of resources to engage in cross-border enforcement, with some PEAs being required to investigate all complaints they receive, leaving little time and resources to dedicate to cross-border cooperation.\(^{576}\) Finally, another complication that must be dealt with by the ASEAN, should it adopt a cross-border enforcement mechanism similar to that being used by OECD’s GPEN, are unclear, conflicting, or inexistent policies on seeking and enforcing redress, and the ability to use judgments, court orders, and evidence obtained abroad.

A possible solution lies in a hard harmonization project that will recommend that all PEAs in the Southeast Asian region should possess the power and authority necessary to enable them to cooperate with their foreign counterparts. This power and authority should clarify the process through which PEAs could cooperate with each other, the extent and limitations of this authority, the requirements and safeguards which would allow PEAs to responsibly share necessary information with foreign counterparts, and the government agency that could adjudicate matters regarding this authority.

\(^{573}\) Id.  
\(^{574}\) Id at 5.  
\(^{575}\) Id.  
\(^{576}\) Id.
As for the lack of resources that PEAs may have to grapple with, a way to help ensure that there will be more resources that could be allocated to cross-border enforcement efforts is to reduce the number of complaints that would have to be processed by the PEAs. As previously mentioned, co-regulation could reduce the number of complaints that would have to be processed by PEAs, since SROs could assist in receiving complaints and settling disputes. SROs would then only refer to PEAs those complaints and disputes that they could not settle, resulting in a decrease of complaints and disputes to which PEAs have to allocate resources.

With regard to the unclear, conflicting, or inexistent policies on seeking and enforcing redress and the ability to use judgments, court orders, and evidence obtained abroad, the ASEAN could use, for purposes of cross-border enforcement of data protection laws, the ASEAN Treaty on Mutual Assistance in Criminal Matters, which states that Parties are to render to one another the widest possible measure of mutual legal assistance in criminal matters, namely investigations, prosecutions and resulting proceedings.577 The assistance contemplated covers evidentiary matters, service of judicial documents, searches and seizures, production of documents, identifying and tracing instrumentalities of a crime, freezing, recovery, forfeiture or confiscation of property, and location and identification of witnesses and suspects.578 This treaty could provide legal bases for seeking assistance with regard to criminal violations of data protection laws. Should the violations not be criminal in nature, a similar arrangement, but adapted to non-criminal offenses, is a viable solution.

3.3.2.2. APEC Cross Border Privacy Rules and the APEC Cross Border Privacy Enforcement Arrangement

The APEC Cross Border Privacy Rules (CBPR) System is a voluntary accountability-based system to facilitate privacy-respecting data flows among APEC economies.579 It requires businesses to develop their own internal privacy-based rules governing the transfer of personal data across borders under standards that meet or exceed the APEC Privacy Framework.580

However, before a business may participate in the System, its home country, which must be an APEC member economy, must first “have laws and regulations... the enforcement of which have the effect of protecting personal

578 Id. at Article I (2).
information consistent with the APEC Privacy Framework.\textsuperscript{581} The CBPR Joint Oversight Panel (JOP) issues a Findings Report on each member country's application to participate. However, this is not a process by which an independent body makes a substantive determination that the member economy indeed has a law which meets the APEC Framework standard; it is more akin to a requirement that the applicant economy submits a 'self-assessment' that it does meet the required standard.\textsuperscript{582} As of this writing, there are only 4 participating member economies: the United States, Mexico, Japan, and Canada.

The CBPR System consists of four elements: (1) Self-Assessment, (2) Compliance Review, (3) Recognition or Acceptance and (4) Dispute Resolution and Enforcement.\textsuperscript{583} In order to comply with the CBPR System, organizations must first conduct a Self-Assessment of their data protection policies, in comparison with the APEC Privacy Framework. This is done with an APEC-recognized questionnaire.\textsuperscript{584} The completed questionnaire and any associated documents are then submitted to an APEC-recognized AA for review.

The AA then conducts the Compliance Review, to ensure that the organization does not fall below the minimum CBPR program requirements.\textsuperscript{585} If compliant, APEC will certify the organization, and the organization will be eligible for Recognition/Acceptance.\textsuperscript{586} Under this third element, the organization's business details will be published in an APEC-hosted website for consumers and stakeholders to reference.\textsuperscript{587} Finally, Enforcement and Dispute Resolution is administered through the Cross-Border Privacy Enforcement Authority (CPEA).\textsuperscript{588}

The CPEA provides a multilateral mechanism though which PEAs can share information; cooperate by referring matters to each other and conducting parallel or joint investigations or enforcement actions; and share information

\textsuperscript{582} Id. at 531-532.
\textsuperscript{583} http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPRPoliciesRulesGuidelines.ashx
\textsuperscript{584} Id.
\textsuperscript{585} Id. See also, APEC Cross-Border Privacy Rules System Program Requirements, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPRProgramRequirements.ashx
\textsuperscript{587} Id.
\textsuperscript{588} Id.
and cooperate on privacy investigation and enforcement, even with PEAs outside APEC.  

3.3.2.2.2.1. Advantages and Successes of the APEC CBPR and CPEA System

Presenting the advantages and successes of the APEC CBPR and CPEA will help the ASEAN evaluate whether certain features and characteristics of these arrangements might be similarly beneficial for the Southeast Asian region, should it adopt its own data protection soft law framework. The benefits are classified into three categories: benefits to government stakeholders, business stakeholders, and regulators.

3.3.2.2.2.1.1. Government Stakeholders

3.3.2.2.2.1.1.1. A baseline set of privacy standards

Some APEC economies, such as Mexico, India, the Philippines, Singapore, and Uruguay, have significant interests in services that handle large amounts of personal data from other economies, such as call centers and other services like data processing and analytics that handle financial information and human resources data; hence, having data transfer arrangements and protections in place is important. According to Annelies Boens and Michael Crompton, “[t]he CBPR System contributes to supporting the advancement of global trade and economic growth by providing a scalable baseline set of privacy standards.”

A system such as the CBPR helps assure foreign businesses that a company based in a member economy has privacy policies that meet an internationally-recognized standard. For instance, Argentina gaining EU adequacy has led to significant growth in its data service industry. Should the ASEAN adopt a similar system, a business based in an ASEAN Member State (especially a country which is not an APEC member economy) would have the opportunity to claim that its privacy policies meet an internationally-recognized standard. This, in turn, would bolster its reputation as being able to adequately protect the data of individuals, and thus be more attractive to potential investors, both within and outside the ASEAN.

---

591 Id.
592 Id.
This benefit being available to ASEAN businesses would pre-suppose the following: a) that an ASEAN data protection soft law framework, and its accompanying cross-border data protection rules, would gain recognition as a standard worthy of being made the basis of a company's data protection policies; b) that all ASEAN Member States would have data protection legislation; c) that all ASEAN Member States would have PEAs / DPAs, or in the alternative, an existing government agency specially tasked to enforce data protection laws; and d) that the ASEAN will have a mechanism similar to APEC's CPEA, through which Southeast Asian PEAs / DPAs could cooperate with each other, and with PEAs / DPAs outside the region, for purposes of referring matters and coordinating enforcement efforts.

3.3.2.2.2.1.1.2. International cooperation

The CBPR System, as a regional data protection tool for the Asia Pacific, can potentially make connections with other international data protection frameworks, including in the EU. This is made possible by the work on connecting the APEC CBPR System and EU Binding Corporate Rules (BCR) System through a common referential, which is “an informal pragmatic checklist for organizations applying for authorization of BCR and/or certification of CBPR.”

The referential facilitates the design and adoption of personal data protection policies compliant with each of the systems. It lists in a single document the main elements generally required by national DPAs in the EU, and by the relevant bodies in APEC economies, in privacy policies submitted for authorization as a BCR in the EU in accordance with data protection laws applicable in EU Member States, and/or as a CBPR in accordance with rules applicable in APEC Economies.

Although absolute uniformity and harmonization of data protection legislation across the entire globe is far from easily achievable, projects such as the APEC-EU referential eases the compliance demands in a global environment with a patchwork of data protection laws. This tool is recognized as a response to the clamor for a more streamlined global privacy regime, and is a major step towards a framework that narrows the existing gaps in policies on cross-border data transfers. Perhaps the biggest benefit of this tool, which

---

593 Id.
595 Id.
596 Id.
maps out the rules that cover many of the major economies of the world, is it helps “businesses figure out how to adopt one policy framework that can be used on a global uniform basis to cover the most risk in the most territories while they wait for a uniform set of rules.”

Should the ASEAN undertake efforts similar to the APEC-EU referential, it would help companies conducting business in the region, and with partners in Southeast Asia, navigate through the complexities of data protection requirements in the ASEAN region and in the Asia Pacific and/or the EU. A tool that will increase awareness of the data protection requirements in the different major economic regions of the globe would make compliance easier by mapping out the various requirements, and by lowering costs and increasing efficiency for businesses who would otherwise have to grapple with numerous and varying national requirements.

A way to further ease the burden of complying with numerous data protection requirements all over the globe is for the ASEAN to propose to the APEC and the EU that it join the existing referential, once it has created its own data protection soft law framework. This would require the ASEAN data protection soft law framework to have a feature similar to the APEC CBPR and the EU BCR systems. With this in mind, the ASEAN should consider not deviating significantly from the requirements of the EU BCRs and the APEC CBPRs. In doing this, the ASEAN could contribute to narrowing the existing gaps in data protection requirements for businesses across the globe.

3.3.2.2.1.2. Business Stakeholders
3.3.2.2.1.2.1. Trade Benefits

The CBPR System increases the privacy protection offered by participating businesses in economies where there is no data protection law, while not diminishing privacy protection in economies where there is data protection law with which businesses must comply. This is because in countries without applicable data protection laws, a business, in joining the CBPR system, commits to complying with the minimum baseline privacy standards set by the APEC. And since joining the CBPR presupposes that there is a regulator that can enforce compliance with the CBPR program requirements, businesses transacting with a CBPR-certified enterprise are not only assured of compliance with an internationally-recognized set of privacy standards and rules, they are also assured that enforcement can be had against an erring business. Privacy protections are not diminished in economies with data protection laws, because businesses that join the CBPR system are still expected to comply with their national data protection laws.

---

598 Id, quoting Field Fisher Waterhouse partner, Phil Lee.
Businesses exporting data, and individuals using their services, would be more confident exporting to economies without data protection laws, if enterprises in those member economies are CBPR participants, because of the guarantees provided by the system: that of compliance with APEC privacy standards, and availability of enforcement measures. Likewise, businesses importing data from economies with national data protection laws are more likely to be attractive data recipients, if they participate in the CBPR system, because of the same guarantees.

These justifications are especially applicable to the ASEAN region, where, at present, only three Member States out of ten have comprehensive data protection laws. Should the ASEAN adopt a system similar to the CBPR before all ten ASEAN countries have data protection legislation, benefits could already accrue in favor of enterprises in ASEAN countries, in the form of increased trust in their data protection policies from potential investors. This would have to presuppose that there are regulators that can enforce the ASEAN’s version of CBPRs. These could be consumer protection agencies, or information and communication ministries, either of which is present, in one form or another, in all ASEAN Member States. Although the goal of the ASEAN is to ensure that all Member States have data protection laws, and although it would be ideal for all Member States to have DPAs, this would take a considerable amount of time and resources. In the meantime, as more companies are looking to outsource data processing to Asian countries, a CBPR-like system for the ASEAN would be able to provide some assurance to those potential investors. That assurance is that a business that joins an ASEAN system similar to that of the CBPR complies with a baseline standard of data protection policies, and these policies could be enforced by a government regulator against the enterprise.

3.3.2.2.1.2.2. Organizational benefits

3.3.2.2.1.2.2.1. One global compliance system

The APEC region is diverse, with numerous varying cultures. As mentioned by Moens and Crompton in their research on the APEC CBPR System, “[h]aving a common set of baseline standards which are interpreted in the same way can help overcome cultural differences that would otherwise make cross-border data transfers even more complex.” Businesses with regional and global operations could benefit from a simplified compliance system if they could adopt one standard for all their operations. This has the potential benefit to end user privacy of having resources that are focused on better privacy instead of complex layers of compliance. Furthermore,
regional frameworks that can be integrated with other similar frameworks make this process easier. 604

ASEAN implementing an arrangement similar to that of the CBPR would greatly help regional and global businesses operating in the region, since they could adopt one standard for all their operations in Southeast Asia. This would lead to lower costs and increased efficiency, in terms of creating and enforcing data protection policies, since they could rely on a single, regional standard. This presupposes that all ASEAN Member States will join a CBPR-like system for its region, and that businesses based in these countries, which have significant cross-border data flows, apply for certification and acceptance to this system.

To avoid a situation wherein a business with global operations would encounter difficulty in having to grapple with two or three systems which all have, as a common goal, facilitating privacy-respecting data flows, a possible solution would be, as previously mentioned, the ASEAN joining the APEC and EU referential system. It is argued that, since having a harmonized data protection framework which covers all global regions is an exceedingly ambitious and difficult endeavor, projects that attempt to streamline various regional efforts which facilitate privacy-respecting data flows is a positive development that would, in the meantime, assist businesses attempting to navigate through a patchwork of varying data protection laws.

3.3.2.2.1.2.2.2. Assurance and Trust

The CBPR System operates on an external validation model with AAs (which can be public or private sector entities) that ascertain whether requirements for the certification have been fulfilled, and a PEA / DPA that can enforce the requirements of the System. 605 This provides a level of assurance to external stakeholders, such as consumers, users, and potential business partners, that a business which bears CBPR certification complies with an internationally-recognized privacy standard, with regard to its data protection policies. It also communicates that enforcement measures are available in cases of breach.

Should the ASEAN pursue a similar program, it could provide businesses based in the region with a way to assure consumers and potential partners that they comply with a particular privacy standard, and that the latter have a way to seek redress in cases of breach because of the available enforcement measures. However, as asserted by Moens and Crompton, for trust levels to increase, consumers need to recognize the significance of a certification, see it across a wide number of businesses, and experience the

604 Id.
benefits, such as better complaint-processing and better management of their personal information. Business-to-business trust levels could also increase when businesses transact with certified businesses, on the presumption that those enterprises understand the value of the certification and deem it important.

3.3.2.2.1.3. Regulator Stakeholders - Improved strategic resource allocation

The CBPR System can potentially assist PEAs in focusing their efforts and resources on systemic, high profile, and high impact privacy issues, instead of being on the frontlines of receiving and handling complaints, since Accountability Agents (AAs) can take on this task. Efficient and effective complaint handling by an AA can lower the workload of PEAs to enable them to focus their efforts strategically.

Assuming that an ASEAN data protection soft law framework would call for the establishment of PEAs in each Member State, this abovementioned benefit could redound to Southeast Asian PEAs if an ASEAN system patterned after the CBPR ensures that designated AAs are able to receive and process complaints effectively. In the case of a non-PEA government entity performing the functions of a PEA, the value of an AA would be heightened, since having an AA would lessen the data protection-related complaints that a non-PEA government agency would have to handle. This is because an AA could be at the frontlines of receiving and processing complaints. It need only refer to PEAs (or entities performing the functions of a PEA) those complaints that it could not resolve.

Having an AA for each ASEAN Member State is highly unlikely, considering the lack of existing companies in the region that could fulfill an AA’s role. A possible solution is for the ASEAN to establish an office within the Association, that could take on the tasks of reviewing applications, compliance assessment, issuing certifications, receiving complaints, and referring matters to the proper national government entities which could handle enforcement. Alternatively, the ASEAN could accredit a private entity that could perform the functions of an AA, and could process and approve applications for organizations based in any Southeast Asian country.

---

607 Id at 17.
608 Id.
3.3.2.2.2. The disadvantages and weaknesses of and the challenges involved in implementing the APEC CBPR System

A discussion of the APEC CBPR System’s disadvantages and weaknesses, and the challenges that it faces, will be useful for the ASEAN, should it contemplate adopting a similar system. Knowing these possible pitfalls will alert the ASEAN to undertake the necessary measures to improve upon a system that could operate in a similar manner.

3.3.2.2.2.1. Lack of transparency and public participation

It has been observed by Graham Greenleaf that there is no provision for external inputs as to whether there are substantial objections to a proposed AA approval. \(^{609}\) There are no procedures to invite written inputs, or to make the public aware that deliberations on this matter are being undertaken. \(^{610}\) In addition, company policies are to be regarded by AAs as confidential, with regard to the procedure wherein an AA verifies an applicant company’s self-assessment of its compliance with the CBPR program requirements. Hence, as Greenleaf noted, there is no mechanism through which external parties can verify, either before or after certification, that a company accurately stated its policies to obtain certification. \(^{611}\)

A possible solution to this complaint would be for the ASEAN, should it implement a CBPR-type system, to provide a mechanism through which the public could express their objections to a proposed AA approval. The ASEAN would then have to publish, perhaps through a website, that a company has applied for accreditation, and it would also have to publish the company’s self-assessment, its corresponding data protection practices and policies, and other pertinent documents. It is argued that a company applying for certification should, in general, not be able to have their data protection practices and policies considered confidential. This is because stakeholders, such as potential consumers and business partners, should be able to ascertain for themselves whether a company indeed complies with the necessary requirements for certification. Barring any laws that grant confidentiality to data protection practices and policies, such as laws on intellectual property, wherein certain aspects of a company’s operations should be kept confidential for trade secret or patent law justifications, a company applying for certification should disclose their pertinent data protection practices and policies.

\(^{610}\) Id.
\(^{611}\) Id at 533.
A criticism against the CBPR is that currently, AAs do not cover businesses in all sectors of the economy. For example, in the US, the Federal Trade Commission (FTC) is currently the only relevant PEA, but it does not have jurisdiction over the health and non-profit sectors, and some areas of the financial services industry.\(^\text{612}\) Hence, these types of enterprises cannot as yet be part of the CBPR System, and TRUSTe, the CBPR accountability agent in the US, cannot be an AA for these sectors.\(^\text{613}\)

The situation is similar in Japan. Its Ministry of Economy, Trade, and Industry (METI) established the Japan Information Processing Development Center (JIPDEC), the CBPR AA for Japan; hence, its scope is limited to that covered by METI, which excludes the telecommunications and health sectors.\(^\text{614}\) Thus, in Japan, pending implementation of the amended data protection law, its AA only covers the sectors within its responsibility, as covered by METI.\(^\text{615}\) However, once the amendments come into effect, and the Japanese PEA obtains jurisdiction over all sectors, the AA will also have the ability to certify businesses in all sectors.\(^\text{616}\)

Should the ASEAN adopt a CBPR-like system as part of its regional data protection efforts, its system’s AA, (which, as previously suggested, could be one that is established by the ASEAN itself, or a private enterprise designated by the ASEAN, with the authority to issue certifications for businesses based in any Southeast Asian country) should be able to certify all sectors that engage in cross-border data transfers. However, this presupposes that there is, in every Southeast Asian government, an agency or multiple agencies, which has / have the ability to enforce the relevant remedies against various types of businesses that transfer personal data across national borders.

An ASEAN CBPR-like system should thus equip its AA with the ability to refer matters, not only to Southeast Asian PEAs / DPAs, but also to other government agencies tasked with enforcing national data protection laws. Southeast Asian PEAs / DPAs, or various government agencies, taken together, should ideally have jurisdiction over all enterprises that engage in cross-border data transfers. These agencies must, of course, possess the authority to receive and handle complaints, and to impose remedial actions, which may take the form of issuing warnings, demanding compliance, and imposing penalties.

---

\(^{612}\) Annelies Moens and Michael Crompton, Preliminary Assessment: Potential Benefits for APEC Economies and Businesses Joining the CBPR System, p. 16 (2016).

\(^{613}\) Id.

\(^{614}\) Id.

\(^{615}\) Id.

\(^{616}\) Id.
3.3.2.2.2.3. Confusion with regard to the implications of the certification

In the CBPR System, the AA does not certify that the company complies with local data privacy laws of the economy concerned, only with its CBPR requirements.\(^{617}\) Hence, a consumer, through a CBPR certification, will not know if a CBPR-compliant company is in fact ‘law abiding’.\(^{618}\) For less discerning consumers who are not well-versed in data protection laws, a certification such as that provided by the APEC CBPR System might cause confusion, or even a false sense of security.

In the ASEAN, a possible solution could come in the form of a disclaimer on the certified company’s website. This disclaimer should communicate that a certification issued by the ASEAN’s designated AA only certifies that the company complies with ASEAN data protection standards, but it does not necessarily certify that the company complies with the relevant national data protection laws. A disclaimer such as this one gives adequate notice to one who wishes to know about a company’s compliance with data protection laws that an ASEAN certification does not serve to guarantee a company’s compliance with national data protections laws.

3.3.2.2.2.4. Fine-print exclusions

Some APEC CBPR members, as Chris Connolly, Graham Greenleaf, and Nigel Waters pointed out, “use fine print in their privacy policies to exclude certain activities, such as mobile applications and cloud services, from their APEC certification.”\(^{619}\) APEC stated that this behavior is allowed under the CBPR rules, and that the same ‘scoping’ issue occurs in the EU US Safe Harbor.\(^{620}\) However, these fine print exclusions have a tendency to mislead consumers who may see a prominent APEC certification logo on a website, but would unlikely look for the exclusions that are buried in a lengthy document located in another part of the visited website.\(^{621}\)

Should the ASEAN allow similar exclusions, any certification logo that will be placed by a company on its website should have a prominent feature that would alert consumers to the fact that the certification it received from the ASEAN AA excludes certain activities. This would prompt a concerned consumer to look for the exclusion, which should be clearly and prominently stated, in layman terms, in an easily-accessible section of the company’s website. A policy such as this would reduce the likelihood of a consumer being

\(^{617}\) APEC CBPR System-Policies, Rules and Guidelines (APEC, undated), para. 45.
\(^{620}\) Id.
\(^{621}\) Id.
misled about the limited nature of the ASEAN certification received by a company.

### 3.3.2.2.2.2.5. Issues with accountability agents

A civil society submission to the Joint Oversight Panel (JOP) of the APEC CBPR System pointed out deficiencies in the application of TRUSTe as a CBPR AA. These include the observation that TRUSTe’s program standards or requirements failed to meet at least 21 of APEC’s program requirements (for instance, the requirement that access to personal information must be provided within a reasonable time was missing, and the requirement that correction should be provided within a reasonable time was likewise missing); that it restricted monitoring and certification to online activity, although APEC’s criteria required all activity to be monitored; and that there are conflicts of interest, since TRUSTe was certifying companies where the target company had the same owners and directors as TRUSTe. These criticisms seriously undermine the credibility of the CBPR System.

Although a new set of program requirements released by TRUSTe in January 2015 already extended the program to all personal data collection, rather than restricting it to online data collection as it had in the past, and the new requirements also corrected omissions pertaining to access and correction requirements, the other defects remain.

ASEAN should take sufficient measures in ensuring that the entity that will issue certifications complies with all program requirements, and that conflicts of interest are avoided. A previously mentioned suggestion is worth reiterating here – instead of relying on private companies to issue certifications, the ASEAN should consider the viability of establishing an office within the Association that performs functions similar to those of an AA in the APEC CBPR System.

An entity attached to the ASEAN will more likely comply with ASEAN-specific program requirements, since it does not have preexisting generic program requirements upon which to rely – note that TRUSTe initially used its own existing generic program requirements in its application for AA status. It was only after civil society intervention that TRUSTe was compelled to develop and publish APEC CBPR-specific program requirements. It addition, an ASEAN entity will more likely comply with program requirements because it is under the supervision and control of the Association.

---

Should the existence of such an office be infeasible, an alternative would be for the ASEAN to accredit AAs that could issue certifications for businesses operating anywhere within Southeast Asia. However, in doing so, ASEAN should ensure that any AA that it accredits complies with the program requirements, and that AAs have sufficient internal safeguards in place to prevent any conflict of interest from occurring.

3.3.2.2.2.6. Lack of APEC-wide certification

A common criticism against the APEC CBPR system is that its certification has no effect on the same company in its operations in other APEC economies. Indeed, according to Greenleaf, “[c]ertification would need to be obtained separately in each country to which data was to be transferred.” If a company that wishes to be APEC-CBPR compliant across the region operates in several APEC economies, this lack of an APEC-wide certification is inconvenient and time and resource-consuming.

Considering ASEAN’s plans for regional economic integration, and its goal of becoming a single market and production base, it should consider making its certifications region-wide. A regional certification could attest that a company’s data protection policies and practices across its operations in Southeast Asia complies with the ASEAN’s program requirements. A system like this encourages companies to standardize their data protection policies across the region. This also encourages compliance with a minimum standard; for companies based in countries that do not yet have data protection laws, a system that offers accreditation on a regional basis, depending on a company’s compliance with ASEAN’s program requirements, will at least have a minimum standard with which to comply – that of the ASEAN’s.

A region-wide certification is also convenient and efficient, since a company that presumably standardizes its data protection policies and practices across Southeast Asia need not exhaust additional time and resources in order to be ASEAN-certified in every country in which it operates within the region.

This would be more feasible, considering that the ASEAN could potentially have one or several entities, whether an attached ASEAN office, or a private company, issue certifications that could cover the entire region, instead of having to rely on AAs operating in each country that could only issue certifications for companies operating in that Member State. This could lead to greater participation in the system by companies because of its increased convenience, and the higher value of an ASEAN certification that covers all 10 Southeast Asian Member States.

626 Id.
In sum, considering the APEC CBPR System’s successes and weaknesses, for ASEAN governments, businesses, regulators, and consumers to enjoy the possible benefits that could accrue from a similar system being implemented in Southeast Asia, a similar certification system would need the following features and characteristics:

a) an ASEAN data protection standard deemed adequate and robust enough by stakeholders to truly protect consumer interests;

b) an AA deemed credible by regulators, businesses, and consumers;

c) PEAAs / DPAs (or government agencies that could perform the tasks usually undertaken by these entities) in each Southeast Asian country;

d) Government regulators that, taken together, are able to enforce data protection laws against all sectors that engage in cross-border transfers of personal data;

e) a transparent certification system which allows regulators and the public to verify, or ascertain for themselves, whether the business applying for, or given a certification, indeed complied with all the necessary requirements;

f) a seal that makes clear that certification does not necessarily mean compliance with all national data protections laws, but only compliance with the ASEAN’s data protection standards, and, if necessary, this certification should communicate any exclusions;

g) an “ASEAN-wide” certification; and

h) an accessible mechanism for filing and following-up complaints.

3.4. Chapter Conclusion

The conditions are ripe for policy convergence on data protection within Southeast Asia. Because of ASEAN’s strong tradition of eschewing legally binding and enforceable commitments, it is highly likely that the data protection legal structure that will emerge in the region is soft law in character. The need for regulatory flexibility increases the likelihood that the resulting legal structure for the ASEAN will take the form of a framework, which will set diffusely formulated and general rules, instead of a set of highly-detailed and specific provisions. The increasing cross-border transfers of data has given ASEAN policy makers the signal to ensure that this data protection soft law framework will address concerns regarding the conduct of states with and among each other, and the conduct of private parties involved in cross-border transactions, in relation to the gathering, registering, storing, use, and
dissemination of personal information. An international data protection soft law framework is inevitable for Southeast Asia.

This inevitability demands that existing international data protection soft law frameworks such as the OECD Privacy Guidelines and the APEC Privacy Framework be studied so that lessons can be drawn from them. These lessons should help inform the discussions that could lead to a similar framework for Southeast Asia.

These lessons reveal that there are certain features and characteristics that are likely to yield positive results in terms of promoting data protection within a region, if included in international data protection frameworks, and if implemented properly. Some of these features and characteristics are provisions that call for measures such as a review of domestic data protection law frameworks, establishing PEAs / DPAs / Privacy Commissions, promoting legislative and co-regulatory approaches, encouraging the establishment of privacy management programs, professionalizing the privacy practice, encouraging the deployment of PETs, and having Member States report on the domestic implementation of these measures for monitoring purposes.

In implementing these, the Member States would benefit greatly if resources are shared, the ASEAN sets specific, measurable goals with a set timetable, and if a hard harmonization project is first undertaken. This hard harmonization project should, among other things, minimize and fill in legislative gaps, ensure the enactment of policies that will authorize PEAs to coordinate with and among each other, and create a mechanism that will facilitate the coordination of PEAs with regard to cross-border enforcement of data protection laws. It should also be a venue through which the Member States could settle on a default regulatory position as regards cross-border data transfers; ideally, this default position should be one wherein regulations do not require a separate legal basis for cross-border data flows, or routinely subject them to prior regulatory approval or registration.

Other implementation strategies include information exchange, providing avenues through which Member States could enter into bilateral or multilateral law enforcement arrangements, and an accreditation system that would certify whether ASEAN businesses joining this system are fully compliant with its data protection standards, and provides easily-accessible enforcement measures, should those companies later be found non-compliant.

As a result of the discussions in this chapter and the one previous to it, the ideal features and characteristics of an ASEAN data protection soft law framework will be presented systematically and described in more detail in the following chapter.
4. The Ideal Features and Characteristics of an ASEAN Data Protection Soft Law Framework

Chapter Five Outline

5.1 Chapter Abstract
5.2 An ASEAN Data Protection Agreement
   5.2.1 Matters of form
      5.2.1.1 Clear and precise objectives and specific goals
      5.2.1.2 Provides flexibility in the means to be used to attain the objectives and goals
      5.2.1.3 Seeks compatibility and interoperability with existing data protection soft law frameworks
      5.2.1.4 Comprehensive and consolidates related instruments
      5.2.1.5 Specifies and provides different deadlines
      5.2.1.6 Has Implementation Guides and Checklists
   5.2.2 Matters of substance / Measures to Promote Data Protection in the ASEAN Region
      5.2.2.1 Encourage the use of Privacy-Enhancing Technologies
      5.2.2.2 Encourage the establishment of Privacy Management Programs and publication of Accountability Guides
      5.2.2.3 Makes provisions for the professionalization of the privacy practice
      5.2.2.4 Provides for a system of reporting and monitoring
      5.2.2.5 Provides a venue for participation of various stakeholders
      5.2.2.6 Regular meetings and reviews of the Agreement
5.3 An ASEAN data protection standard deemed adequate and robust by stakeholders
5.4 Information Network Features
   5.4.1 Establishing a network of Data Protection Authorities
   5.4.2 Providing technical assistance, training, and capacity building for regulators, law enforcement, legislators, and judges
5.5 Undertaking a Hard Harmonization Project: Working through Harmonization Networks and Tools
   5.5.1 Having Data Protection Authorities Participate in Harmonization Efforts
   5.5.2 Begin with a review of domestic frameworks
   5.5.3 Facilitate the enactment of harmonized data protection laws through model laws
   5.5.4 Encourage the development of comprehensive legislation instead of sectoral laws
   5.5.5 An interim measure: voluntary model codes
5.6 Enforcement Network Features
   5.6.1 Independent Data Protection Authorities equipped with the necessary powers and functions to cooperate on cross-border matters
   5.6.2 Encouraging the development of a system of co-regulation
   5.6.3 Looking into jurisdictional matters over data protection offenses
   5.6.4 An improved Cross Border Privacy Rules System
5.7 Chapter Conclusion

130
4.1. Chapter Abstract

The objective of this chapter is to present the ideal features and characteristics of an ASEAN data protection soft law framework, drawing from the lessons learned from ASEAN’s experience with soft law instruments, and APEC’s and OECD’s experiences with their respective data protection soft law frameworks. Chapter 3 presented which types of measures recommended by, and which features and characteristics of ASEAN soft law instruments are likely to lead to the attainment of the policy goals specified in these instruments. Chapter 4, on the other hand, showed the advantages and disadvantages of certain features and characteristics of the APEC Privacy Framework and the OECD Privacy Guidelines. It also delved into the successes of and challenges involved in the implementation of these features and characteristics. This chapter is the product of the observations and analyses made in Chapters 3 and 4.

This chapter begins by describing the instrument that could embody an ASEAN data protection soft law framework (sub-chapter 5.2). It first presents matters of form (sub-chapter 5.2.1), and then provides features or mechanisms that could increase the Agreement’s effectiveness (sub-chapter 5.2.2). It then discusses the data protection standard that could be used as the foundation of this framework (sub-chapter 5.3), which is in the form of a set of privacy or data protection principles. The chapter, drawing lessons from previous ASEAN experience with various soft law instruments, and the experience of the OECD and APEC in implementing their data protection soft law frameworks, then goes on to describe additional measures, features, and characteristics that could be recommended or possessed by an ASEAN data protection soft law framework in order to effectively promote data protection in the region (sub-chapters 5.4 – 5.6).

The latter part of the chapter is structured according to Anne-Marie Slaughter’s conception of government networks in a New World Order. Hence, there will be brief discussions on harmonization networks, enforcement networks, and information networks. Measures, features, and characteristics, in addition to those provided in the earlier sub-chapters, that are best suited to each type of government network, will be described together under their respective categories.

4.2. An ASEAN Data Protection Agreement

It is likely that ASEAN will resort to the signing of an Agreement to carry out their stated objectives of promoting data protection, ensuring that all ASEAN Member States have legislation in line with regional best practices and regulations in e-commerce activities, including data protection, and having a harmonized legal infrastructure for e-commerce, also with an emphasis on data protection. The Association commonly adopts this approach in order to address the need for providing the basis for the Member States’ cooperative efforts.
This Agreement will be the foundation of an ASEAN data protection soft law framework, in the same way that other ASEAN Agreements served as the bases for regional cooperative efforts on matters the Association deemed important and necessary to address.

Since an ASEAN Agreement on Data Protection (the title this dissertation will use for the soft law instrument ASEAN will likely enact to achieve the above-mentioned goals) is a significant element of the region’s data protection soft law framework, it is worth evaluating the features it would ideally possess.

When people speak of the effectiveness of an international instrument, such as an Agreement, it can mean, among other things, the Agreement’s ability to attain its goals, “that is, it has solved the problem that prompted its creation.” It relates to whether the instrument is able to cause States and/or individuals to modify their behavior in the “right” direction – that is, towards achieving the Agreement’s objectives.

In assessing an Agreement’s effectiveness, it is crucial to understand that these international instruments serve different functions and must be measured against different standards of effectiveness. Regulatory agreements, which seek to regulate the behavior of States, businesses, or individuals, are said to be effective if they result to actual changes in the behavior of the regulatory target. According to Daniel Bodansky, in his work on the effectiveness of international agreements, framework agreements, seek to establish a “general system of governance for an issue area, in order to facilitate the development of consensus about the relevant facts and the appropriate international response.” Bodansky elaborated, saying that “[t]o the extent that a framework convention affects the behavior of States or individuals, it does so indirectly, by facilitating the development of regulatory protocols through changes in attitudes, values and beliefs.” Assessing the effectiveness of these agreements is more difficult and is a long-term effort. Aspirational agreements aim to change the attitudes of States and individuals about what is right and wrong, and what is acceptable and unacceptable.

An ASEAN Data Protection Agreement should aim to serve all three of these functions. At a minimum, it should have sufficient moral weight, expressing the ASEAN’s concerns about the importance of promoting data

---

627 The full definition of this term is provided in Chapter 4, Section 4.2.1.1.2 of this dissertation.
629 Id.
630 Id. at 27.
632 Id. at 27.
633 Id.
protection within the region. It should also establish a framework for further action by establishing basic institutions, and laying out specific measures that work towards achieving its policy goals. Finally, it should also seek to change or direct the behavior of States, businesses, and individuals – for example by providing mechanisms for enforcement, rewarding compliance, complaint-filing, and seeking redress. These are what the Agreement, and ultimately, an ASEAN data protection soft law framework, seeks to accomplish.

Although the effectiveness of international legal instruments depends on a multitude of factors, two of these factors are the design of an agreement, or its form, and its substantive contents. This subchapter is thus divided into two: the first one focuses on those matters of form, while the second one provides specific measures that could be undertaken in order to pursue the Agreement’s overall objective of promoting data protection in the ASEAN region.

4.2.1. Matters of Form

4.2.1.1. Clear and precise objectives and specific goals

Clear and precise objectives and specific goals are more likely to largely influence the behavior of States than ambiguous or vague ones. To the extent that States want to comply with international commitments, clear and precise objectives and goals communicate what is expected of them. The international agreements that have had greatest effect on States’ behavior have tended to be those with very precise obligations; on the other hand, vague or ambiguous expectations are unlikely to affect behavior.

For instance, ASEAN’s ATIGA clearly spells out that Member States shall eliminate import duties on all products traded between the Member States by 2010 for ASEAN-6 and by 2015, with flexibility to 2018, for CLMV. Each Member State was expected to reduce and/or eliminate import duties on originating goods of the other Member States in accordance with specified rates and schedules. This degree of specificity eased compliance and the corresponding assessment of such compliance, because the expectations for each Member State were clear and unambiguous.

---

634 See Id at 37.
637 Id.
638 ASEAN Trade In Goods Agreement, Article 19.
639 “ASEAN-6” refers to Brunei Darussalam, Indonesia, Malaysia, the Philippines, Singapore and Thailand.
640 “CLMV” refers to Cambodia, Lao PDR, Myanmar and Viet Nam.
641 ASEAN Trade In Goods Agreement, Article 19 (2).
Indeed, even a State that means to comply with its obligations is unlikely to change its behavior significantly if the expected result is unclear and is subject to differing interpretations. As Bodansky asserted, “understandably, [states] will adopt the interpretation that requires the least change in its behavior. Failure to achieve a clear, precise goal, in contrast, is more difficult to rationalize.”

4.2.1.2. Provides flexibility in the means to be used to attain the objectives and goals

Exacting specificity and clarity of the goals and objectives to be attained, however, is immensely different from specificity of the means to be used to achieve those goals.

Kenneth Bamberger and Deirdre Mulligan, in their article Privacy on the Books and on the Ground, argued that “[r]ules are notoriously both under- and over-inclusive, identifying certain relevant factors that can easily be codified, while ignoring others.” In fact, specific rules often cannot reflect the numerous variables involved in working towards achieving complex regulatory goals, such as reducing the types of risk produced by a combination of factors. Drawing analogies with the economics of contracts identifies “problems with complete contracting—attempting to fully articulate terms ex ante— in situations of complexity and uncertainty.” In such instances, an instrument’s terms should be left vague or unspecified, while delegating future decisions about how to resolve imprecision to the contracting parties that will, at the proper time, have best access to relevant information.

As observed by Bamberger, “the past two decades have seen widespread experimentation with regulatory requirements framed in terms of broad principles rather than precise rules, which create greater ambiguity regarding appropriate methods of compliance.” Indeed, policymakers have relied increasingly on general mandates instead of specific requirements in an attempt to address the complexity of the public goals at issue. Moreover,

---

643 Id.
recent studies suggest flaws in privacy regimes that only rely on highly specified and proceduralized behavioral mandates.\textsuperscript{650} Bamberger & Mulligan cite a multidisciplinary report reviewing the European Union’s Data Protection Directive, which found that a focus on specific mandated process “risks creating an organisational culture that focuses on meeting formalities to create paper regulatory compliance (via check boxes, policies, notifications, contracts, . . . ), rather than promoting effective good data protection practices.”\textsuperscript{651}

Their article\textsuperscript{652} cites the Federal Trade Commission’s approach that offers a model “in which regulatory ambiguity may provide a space within which regulators can play a more active role in catalyzing the field’s development of legal meaning.” In particular, its course places an emphasis on dynamism and collaboration, specifically, the regulator’s ability to draw recurrently from “experience at the relatively local level” and changing challenges as they arise, in order to “continually . . . update the standards all must meet,”\textsuperscript{653} and the regulator’s capacity to “harness[] the power of new technologies, market innovation, and civic engagement to enable different stakeholders to contribute to the project of governance.”\textsuperscript{654}

These are perhaps the reasons why ASEAN avoids mandating specific means in its Agreements, but rather resorts to Implementation Guides drafted in cooperation with various experts and stakeholders from the Member States. These Implementation Guides do suggest specific measures, but allow for flexibility in their implementation. In addition, these Implementation Guides are subject to periodic revision and review, again in conjunction with stakeholders. This then allows for input from those more directly involved in the national implementation of the Agreement, and similarly allows or even expects revisions to be made, in accordance with current national conditions and prevailing necessities.

Such an approach would then be ideal for an ASEAN data protection soft law framework: an Agreement that provides specific objectives and goals, yet allows flexibility in the means to achieve those goals; and accompanying this Agreement is an Implementation Guide which suggests various measures which may be undertaken locally in order to achieve those goals, this Guide being subject to periodic revision or re-issuance, as dictated by new developments, capabilities, and needs.

\textsuperscript{650} Id. at 307.


\textsuperscript{652} Id. at 308.

\textsuperscript{653} Id. citing Michael C. Dorf, The Domain of Reflexive Law, 103 Colum. L. Rev. 384, 384 (2003) (reviewing Jean L. Cohen, Regulating Intimacy: A New Legal Paradigm (2003)).

\textsuperscript{654} Id. citing Orly Lobel, The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought, 89 Minn. L. Rev. 342, 343-344 (2004)
4.2.1.3. Seeks compatibility and interoperability with existing data protection soft law frameworks

It is expected that an ASEAN Agreement on Data Protection would be compatible with existing international data protection soft law frameworks. This is due to ASEAN’s objective to have a regional economy that is largely integrated and compatible with the rest of the globe. This objective is rooted in the desire to encourage and increase commerce with countries outside the region. Consequently, ASEAN Member States would want to ensure that their legal infrastructure would be compatible with international developments. Having significant commonalities among data protection frameworks would help governments, businesses, and individuals navigate through the patchwork of data protection laws across the globe, thus making compliance easier for stakeholders. Absolute uniformity and harmonization among the existing national data protection laws is a lofty goal that will likely not be achieved in the near future. However, a global system of regional frameworks that reduce gaps, inconsistencies, and conflicting policies will greatly contribute to making the global data protection law environment more navigable for those who wish to comply with various laws and different frameworks.

Recall how the ASEAN drafted its definition of “terrorist offense” in its Convention on Counter-Terrorism by including offenses defined as such by 14 other counter-terrorism treaties. It did this to ensure that its definition is comprehensive, and to comply and be consistent with other international initiatives. Doing something similar for an Agreement on data protection, that is, taking steps to make certain that significant definitions are comprehensive and take into consideration the definitions provided by other frameworks, will help increase consistency among data protection frameworks.

Another example worth noting is that of the APEC-EU referential, a tool that facilitates the design and adoption of personal data protection policies compliant with each of the systems. The ASEAN should consider taking efforts to join this referential, in order to help ease compliance for those stakeholders who wish to comply with all three frameworks.

An additional way of increasing compatibility with other data protection frameworks is by adopting their various data protection or privacy principles. Considering that the OECD Guidelines and the APEC Framework are usually regarded as low standards, the ASEAN could consider looking at the privacy principles being adopted in Europe, especially if certain ASEAN Member States are considering seeking EU recognition, with regard to having adequate

---

data protection, for purposes of facilitating data flows. A more detailed discussion on this matter is in the next sub-section.

Indeed, an Agreement that provides for concrete steps to seek compatibility and interoperability with other data protection frameworks, through the means provided here and elsewhere, would be greatly beneficial in reducing the costs of complying with various national data protection laws, easing enforcement, and increasing secure cross-border data flows.

4.2.1.4. Comprehensive and consolidates related instruments

A feature that made the ATIGA more user-friendly for those seeking to comply with its provisions is that it consolidates all related policies in one comprehensive instrument. As such, one who needs to know about this Agreement’s rules and regulations, procedures, standards and required measures need not look further than the Agreement and its annexes. Such an instrument would indeed ease compliance.

The ASEAN should thus ensure that when it releases an Agreement in line with its data protection soft law framework, all the necessary policies and implementation guides are contained in a single instrument, with references to any related instruments.

4.2.1.5. Specifies and provides different deadlines

Another feature of an ideal ASEAN agreement is that it recognizes the different levels of institutional capacity and available resources among Member States. This is why Agreements such as the ATIGA provide for two deadlines. In the ATIGA, all Member States were expected to issue a legal enactment to give effect to the implementation of the tariff liberalization schedules in the ATIGA. However, the ASEAN-6 had a deadline of 90 days from the date the ATIGA entered into force to comply with this requirement, while the CLMV bloc were given 6 months to comply. The ASEAN, in doing this, recognized that the former set of countries had more resources and the necessary institutional capacity to comply with this requirement sooner, as opposed to the latter group of countries.

The ASEAN should then consider having two deadlines for its Member States to fully comply with the various provisions of its data protection Agreement; an earlier deadline for the ASEAN-6, and a later deadline for the CLMV. This will even allow the ASEAN-6 to provide technical assistance to the CLMV in the drafting of data protection legislation, rules and regulations, and in the setting up of the necessary national institutions that will carry out these policies.

---

656 ASEAN Trade in Goods Agreement, Art. 21 (1) (a).
4.2.1.6. Has Implementation Guides and Checklists

Essential to the success of an Agreement are Implementation Guides and Checklists designed to direct ASEAN officials and the relevant officials of Member States as they enact the measures necessary to achieve the Agreement’s goals. In the ASEAN, these guides and checklists specify the specific measures that may be taken by the Member States in order to help ensure the attainment of the goals in the Agreement to which it is attached.

In the same way that the ASEAN Handbook on International Legal Cooperation in Trafficking in Persons Cases was designed to be part of a collection of tools and resources aimed at strengthening national and regional responses to trafficking in persons, in line with the objectives of the ASEAN Declaration Against Trafficking in Persons Particularly Women and Children, a Handbook or Implementation Guide would also be a useful tool that will aid in carrying out the objectives of an Agreement on data protection.

In the same vein, checklists could also be used to help ensure that the measures necessary to achieve the desired goal of promoting data protection in the region are in place. Checklists were used by the ASEAN in their e-commerce hard harmonization project, and it guided both ASEAN and country officials in determining which measures must be implemented, and what stage, to attain their desired result. This also helps the ASEAN evaluate the levels of compliance in the region, and whether the Member States are on schedule in implementing the Agreement.

4.2.2. Matters of Substance / Measures to Promote Data Protection in the ASEAN Region

This subchapter specifies a few features that should also be considered for inclusion in an ASEAN Agreement on Data Protection, because they have demonstrated effectiveness in achieving ASEAN policy goals in the past, or because they aided in the promotion of data protection elsewhere.

4.2.2.1. Encourage the Use of Privacy-Enhancing Technologies

The use of Privacy-Enhancing Technologies (PETs), as discussed in the previous chapter, has been shown to help achieve compliance with data protection laws. PETs, by restricting the ability of entities and individuals to commit acts that would be considered as violations of data protection laws and regulations, serve as effective preventive tools. By focusing on preventing the commission of unwanted acts by limiting what technology can do, the use of PETs result in a reduction of violations, in turn, likewise reducing the need for costly administrative oversight.657 Two other benefits are fostering a general

---

657 See Benjamin J. Goold, Building it In: The Role of Privacy-Enhancing Technologies in the Regulation of Surveillance and Data Collection, in New Directions in Surveillance Privacy, edited by Benjamin J. Goold and Daniel Nyland, p. 28 (2013).
attitude of considering privacy as being intrinsically necessary to a product or service, and the reputational gains that could come from being regarded as privacy-respecting.

By encouraging the use of PETs in its data protection Agreement, the ASEAN will send a clear message to its Member States that legislation is not sufficient to promote data protection in the region. Complementary measures, such as encouraging, or even requiring the use of PETs will contribute to having a more holistic approach to data protection.

4.2.2.2. Encourage the establishment of Privacy Management Programs and publication of Accountability Guides

A comprehensive privacy management program has been shown to be an effective tool in helping a company protect the personal data they process, manage risks, and comply with data protection laws and regulations. Such a program instills a culture of privacy throughout an organization. However, implementing a privacy management program could be hampered by the view that it is costly and time- and resource-consuming, and has little value or relevance to the company.

As such, should ASEAN consider encouraging the establishment of privacy management programs in companies and institutions across Southeast Asia, it should endeavor to publish an Accountability Guide, similar to those released by privacy regulators in Canada, Hong Kong, France, Australia and Colombia. These Guides, if widely publicized and disseminated, could inform data controllers about privacy management programs and their value. More importantly a free Accountability Guide is an affordable solution for data controllers who wish to begin building privacy management programs.

In addition, incentivizing the full implementation of an Accountability Guide, perhaps by giving compliant companies an accreditation, could be an effective way to increase the number of entities who would attempt implementing their own privacy management programs. Moreover, having an ASEAN Accountability Guide that could be used across the region would have a standard-setting and harmonizing effect on the data protection practices and policies among those entities who would be using it as a guide in starting their own programs.

---

4.2.2.3. Makes Provisions for the Professionalization of the Privacy Practice

With the necessity of privacy management programs come the need for people to manage these programs. In the US and EU, “corporate structures frequently include direct privacy leadership, in many instances by C-level executives. The individuals managing corporate privacy have an applicant pool of trained professionals to draw from. There is ongoing training, certification, and networking.”\(^659\) This shows the emergence of a community of corporate privacy managers.\(^660\)

Such an emergence, at a similar scale, has not yet occurred across Southeast Asia. However, with increasing foreign investments, multi-national corporations setting up shop in various cities across the region, businesses that automatically process data locally and transfer data internationally, and a trend of data protection laws being enacted, the need for trained and accredited privacy professionals will likely increase in the years to come. Hence, it will be prudent for ASEAN to anticipate this by taking steps to professionalize the privacy practice in the region.

The ASEAN could begin by developing professional standards and establishing a certification program (perhaps through the IAPP), and organizing a governing body that will be in charge of administering an association for ASEAN privacy professionals. Facilitating the flow of privacy professionals from one Southeast Asian jurisdiction to another, first by establishing a pool of these professionals, and then connecting them with enterprises in need of their services, will bring new technology, methods, management skills, and ideas on improving the company policies and practices of various entities in the region, and can thus help ASEAN businesses collectively upgrade their privacy management programs.

4.2.2.4. Provides for a System of Reporting and Monitoring

Requiring Member States to submit regular reports on the status of their implementation of the Agreement on a national level can promote effectiveness in several ways. The most apparent is to facilitate evaluation of a Member State’s performance, which in turn promotes transparency.\(^661\) Assuming that Member States are less than forthright, country reports can aid in the evaluative process by providing a focal point for NGOs, intergovernmental bodies, and other observers to assess the information provided and to comment on it.\(^662\) Even incomplete or poorly-analyzed data could give observers and

---


\(^{660}\) Id.


\(^{662}\) Id.
stakeholders the necessary information that they can use in their own analyses of policy options and compliance.\textsuperscript{663}

In addition, reporting requirements force Member States to, at the very least, examine the level and quality of their compliance with an agreement and can help in bringing about changes in policies and practices. As observed by Paul Szasz, the agency that prepares the national report must gather the data, and in doing so reminds the other offices of their obligations under the international agreement, and of the need to generate data specifically to facilitate compliance; such offices are able to raise the bureaucratic conscience about their obligations and they will exercise a perhaps small but persistent insistence on compliance.\textsuperscript{664}

The prospect of having these reports publicized likewise puts pressure on the Member States to comply, as non-compliance will likely negatively affect their reputation among peers, observers, and potential investors. Indeed, as pointed out by Andrew Hurrell & Benedict Kingsbury, “states generally comply with international obligations . . . because of their broader concern with their reputation as reliable partners and their interest in a rule governed . . . international system.”\textsuperscript{665} Moreover, “[w]hen a member of an organization goes back on a commitment, it compromises in some degree its reputation as a reliable partner and jeopardizes it ability to continue to reap organizational benefits.”\textsuperscript{666}

However, learning from the APEC’s experience with its Data Protection IAP project, particular attention should be given by the ASEAN in ensuring that country compliance reports are regularly submitted. Furthermore, the ASEAN should also commit to go beyond collecting and publishing its Member States’ reports. It should, after considered analyses, make assessments as to the States’ levels of compliance, and suggest remedial measures in cases of substandard compliance.

In addition to national reports, the ASEAN could also monitor the Member States’ compliance with their data protection soft law framework obligations by drawing upon outside sources, and by relying on their own (or contracted) expert teams. For instance, NGOs, trade associations, and academics can provide useful information about a Member State’s

\textsuperscript{663} Id.
\textsuperscript{664} Id citing Paul Szasz, Administrative and Expert Monitoring of International Treaties, p. 15 (1999).
performance and contribute to transparency. An office within the ASEAN, or a private consultant can also help track the accomplishments and shortcomings of the Member States as they try to comply with their obligations.

As observed by Daniel Bodansky, “[i]nternational monitoring is useful not only as a means to detect violations, but also to reveal why a State is having difficulty in complying with a treaty and what kinds of assistance would be most helpful.” As such, similar to what should ideally be done with country reports, the results of monitoring efforts should lead to offering recommendations for remedial measures and assistance to Member States to help them comply with their obligations.

4.2.2.5. Provides a venue for participation of various stakeholders

One criticism that arose in the review of ASEAN agreements in Chapter 3 was that there was a lack of opportunity for stakeholders such as NGOs, trade associations, technical experts, and academics to participate in the agreements’ implementation. Although the evidence regarding this type of participation are varied, encouraging participation may contribute to an Agreement’s legitimacy, and hence its effectiveness. “Participants tend to feel a greater stake in the process and therefore a greater interest in its success. They also form a cadre of people who are more likely to help implement the treaty at the domestic level.”

Thus, the following stakeholders should be given a venue to participate in the implementation of an ASEAN agreement embodying the region’s data protection soft law framework: NGOs, trade and professional associations whose businesses and practices will be significantly affected by data protection legislation, experts in the field of data protection, privacy, and security, academics who specialize in the field, legal practitioners, and the relevant regulators and officials of various government agencies.

4.2.2.6. Regular meetings and reviews of the Agreement

Regular meetings among Member States ensure that ongoing attention is given to a particular issue, and on what they are doing to address it. Moreover, they provide a forum for negotiations, consultations, and knowledge-sharing among parties. In addition, an ASEAN Agreement on Data Protection...
Protection should provide for regular reviews of the instrument itself, and of the means being undertaken to implement it, to see if they are effective, if changes must be made, and additional measures planned. The technological aspect of data protection makes regular reassessments even more necessary, due to the speed with which technological advances are made, not only to promote data protection, but to defeat the technologies designed to keep data secure.

A section that calls for annual meetings would facilitate these negotiations, consultations, and knowledge–sharing activities. Furthermore, a review of the Agreement every five years, which aims to revise the Agreement and its Implementation Guide, as seen fit by the ASEAN and by national representatives, to respond to developments, would be ideal.

4.3. An ASEAN data protection standard deemed adequate and robust enough by stakeholders

A common criticism against the APEC Privacy Principles is that collectively, they represent a low privacy standard. Even though they were patterned after the OECD Privacy Principles, they do not, for instance, include the OECD Principles concerning Purpose Specification or Openness. More significantly, neither do they include any of the stronger principles contained in any of the APEC region’s privacy legislation developed since 1980. “They are at best an approximation of what was regarded as acceptable information privacy principles twenty years ago.” Indeed, the APEC Privacy Principles are not aspirational; in fact, they are the bare minimum, when it comes to being a standard for privacy protection.

Graham Greenleaf spoke of “Minimum” or first generation principles and “European” or second generation principles. The core of the OECD Guidelines lies in the eight “basic principles of national application” in Part Two (principles 7 to 14). “CoE Convention 108 included eight ‘basic principles for data protection’ in Chapter II, including all the OECD principles, plus others which anticipated the later ‘European’ principles.” The eight principles that they hold in common are:

1. Collection limitation principle—limited, lawful, and by fair means; with consent or knowledge (OECD 7; CoE 5(c), (d)).
2. Data quality principle—relevant, accurate, up-to-date (OECD 8; CoE 5(a)).
3. Purpose specification principle—at time of collection (OECD 9; CoE 5).

673 Id.
674 Id.
4. Use limitation principle—uses and disclosures limited to purposes specified or compatible (OECD 10; CoE 5(b)).
5. Security safeguards principle—through reasonable safeguards (OECD 11; CoE 7).
6. Openness principle—concerning personal data practices (OECD 12; CoE 8(a)).
7. Individual participation principle—individual rights of access and correction (Access: OECD 13; CoE 8(b); Correction: OECD 13; CoE 8(c), (d)).
8. Accountability principle—data controllers accountable for implementation (OECD 14; CoE 8).

These minimum privacy standards are now universally accepted as part of any data protection law, and are mostly found in over 100 national data protection laws, almost half of which are from outside Europe. An extended set of principles based on, and incorporating those enumerated above were developed for the EU Directive, plus some additional elements already found in CoE Convention 108. This occurred prior to the widespread use of the Internet, and therefore can be considered ‘pre-Internet’ development. Then in 2001, the CoE Convention adopted, via its Additional Protocol, some supplementary principles from the EU Directive, specifically the requirement to limit data exports. The following list, also by Greenleaf, of the most significant differences regarding privacy principles between these European instruments and the “minimum” OECD/APEC instruments is not comprehensive, but is enough to illustrate the higher, stricter standards embodied by one or both of the EU Directive and the CoE Convention plus CoE Protocol.

None of the following eight elements is required, or even recommended, by the OECD Guidelines or APEC Framework:

1. Data export restrictions based on destination—Requirement of restrictions on personal data exports to countries which did not have a sufficient standard of privacy protection (defined as ‘adequate’) (EU Directive and CoE Convention 108).

2. Minimal collection—Collection must be the minimum necessary for the purpose of collection, not simply ‘limited’ (both EU Directive and CoE Convention 108).

---

676 Id. citing OECD Guidelines
677 Id. at 55.
678 Id. at 55-56.
679 Id. at 56.
680 Id.
681 Id.
3. ‘Fair and lawful processing’—A general requirement of ‘fair and lawful processing’ (not just collection) (both EU Directive and CoE Convention 108). ...

4. ‘Prior checking’—Personal data systems which raise potentially high levels of risk should be identified and examined before they operate (EU Directive only).

5. Deletion—Destruction or anonymization of personal data after the purposes for which it is held are completed (both EU Directive and CoE Convention 108).


7. Automated processing controls—Data controllers should ensure that automated decision-making which significantly affects data subject is subject to human checking, and data subjects should be able to know the logic of such automated data processing (EU Directive only).

8. Direct marketing opt-out—Requirement to provide ‘opt-out’ of direct marketing uses of personal data (EU Directive only).

These “European” data protection principles have been adopted by all EU countries, and by almost all of the non-EU countries of Europe which are members of the CoE; they have also been adopted by many of the countries outside Europe that have enacted data protection legislation. The result is that there are at least 16 data privacy principles (8 ‘minimum’ and 8 ‘European’) derived from international agreements, that have become, to varying extents, standards, adopted in the overwhelming majority of data protection laws enacted globally. As such, this is the ideal basis against which to determine the data protection principles that should be considered by the ASEAN for its data protection soft law framework.

Greenleaf suggested the following approach for Asian countries wishing to enact legislation. It is based on what has already been enacted in existing data protection laws across the continent: if any of the 16 “minimum” or “European” principles, or some aspect of their implementation, is included in at least seven of the 11 Asian jurisdictions with significant data privacy laws, then a “best fit” approach to developing a model law (or corporate

---

682 Id. at 57.
683 Id.
684 Id. at 503.
685 China, Hong Kong, India, Japan, South Korea, Macau, Malaysia, the Philippines, Taiwan, Singapore, and Viet Nam.
standard) should include it. Such an approach, Greenleaf asserts, is not a “lowest common denominator” approach, or an overly idealistic approach including all elements that could be argued to be desirable; nor is it based on what future international standards might be – it is a realistic approach, based on what the leading Asian jurisdictions are already enacting. Based on Greenleaf’s comparative analysis, the following 11 principles would be a “best fit” since they have been adopted in at least seven of the 11 Asian jurisdictions considered:

(i) *Purposes specified*—A specific purpose of collection should be specified prior to collection of any personal data; stated in a publicly available privacy policy prior to collection; and clearly communicated to the data subject by notice (express or implied) no later than the time of collection.

(ii) *Minimal collection*—Collection should be limited to only the ‘minimal’ or necessary personal information for the specified purpose.

(iii) *Fair and lawful collection*—Collection should be only by means that are lawful and fair. ...

(iv) *Uses and disclosures limitation*—Uses and disclosures should be limited to the purpose of collection, plus any purposes directly related to that purpose; with any such changes of purpose specified and communicated to the data subject; and any exceptions limited to the minimum necessary in the public interest.

(v) *Data quality*—Personal data should be relevant to the specified purposes, and as necessary for those purposes, accurate, complete, and kept up to date.

(vi) *Security safeguards*—Personal data should be protected by appropriate security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data; (+ Requiring consideration: the circumstances when data breaches must be notified, and to whom).

(vii) *Deletion*—Personal data should be destroyed or anonymized after the purposes for which it is held are completed.

(viii) *Direct marketing*—A readily available facility should be provided to allow opt-out of direct marketing uses of personal data, or there should be an opt-in requirement.

---

686 Id.
(ix) **Openness**—There should be a general policy of openness to any person about developments, practices, and policies with respect to personal data systems; including means by which any person can readily establish the existence and nature of personal data, its main purposes of use, and the identity and contact information of the data controller.

(x) **Individual participation**—An individual should be able to (a) obtain confirmation whether a data controller holds personal data about him or her; (b) access that data; (c) obtain correction of contested data by having it erased, rectified, completed, or amended as appropriate; (d) obtain reasons for any refusal of confirmation, access, or correction; and (e) challenge any such refusals; ...

(xi) **Accountability**—A data controller should be accountable for complying with measures which give effect to the principles stated in (i)–(x).

This set of principles is not as high a standard as is found in the EU Directive, but is higher than those in the OECD Guidelines and APEC Framework. However, there are good reasons for legislation in Asia to exceed this moderate “best fit” set of standards. For instance, if a country wants to obtain an adequacy finding from the EU, then there are three additional principles that need to be considered. Notably, each of these principles is already implemented in five Asian jurisdictions:

(xii) **’Fair and lawful processing’**—Personal data should be processed fairly and lawfully. (This general principle does not only apply to collection, as in (iii) above.)

(xiii) **Sensitive data protections**—Categories of sensitive data should be specified and given additional protections.

(xiv) **Data export restrictions based on destination**—There should be restriction on exports of personal data to countries which do not have a sufficient standard of privacy protection (defined in Europe as ‘adequate’), so as to ensure that the personal data does have sufficient protection, and the data subject can ensure that protection is observed.

---

687 Id. at 504.
688 Id. at 505.
689 Id.
690 Id.
691 Id.
The two remaining of the 16 principles are not commonly included in Asian data protection laws, but may become more common as Asian countries increase the sophistication of their decision-making and the scope and potential dangers of their information systems:

(xv) **Automated processing controls**—Data controllers should ensure that automated decision-making which significantly affects data subjects is subject to human checking; and data subjects should be able to know the logic of such automated data processing.

(xvi) **Prior checking**—Personal data systems which raise potentially high levels of risk should be identified and examined before they operate.

Given the aspirational nature of ASEAN’s Agreements, the ASEAN Economic Community’s goal of becoming a region fully integrated with the global economy, and this dissertation’s proposal of working towards a data protection soft law framework that is, as much as possible, compatible and interoperable with other existing data protection frameworks, including that of the European Union, it is submitted that the data protection principles of an ASEAN data protection soft law framework should, and will likely go beyond what Greenleaf termed as a “moderate best fit.” Although this “moderate best fit” of privacy principles is realistic, it would benefit the ASEAN to aspire for a higher standard. Apart from enabling its Member States to possibly obtain an adequacy finding from the EU, going beyond the “moderate best fit” – that is, abiding by data protection principles in addition to those xi, such as principles (xii) to (xvi), and possibly more, - leads to other benefits.

One is that the ASEAN would gain the reputation of wanting to raise its Member States’ data protection standards. Another is that Member States would tend to aspire to comply with as many data protection principles recommended by an **ASEAN Agreement on Data Protection**. Hence, this is a way to “raise the bar” for the Member States who will draft (or even revise) their legislation. Another benefit lies in the possible privacy management program guide that could be issued by the ASEAN to assist companies and entities in the region who will seek assistance in building their programs. This guide will presumably abide by the higher standard proposed for the ASEAN; in turn, these companies and entities will be encouraged to implement a privacy management program that will provide greater protection for the data subjects whose data they process. Going beyond the “moderate best fit” will also allow the ASEAN to keep up, or even surpass the trajectory of Asian data protection laws which have, in recent years, been leaning towards stronger privacy principles. This will lessen the necessity of having to amend, not only the ASEAN data protection Agreement, but also those national laws that could be

---

692 Id.
patterned after it. This will also make the economies of the ASEAN Member States more attractive to investors seeking to conduct business in Asian jurisdictions with stronger data protection laws.

In addition, the “moderate best fit” (principles i-xi, above) has already been surpassed, in one way or another, by the data protection laws of ASEAN Member States. For instance, data protection laws of Malaysia and the Philippines already include principle (xiii), which pertains to providing additional protection for a broad range of categories of sensitive personal data.\(^{693}\) Principle (xv), which refers to the right to object to automated individual decisions, which implies that final decisions on significant matters should be subject to human oversight, is already found in the Philippine Data Privacy Act.\(^{694}\) The Philippine Data Privacy Act of 2012 also contains a right to data portability,\(^{695}\) a relatively new principle that has, only recently, become a new right in the EU’s General Data Protection Regulation (GDPR) in April 2016. The same Act, interestingly, explicitly provides for transmissibility rights of a data subject.\(^{696}\) Malaysia provides for a “right to copy of structured e-data.” Data breach notifications, both to the DPA and the data subject, also figure prominently in the Philippine Act.

However, the ASEAN should also perhaps look to a jurisdiction closer to the region – South Korea. This North Asian country abides by the following additional and innovative “Asian principles” – as termed by Greenleaf:\(^{697}\) the requirement of a privacy officer; placing the onus of proof on the data controller; ensuring anonymity in transactions where possible; no denial of service (also found in Singapore); the ‘unbundling’ of consents; segregation of consent and non-consent items; requiring opt-in for marketing purposes (also in Hong Kong); providing data breach notifications to the DPA (China, Japan, South Korea, the Philippines, Vietnam); providing data breach notifications to data subjects (Taiwan, the Philippines, South Korea); the deletion of data upon request of the data subject; and user rights on sale of businesses.

In sum, in order to maximize the opportunity to promote data protection in the region by raising the standards, the ASEAN will likely, and

\(^{693}\) Id. at 493.
\(^{694}\) Id. at 494.
\(^{695}\) Philippine Data Privacy Act of 2012, Section 18. Right to Data Portability. – The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.
\(^{696}\) Id. at Section 17. Transmissibility of Rights of the Data Subject. – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.
\(^{697}\) Graham Greenleaf, Asian Data Privacy Laws, p. 503.
should consider, not only Greenleaf’s “moderate best fit” principles; it should likewise consider the viability of including principles xii – xvi, and the innovative “Asian principles”. The latter category is even more promising in terms of feasibility, considering its adoption, in varying degrees, across Asia, and even in Southeast Asian jurisdictions.

4.4. Information Network Features

As mentioned in this Chapter’s abstract, this subsection and the two succeeding ones will be structured according to Anne-Marie Slaughter’s conception of governance networks. Networks of government officials, such as law enforcement officers, regulators, judges, and legislators increasingly exchange information and coordinate activity to combat global crime and address common problems on a global scale.\(^{698}\) This could, perhaps, be attributed to the fact that peoples and their governments need global institutions to solve collective problems that can only be addressed on a global scale.\(^{699}\) Data protection, especially its cross-border implications, is a prime example of a collective issue that must be addressed globally. For Slaughter, government networks offer a flexible and relatively expedient way to “conduct the business of global governance, coordinating and even harmonizing national government action while initiating and monitoring different solutions to global problems.”\(^{700}\)

A network is a “pattern of regular and purposive relations among like government units working across the borders that divide countries from one another and that demarcate the ‘domestic’ from the ‘international’ sphere.”\(^{701}\) In a world of government networks, officials such as judges, regulators, and legislators who act domestically are also reaching out to their foreign counterparts to help address the governance problems that arise when national actors and issues go beyond their borders.\(^{702}\) The first type of network is the information network. As the name suggests, it brings together regulators, judges, or legislators to exchange information and to collect and distill best practices.\(^{703}\) This information exchange can also occur through technical assistance and training programs provided by one country’s officials to another.\(^{704}\) It is best to begin with a discussion centered on information networks because the “glue of any transgovernmental network is the exchange of information and ideas.”\(^{705}\)

Information networks often actively collect and distill information about how their members do business, and the usual product of this distillation

\(^{699}\) Id. at 8.
\(^{700}\) Id. at 11.
\(^{701}\) Id. at 14.
\(^{702}\) Id. at 16.
\(^{703}\) Id. at 19.
\(^{704}\) Id.
\(^{705}\) Id. at 52.
is a code of “best practices” - a set of the best possible means for achieving a desired result identified by any members of the network at a given point in time. 706 “In information networks, participants exchange information on common problems and actual and potential solutions.” 707

They collect information on various national regulatory practices and distill them into codes of best practices, which they then disseminate with the special imprimatur of a transgovernmental organization—benefiting not only from combined technical expertise, but also from the ability to change and amend these practices as new information, which also includes information about each other’s reputation for probity and competence, is received.708

In the context of this dissertation, the participants could primarily be national Data Protection Authorities (DPAs), and the transgovernmental organization with the ability to facilitate coordination among these DPAs, the ASEAN. The other participants could include legislators, judges, and law enforcement officials who will be involved in their national data protection efforts.

In addition to the previously discussed characteristics, features, and measures, this sub-chapter describes those measures that may be undertaken, specifically to bring together these information network participants, so that they may learn from and provide technical assistance to each other, with the ultimate goal of coming up with a set of best practices for data protection within the region.

4.4.1. Establishing a network of Data Protection Authorities

The existence of a DPA is “the sine qua non of good privacy protection inasmuch as laws are not self-implementing and the culture of privacy cannot securely establish itself without an authoritative champion.”709 DPAs could fulfill the roles of “ombudsmen, auditors, consultants, educators, negotiators, policy advisers and enforcers”710 depending on the authority bestowed upon them by legislation. As such, the ASEAN should encourage each Member State to establish its own Data Protection Authority. Alternatively, if resources are scarce, Member States may choose to designate and authorize an existing government agency, such as an agency in charge of consumer protection or information and communications technology, to fulfill the responsibilities commonly associated with DPAs.

706 Id. at 53.
707 Id. at 63.
708 Id.
710 Graham Greenleaf, Asian Data Privacy Laws, p. 66
Indeed, the various responsibilities of DPAs would have them classified as regulators that could engage not only in information networks, but also in harmonization and enforcement networks. This sub-section delves into their responsibilities that would correspond with being part of an information network. The other functions that would better fit into their role as participants in harmonization or enforcement networks would be discussed in the succeeding corresponding sub-chapters.

DPAs, apart from their role as primary enforcers of a national data protection law, are also the repositories and communicators of information pertinent to the implementation and enforcement of the said law. In fact, the data protection statutes of the ASEAN Member States who have a comprehensive law, speak of the following DPA powers, responsibilities, and functions: regular publication of data protection laws, rules, and regulations; regular publication of case records and notices; formulation and publication of privacy codes; provision of assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person; provision of assistance to companies doing business abroad to respond to foreign privacy or data protection laws and regulations; undertake or cause to be undertaken research into and monitor developments in the processing of personal data, including technology, in order to take account any effects such developments may have on the privacy of individuals in relation to their personal data; promote awareness and dissemination of information to the public about the operation of data protection laws; and provide consultancy, advisory, technical, managerial or other specialist services relating to data protection.

These DPAs, due to the performance of these functions, are a rich and invaluable resource for legal and technical knowledge, and administrative experience. Should the ASEAN encourage the establishment of similar agencies in the other Member States, and should it assist in the building of a network among the region’s DPAs, the result would be a venue through which the Member States’ DPAs could share their knowledge and experience. The intended result is better policy coordination and convergence, the collective building up of governance capacity, avoidance of the challenges and problems encountered by the Member States who first had to implement data protection laws, adoption of measures which are more likely to achieve results, and a larger body of shared research.

711 See the Philippine Data Privacy Act of 2012, Section 7; the Personal Data Protection Act of 2010 of Malaysia, Section 48; and the Singapore Personal Data Protection Act of 2012, Part II, Section 6.

712 “Soft law codes of conduct issued by trans governmental regulatory organizations, as well as the simple dissemination of credible and authoritative information, also promote convergence. Promoting convergence, on the other hand, can also give rise to informed divergence, where a national governmental institution or the government as a whole acknowledges a prevailing standard or trend and deliberately chooses to diverge from it for reasons of national history, culture, or politics.” Anne-Marie Slaughter, A New World Order, p. 24.
Interestingly, the establishment of this type of information network can also lead to the improved performance of regulators. This network will make available information concerning the competence, quality, integrity, and professionalism of their fellow DPAs. Once a network is established, it becomes a conduit for information about members’ reputations— even if they didn’t have or care about their reputations beforehand. Having and caring about a reputation among one’s peers is a very powerful tool of professional socialization—in the profession of governance no less than in the private or nonprofit sector. Since members of a network face common challenges and responsibilities, they are likely to build norms of professionalism; it is likely that violations of those norms would be transmitted across the network, raising the cost of those violations.

The information-sharing efforts of this network of DPAs could be administered by a secretariat based in the ASEAN Headquarters in Jakarta. This secretariat, which, for purposes of this dissertation, will be called the ASEAN Data Protection Office, would deal specifically with administering an ASEAN Agreement on data protection. It is, among other things, an “information agency” created as part of a traditional international agreement-making process, whereby the parties to the agreement conclude the document and establish a secretariat to administer it. This secretariat can be the focal point for government networks of national officials concerned with the particular subject of the agreement – in this case, data protection; additionally, the secretariat, like some regional parliamentary groups, can also orient its activities toward helping national officials. Among other things, it can help direct and ensure the efficiency of the coordination of the DPA’s information-sharing activities. It can also facilitate the effective implementation of ASEAN’s data protection projects and activities.

4.4.2. Providing technical assistance, training, and capacity building for regulators, law enforcement, legislators, and judges

Managerialism, an approach to compliance most attributed to the work of Abram and Antonia Handler Chayes, asserts that the primary drivers of non-compliance are rule ambiguity and, more notably, lack of domestic regulatory capacity. Hence, it is claimed that compliance is best promoted through assistance and encouragement, rather than deterrence and punishment. To

713 Anne-Marie Slaughter, A New World Order p. 54.
714 Id.
715 Id.
716 Anne-Marie Slaughter, A New World Order, p. 157.
717 Id.
this end, technical assistance, training, and capacity-building are crucial to an Agreement’s effectiveness.

Building the capacity to govern in countries that often lack sufficient material and human resources to pass, implement, and apply laws effectively is an important and valuable consequence of government networks, most especially information networks. “Regulatory, judicial, and legislative networks all engage in capacity building directly, through training and technical assistance programs, and indirectly, through their provision of information, coordinated policy solutions, and moral support to their members.” The ASEAN, as shown in Chapter 3, commonly resorts to capacity-building activities in order to assist regulators, law enforcement, legislators, and judges better fulfill their roles in the national implementation of Agreements.

The efforts undertaken by the ASEAN towards implementing the e-ASEAN Framework Agreement and the ASEAN Agreement on Disaster Management and Emergency Response are particularly relevant. To achieve those Agreement’s goals, ASEAN and its own Member States, provided technical assistance to generate harmonized legislation in the region, and to increase the development of pertinent legal and technical policies. Technical assistance also led to educational and training programs to improve the implementation of these agreements at the national level. These types of activities also transmit information on the methods and technologies that could be implemented and used on a national level in order to execute the provisions of an agreement locally. This was a particularly important step in the ASEAN’s e-commerce harmonization project, since it was necessary to assess the ICT improvements that had to be made, and the technologies that must be adapted, in order to improve the ASEAN Member States’ e-commerce capabilities. This is then similarly important, should the ASEAN embark on a similar endeavor for data protection.

Thus, to further ensure effective compliance with the provisions of an ASEAN data protection soft law framework, the ASEAN should provide technical assistance to the Member States and facilitate knowledge-sharing and capacity-building among them. The types of assistance that could be provided should involve assistance in drafting legislation, rules, and policies; educational and training programs that assist the relevant officials in implementing and enforcing the Agreement’s provisions and the laws and regulations resulting from that Agreement; and knowledge-sharing on the types of technologies, particularly Privacy-Enhancing Technologies that should be used in order to improve data protection.

---

719 Id. at 185.
720 Id. at 185.
4.5. Undertaking a Hard Harmonization Project: Working through Harmonization Networks and Tools

The second type of network is the **harmonization network**. A harmonization network is a network that brings regulators together to “ensure that their rules in a particular substantive area conform to a common regulatory standard.”\(^{721}\) Usually operating within the bounds of a trade agreement, often with a specific legislative mandate, these regulators may work together to harmonize various types of regulatory standards.\(^{722}\) This type of network “contributes to world order by allowing nations to standardize their laws and regulations in areas where they have determined that it will advance their common interests in trade, environmental regulation, communications, protecting public health, or any number of other areas.”\(^{723}\)

Harmonization may mean “the adoption of an international standard that adjusts the regulatory standards or procedures of two or more countries until they are the same,”\(^{724}\) or, in keeping with the definition being used in this dissertation, harmonization refers to efforts designed to align individual country laws to remove unwanted gaps and reduce inconsistencies, with the goal of increasing legal certainty for parties that transact with more than one member country – for instance, multinational enterprises that are attempting to expand their business in a new region.\(^{725}\) “Harmonization networks allow their members to engage in the ongoing, highly detailed work of making national laws in a particular regulatory area consistent with one another. These networks are generally authorized by some international agreement between the participating countries.”\(^{726}\)

It is recommended that the following measures be included in the envisioned ASEAN Agreement that will serve as the foundation of a data protection soft law framework for the region. These measures or features are proposed as tools that a harmonization network may use because of their ability to aid in the alignment of individual country laws to remove unwanted legislative gaps and reduce inconsistencies. As previously discussed, the removal of legislative gaps and the reduction of inconsistencies should be a goal in an ASEAN data protection soft law framework, primarily because it will ease cross-border cooperation among law enforcement and regulators, and facilitate improved compliance with data protection laws, especially for entities that operate in various jurisdictions in the region. Moreover, the harmonization

\(^{721}\) Id. at 20.
\(^{722}\) Id. at 59, citing Marney L. Cheek, The Limits of International Regulatory Cooperation, 33 Geo. Wash. Int. 277, 316 (2009).
\(^{723}\) Id. at 167.
\(^{724}\) Id. at 59.
\(^{725}\) Information Economy Report 2007-2008 - Science and technology for development: the new paradigm of ICT, Prepared by the UNCTAD secretariat; Chapter 8: Harmonizing Cyber Legislation at the Regional Level: The Case Of ASEAN, p. 323.
\(^{726}\) Anne-Marie Slaughter, A New World Order, p. 63.
of national data protection law frameworks is expected to lead to larger internal and external consumer and business markets by facilitating more secure commerce, especially considering that countries reported consumers’ lack of trust in the security of e-commerce transactions and privacy protections as one of the major impediments to seizing the full benefits of e-commerce.\textsuperscript{727}

It is also recommended that these tools and measures be part of a larger project – that of a hard harmonization project that will be undertaken by the ASEAN for purposes of harmonizing the data protection frameworks of its Member States. As opposed to soft harmonization projects that are primarily based on training and capacity-building, hard harmonization efforts are chiefly based on model or uniform laws.\textsuperscript{728} As mentioned in Chapter 3, most e-commerce legal harmonization projects are soft harmonization projects, in that there is no intention for countries to adopt the same (or even model) laws and regulatory systems; all that is undertaken are training and capacity development activities, aimed at ensuring a common (or harmonized) understanding of legal requirements.\textsuperscript{729} On the other hand, an ideal hard harmonization project, being based on concrete and specific implementation measures, is seen to have the following benefits: first, the guidelines are an inclusive instrument, which ensures the participation of less-developed ASEAN member countries.\textsuperscript{730} They also provide for implementation steps that will ensure greater consistency across the region.\textsuperscript{731} In addition, the guidelines include a timetable, which will aid in guaranteeing an orderly, phased development.\textsuperscript{732} Moreover, they leave less room for interpretation and reduce inconsistencies; finally, they are in a flexible instrument that can be updated and reviewed (for example, every three years).\textsuperscript{733}

A previous sub-chapter already touched upon this Agreement having an inclusive nature by providing different deadlines to the Member States, in accordance with their resources and institutional capacities. It also discussed ensuring the delivery of technical assistance to aid the Member States in implementing the Agreement’s provisions. In addition, a previous subchapter also tackled the goal of being compatible and interoperable with other data protection frameworks. This sub-chapter will discuss the other features and measures that could lead to the attainment of the benefits of hard harmonization projects that are described above.

\textsuperscript{728} Id. at 323.
\textsuperscript{729} Id.
\textsuperscript{730} Id. at 324.
\textsuperscript{731} Id.
\textsuperscript{732} Id.
\textsuperscript{733} Id.
4.5.1. Having Data Protection Authorities Participate in Harmonization Efforts

It is foreseen that the primary drivers of the possible harmonization of data protection legal frameworks within the Southeast Asian region will be the Member States’ DPAs. The previous sub-chapter has discussed how these DPAs, with the help of an ASEAN Data Protection Office, can engage in information exchange and capacity-building. It is then most likely that the information and resources necessary for harmonization efforts will be coursed through the same network.

The DPAs (or designated government agencies, such as consumer protection or information and communications technologies offices) can participate in harmonization efforts by participating in the decision-making process, particularly when it comes to determining which measures should be undertaken to facilitate the harmonization of the region’s data protection laws and regulations. In the implementation stage, this network of DPAs can coordinate with each other in order to ensure that the steps they laid out to harmonize their laws and regulations are being implemented in their respective jurisdictions. Constant coordination among Southeast Asian DPAs is crucial to advancing the region’s data protection law harmonization efforts.

4.5.2. Begin with a review of domestic frameworks

Ideally, one of the first steps in a hard harmonization project for data protection in Southeast Asia is conducting a review of the existing domestic frameworks. This will, among other things, aid in the assessment of how similar and different they are, the policy gaps that need to be filled, the possible problems and constraints in terms of legislation and enforcement, the successes and failures encountered by the Member States, and the issues that will have to be anticipated by an ASEAN data protection soft law framework.

As such, this review will have to look at the following elements of a comprehensive legal infrastructure: relevant laws, regulations and codes, regulatory authorities, technical standards, enforcement and review policies and procedures, and training, education, and awareness-raising programs. A survey should be sent out to Member States asking for details pertinent to data protection regarding these elements. These details should cover, not only a description of these elements, but also a narration of the successes and benefits, and the difficulties and challenges related to them. This will help inform the ASEAN about those policies, administrative and regulatory structures, and measures that could be adopted by other States in the region because of their likely success, and those challenges that will have to be addressed in the creation of a regional data protection soft law framework.

---

734 Id. at 333.
4.5.3. Facilitate the enactment of harmonized data protection laws through model laws

Another measure that could advance harmonization efforts in the region is encouraging the enactment of harmonized data protection legislation. This could be done by the publication of a model law, which could be adopted by the Member States in toto, or with modifications, in accordance with the needs and legal limitations specific to each Member State. For those Member States that already have a comprehensive data protection law, they may use the ASEAN data protection model law as a guide for future amendments or revisions.

ASEAN has had extensive experience in using model codes. Its ASEAN Inter-parliamentary Organization (AIPO) works primarily through the provision of information and the development of model legislation for use by its member parliaments. In fact, AIPO members have also used the collective power of the organization to pressure their governments on specific issues, most notably the damage caused by the East Asian financial crisis in 1997. AIPO built its own legitimacy and influence largely through the power of information and socialization. Consequently, its ability to collect and distill information has made it a credible source of legislative initiatives across the region - initiatives which have driven harmonization efforts among Southeast Asian laws.

Such a model law can serve two purposes: first, it establishes minimum acceptable standards for data protection across the Southeast Asian region; second, it facilitates harmonization by being an instrument that the Member States may emulate as they create or revise their own data protection laws.

Establishing a minimum standard for the region will encourage intraregional commerce, since businesses and consumers will have greater assurance that their data will be subject to a certain level of protection, regardless of where it is processed within the region. It will also encourage businesses operating across multiple ASEAN jurisdictions to ensure that the data they process is subject to uniform standards of security, thus raising a company’s data protection standards and practices on a larger scope.

With regard to the second purpose, as previously argued, a major reason why countries do not comply with international obligations is because of a lack of capacity and resources. Having an international organization such as the ASEAN draft a model law for the region, which may be modified, with the assistance of experts, to suit the needs and limitations of each Member State, will ease the burden of the legislators of those Member States that may

---

735 Anne-Marie Slaughter, A New World Order, p. 156.
736 Id. at 110.
737 Id.
738 Id.
otherwise be discouraged from expending resources on the drafting of their own national data protection laws. In addition, as mentioned by Anne-Marie Slaughter, “where states seek to create new legal rules and policies in the face of a dearth of local knowledge and expertise, they often seek to borrow from other states or internationally renowned experts.”\textsuperscript{739} This feature provides the necessary resource for legislators who lack the requisite expertise to craft effective national data protection laws. Moreover, since having a model law will increase the chances of the national data protection laws of the various Member States sharing commonalities, there will be a higher likelihood that the benefits arising from a more harmonized data protection legal framework will accrue.

In terms of harmonization, particular attention should be given to certain matters since they have a significant impact on cross-border enforcement of data protection laws. The ASEAN experience with previous Agreements has shown that cross-border prosecution was sometimes infeasible, due to differences in what constitutes offenses – what may be considered a crime in Malaysia may not necessarily be a crime in Myanmar. Such a scenario would hinder remedies such as extradition, investigation, and other prosecutorial acts. Considering that data protection has large cross-border implications due to the increase in intra-regional data flows, the ASEAN should consider harmonizing what constitutes a data protection offense, in order to ease prosecution efforts. To add, because of a lack of legal harmonization efforts, some countries in Southeast Asia have laws providing for certain penalties, such as confiscation and seizure, while others do not, and this complicates cross border cooperation in terms of enforcing remedies. Thus, matters such as the types of acts that may constitute an offense, the kinds of penalties that may be imposed, and the remedies that may be taken in the event of a violation are ideal subjects of harmonization.

4.5.4. Encourage the development of comprehensive legislation instead of sectoral laws

Another way to facilitate the harmonization of data protection laws across Southeast Asia is to encourage the enactment of comprehensive legislation. It must be conceded that a system of sectoral laws has certain advantages:\textsuperscript{740} it provides for flexibility, allowing rules to be varied according to the legitimate needs of each sector; remedies can be provided in the context of a sector’s own environment; clarity and specific content can be added to rules; and complex exceptions designed for other sectors can be omitted.

\textsuperscript{739} Id. at 179.
However, dependence on sectoral laws have the following disadvantages: \(^741\) this approach does not reflect the growing convergence of many industries in various markets; it requires new legislation to be introduced with each development of new technology; it ignores the reality that sectoral boundaries are becoming increasingly blurred and do not provide any impediment to the flow of data; a piecemeal approach gives rise to ‘boundary’ issues where data is transferred to an unregulated sector, or a sector which is regulated by a different set of rules; it is complicated from a data subjects’ perspective, as similar types of data may receive different treatment, depending on which sector in which they are located; and the risk of having some sectors remain unregulated is increased.

On the other hand, a comprehensive approach has the following advantages: \(^742\) virtually all sectors, save for those explicitly excluded, will be subject to data protection laws, ensuring that more data subjects and more types of data are protected; it is consistent with current global trends, thus allowing a more seamless transfer of data internationally, thus encouraging commerce; and consistency with international statutory regimes minimizes compliance costs for organizations operating in multiple jurisdictions. In order to address the possible need for specialized policies for certain sectors, a solution could lie in co-regulation (to be discussed in a succeeding sub-section), which would encourage certain sectors, government agencies, or regulators to issue rules and regulations that would supplement a comprehensive law with policies that are particularly necessary for those entities that come within their ambit.

Considering not only the global trend, but also the fact that three ASEAN Member States chose to adopt the comprehensive approach, the ASEAN will likely encourage Thailand to pass its comprehensive data protection bill, and urge the six remaining States to follow suit. This will allow for easier harmonization, which has always been one of ASEAN’s major e-commerce objectives. In addition, this will foster an environment wherein those ASEAN Member States who implemented their data protection law ahead of the others will be able to provide technical assistance to the latter.

4.5.5. An interim measure: voluntary model codes

Drafting and enacting a comprehensive data protection law, even with the help of the ASEAN providing model laws and technical assistance, is bound to take time. An interim measure could be the encouragement of the use of voluntary data protection guidelines for the private and public sectors, in the form of Model Codes. \(^743\) Model Codes could also be created through the hard harmonization project described above. Alternatively, the ASEAN could

\(^{741}\) See Id.
\(^{742}\) See Id.
\(^{743}\) Id. at 37.
compile and endorse a list of existing data protection Model Codes that could be used by Southeast Asian entities, as they await a comprehensive data protection law. Ideally, such Model Codes should be given official recognition, and adherence encouraged on a voluntary basis. This approach will have an educative and harmonizing function and should ease the transition into full compliance with legislation.\footnote{See Id.}

### 4.6. Enforcement Network Features

Another type of network – the enforcement network - focuses primarily on enhancing cooperation among national regulators to enforce existing national laws and rules.\footnote{Anne-Marie Slaughter, A New World Order, p. 55.} According to Slaughter, “[a]s the subjects they regulate—from criminals to corporations—move across borders, they must expand their regulatory reach by initiating contact with their foreign counterparts.”\footnote{Id.} In this type of network, members provide assistance to each other in the enforcement of national laws by exchanging information and actively assisting one another in pursuing violators of the web of national and international regulations.\footnote{Id.} Enforcement networks “contribute to world order by helping nations enforce law they have individually or collectively determined to serve the public good.”\footnote{Id. at 167.}

This sub-chapter describes the various features and mechanisms that could aid members of enforcement networks whose goal is to facilitate the enforcement of national data protection laws in Southeast Asia.

#### 4.6.1. Independent Data Protection Authorities equipped with the necessary powers and functions to cooperate on cross-border matters

DPAs should ideally be independent, due to their function of preventing possible abuses of government. DPAs should be able to freely investigate violations perpetrated by government instrumentalities, and they should also have the ability to impose the necessary sanctions. This will be best ensured if, among other things, their independence is required by legislation, their officials have fixed terms of office, their remunerations fixed, there is a prohibition on holding concurrent government positions, and a disclosure and prohibition of possible conflicts.\footnote{See Graham Greenleaf, Asian Data Privacy Laws, p. 509.} Policies such as these help ensure that officials of DPAs are insulated from acts that would render them susceptible to the influence of other government officials whom they may have to investigate. They also aid in guaranteeing that the officials themselves are free from interests that could negatively affect their decision-making.
In addition to being independent, they should also be equipped with the authority to investigate violations, whether on their own or upon the filing of a complaint. More importantly, effective DPAs have the ability to impose sanctions and order remedies – the principle means of enforcement of data protection laws, especially in Asian countries.  However, in addition to these standard powers and functions, it should also be ensured that the DPAs and law enforcement authorities have the authority to cooperate with their foreign counterparts.

The two previous chapters have elaborated on scenarios wherein cross-border enforcement of various laws (such as laws on data protection, preventing drug production and trafficking, and preventing human trafficking) have been thwarted or rendered more difficult due to the lack of authority on the part of law enforcement to cooperate with each other on matters such as sharing of information, investigations, and prosecution. As such, beyond the standard powers and functions commonly granted to DPAs, and law enforcement authorities, there should be in place, clear processes through which they could cooperate with each other; they should have the authority to share the necessary information that would aid them in investigations and prosecutions, subject to certain limitations and safeguards; and clear, consistent policies on seeking and enforcing redress, and the ability to use judgments, court orders, and evidence obtained abroad.

As mentioned in previous chapters, a possible model for this type of cooperation and coordination would be the ASEAN Treaty on Mutual Assistance on Criminal Matters. This treaty provides that parties must render to one another the widest possible measure of mutual legal assistance in criminal matters, namely investigations, prosecutions and resulting proceedings. The assistance contemplated covers evidentiary matters, service of judicial documents, searches and seizures, production of documents, identifying and tracing instrumentalities of a crime, freezing, recovery, forfeiture or confiscation of property, and location and identification of witnesses and suspects. ASEAN authorities could resort to this Treaty, should the data protection violation constitute a criminal offense. Alternatively, it could stand as a model arrangement for an instrument specifically made for enforcement of data protection laws, should it be found unworkable for that purpose.

4.6.2. Encouraging the development of a system of co-regulation

The previous chapter (Section 4.3.2.1.3) explained why a purely legislative approach to data protection is insufficient, and that other measures have to be considered in order complement the enactment of statutes. One of

---

750 Id. at 510.
752 Id. at Article I (2).
these measures is co-regulation. While many countries still adopt the traditional regulatory approach of prescriptive legislation (i.e., "command-and-control"), the trend now is to regulate less but regulate better.\textsuperscript{753} This could be attempted by utilizing self or co-regulatory models, in conjunction with legislative approaches.

Without reiterating the lengthy discussion in the previous chapter, this approach encourages continuous and innovative self-improvement by giving business greater flexibility, within a clear framework of expectations and requirements, jointly formulated by industry and government, rather than stopping at compliance with a set performance or standard;\textsuperscript{754} regulations can quickly supplement the industry-specific gaps in legislation; and this approach reduces dependency on limited government resources by using industry’s knowledge and resources, thus reducing the expense of government being solely responsible for collecting the information, developing this into regulations, monitoring the effects, and serving at the frontline of receiving and processing complaints and disputes, often without an appropriate level of industrial and process experience.\textsuperscript{755}

Thus, a co-regulatory approach, wherein self-regulatory organizations (SROs) can work with government regulators such as DPAs, in creating rules and regulations, monitoring, receiving, and processing complaints, investigating, and other aspects of enforcement would be ideal, especially in the ASEAN region, wherein most governments do not have an abundance of resources to dedicate to data protection efforts. Moreover, the government, with the knowledge they accumulated with the help of SROs, would be in the best position to promote international cooperation and harmonization of regulatory and enforcement schemes, and is more likely to be effective than any single sector in securing the collective action of sectoral organizations.\textsuperscript{756} Indeed, a system that could make use of the knowledge and resources of both government and industry would be a viable option for promoting data protection, not only nationally but regionally.

\subsection*{4.6.3. Looking into jurisdictional matters over data protection offenses}

ASEAN’s e-commerce hard harmonization project revealed that legally effective e-commerce transactions require a method of resolving cross-border jurisdiction issues that is properly defined and certain.\textsuperscript{757} There are a number of benefits to having these deeply complex issues resolved, including an increase

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{753} Report On A Model Data Protection Code For The Private Sector, Prepared by The National Internet Advisory Committee Legal Subcommittee p. 18.
\item \textsuperscript{754} See Id.
\item \textsuperscript{755} See Id.
\item \textsuperscript{756} Id.
\item \textsuperscript{757} Information Economy Report 2007-2008, Science and technology for development: the new paradigm of ICT, Prepared by the UNCTAD secretariat, Chapter 8 Harmonizing Cyber Legislation At The Regional Level: The Case Of ASEAN, p. 330.
\end{itemize}
\end{footnotesize}
in confidence and uptake of e-commerce by businesses and consumers.\textsuperscript{758} The e-commerce project recommended that ASEAN consider developing a guideline on the harmonization of jurisdiction for B2C e-commerce transactions.\textsuperscript{759} One recommendation was for the ASEAN to encourage member countries to adopt measures that ensure that proceedings against consumers are brought only in the State where the consumer is domiciled, and measures that ensure that consumers cannot waive their consumer protection rights in contracts.\textsuperscript{760}

Another recommendation to look into with regard to jurisdiction is one given in a previously-cited ASEAN report.\textsuperscript{761} That report recommended looking into the territoriality principle,\textsuperscript{762} the principle of passive personality,\textsuperscript{763} the principle of nationality,\textsuperscript{764} the principle of “extradite or prosecute,”\textsuperscript{765} and exercising jurisdiction over offenses committed outside the territorial jurisdiction of a State but linked to serious crimes and money laundering planned to be conducted in the territory of that State, as options for jurisdictional policies with regard to cross-border violations.

In prosecuting data protection offenses, due consideration should be given to the cross-border nature of the violations that may have occurred. With violators based within the territory of one or several Member States, with a high likelihood that affected data subjects will be spread across various ASEAN territories, ASEAN should consider an approach to jurisdictional issues that is not only defined and certain, but will widen the scope of the investigatory and prosecutorial scope of its DPAs and other law enforcement authorities.

4.6.4. An improved Cross Border Privacy Rules System

In addition to enforcing data protection laws and regulations on a national level, ASEAN Member States also have to contend with their cross-border enforcement. In Chapter 4, this dissertation looked at APEC’s Cross Border Privacy Rules (CBPR) System and Cross Border Privacy Enforcement Arrangement (CPEA) as a possible model for ASEAN. Having discussed the system’s strengths and weaknesses, and the challenges it encountered in the

\textsuperscript{758} Id.  
\textsuperscript{759} Id.  
\textsuperscript{760} Id.  
\textsuperscript{761} Progress Report on Criminal Justice Responses to Trafficking in Persons in the ASEAN Region p. 9.  
\textsuperscript{762} Id. “A State is required to establish jurisdiction over offences when the offence is committed in the territory of that State or on board a vessel flying its flag or on an aircraft registered under its laws”  
\textsuperscript{763} Id. “A State may exercise jurisdiction over offences when committed outside the territorial jurisdiction of that State against one of its nationals.”  
\textsuperscript{764} Id. “A State may exercise jurisdiction over offences when committed outside the territorial jurisdiction of that State by one of its nationals.”  
\textsuperscript{765} Id. “A State must establish jurisdiction over offences when the offender is present in the territory of the State and the State does not extradite the offender on grounds of nationality.”
previous chapter, below are some suggested features and characteristics to consider, should the ASEAN decide to adopt a similar system.

a) Essential to an accreditation system is an accrediting body deemed credible by regulators, businesses, and consumers. The APEC experience has shown that issues as to an Accountability Agent’s (AA) reputation (especially with regard to conflicts of interest), and failure to fully abide by the CBPR requirements, undermine the credibility of the entire system. As such, should the ASEAN adopt a system similar to the CBPR, it should consider having an office within the Association – perhaps the previously-suggested ASEAN Data Protection Office – issue the certifications. This would help ensure the absence of conflicts of interest, and it will be more likely that this Office would abide by ASEAN program requirements, since it would be under the supervision and control of the Association. Alternatively, if this is too costly, the ASEAN could accredit a private entity similar to TRUSTe (or even TRUSTe itself), but it should ensure that before it does so, this private entity meets ASEAN’s standards for being an AA, that it issues certifications based on ASEAN’s program requirements, and that no conflicts of interest exist, or should any exist, that these be declared. Additionally, the ASEAN should regularly assess the suitability of its AA/AAs, and strip them of this status should they be found not fully compliant.

b) For a system similar to the CBPR to effectively function, the ASEAN should encourage its Member States to take steps to ensure that its government regulators, taken together, are able to enforce data protection laws against all sectors that engage in cross-border transfers of personal data. A criticism against the APEC CBPR is that currently, AAs do not have the ability to accredit enterprises in all sectors of the economy. This is because of scenarios wherein the DPAs, or the other national regulatory authorities, to whom the AA refers matters that it could not resolve on its own for enforcement, do not have jurisdiction over all sectors that engage in cross-border transfers of data. This consequently limits the scope of operation of the CBPR only to those sectors who are under the authority of a DPA or any other authority that enforces data protection laws. Sectors and enterprises that do not fall under their jurisdiction thus cannot seek CBPR accreditation.

To expand the scope of a similar system for the ASEAN, it should consider enacting a provision in its data protection Agreement encouraging Member States to widen the collective scope of authority of their DPAs and other regulatory agencies who may have a similar power to enforce data protection laws, rules, and regulations against entities that may be under their authority. With more entities whose data processing activities are regulated by authorities who can enforce data
As mentioned in the previous chapter, there is no provision for external inputs as to whether there are substantial objections to a proposed AA approval; neither is there a mechanism through which external parties can verify, either before or after certification, that a company accurately stated its policies to obtain a certification from an AA. These contribute to a lack of transparency and opportunities for public participation. Thus, if the ASEAN were to adopt a CBPR-like system, it is necessary to make provisions that will allow for a transparent certification system which allows regulators and the public, not only to comment and object to the granting of a certification, but also to verify or ascertain for themselves, whether the business applying for, or given a certification, indeed complied with all the necessary requirements.

d) Entities who are found compliant with APEC CBPR requirements are certified, and given the right to display the AA’s seal on their websites, to signify this compliance. Note, however, that this does not signify compliance with national data protection laws. In addition, there are APEC CBPR members who use fine print in their privacy policies to exclude certain activities, such as mobile applications and cloud services, from their APEC certification. These might have a tendency to mislead consumers into thinking that the company displaying an AA’s seal is compliant with all relevant national data protection laws, and that all their activities are covered by the AA’s certification. To prevent this from happening, should the ASEAN adopt a similar scheme, it should ensure that the seal to be displayed by a company found compliant with ASEAN standards communicates that the certification does not necessarily mean that the company bearing the seal is compliant with all relevant national data protection laws, but is only compliant with the ASEAN’s data protection standards. Additionally, if necessary, this certification should communicate the fact of any exclusions, to prompt consumers to find out, perhaps by going through the company’s detailed privacy policies, what those exclusions might be.

e) In the APEC CBPR system, an AA is required to investigate complaints made to it against a company it has certified. Thus, should the ASEAN adopt a similar system, an accessible mechanism for filing complaints and dispute resolution is imperative, in addition to the AA’s ability to effectively investigate these grievances. A practical solution would be for the ASEAN to host a website dedicated to this purpose. A possible model is the ASEAN Solutions for Investments, Services and Trade (ASSIST) website, which is designed to be an internet-based and user-friendly facility for receiving, processing, and responding to complaints submitted by ASEAN enterprises. Having a similar website, but for
purposes of receiving, processing, and responding to complaints, and facilitating dispute resolution, in relation to possible data protection violations committed by participants in ASEAN’s system would assist consumers in seeking redress, and would also aid PEAs or regulators in enforcing data protection laws. This would, of course, presuppose the existence of a policy requiring AAs to refer to national authorities those matters that they could not remedy themselves.

This also brings to mind a significant benefit that could be brought about by a system similar to APEC’s CBPR: one of its most notable advantages is that it assists PEAs in focusing their efforts and resources on systemic, high profile, and high-impact privacy issues, instead of being on the frontlines of receiving and handling complaints, and facilitating relatively non-contentious dispute resolution, since AAs can take on this task. Efficient and effective complaint handling by an AA, and its ability to resolve minor disputes, can lower the workload of PEAs to enable them to focus their efforts strategically.

4.7. Chapter Conclusion

Whereas traditional international lawmaking has come in the form of hard law, soft law, which comes in the form of international guidance and non-legal instruments, is emerging as an equally powerful, if not more powerful, form of regulation. It has been argued that substantial harmonization or convergence among national laws frequently results not from hard law of any kind, but rather soft law in the form of principles, guidelines, codes, standards, and best practices. Additionally, as claimed by Slaughter, the “exchange of information, development of collective standards, provision of training and technical assistance, ongoing monitoring and support, and active engagement in enforcement cooperation that does and can take place in government networks can give government officials in weak, poor, and transitional countries the boost they need.”

The goal of the ASEAN is to have legislation in line with regional best practices and regulations, and to have a harmonized legal infrastructure for e-commerce, and more specifically, data protection. The previous chapters have shown that to achieve this goal, the ASEAN can resort to a data protection soft law framework - a legal structure that provides for broad, general rules that influence, in a non-binding and unenforceable manner, the ways in which personal data is processed, both within national borders, and when the data crosses those borders.

767 Id.
768 Anne-Marie Slaughter, A New World Order, p. 178.
769 Id. at 178-179
770 Id. at 266.
The foundation of ASEAN's data protection soft law framework could be a soft law instrument – an ASEAN Data Protection Agreement – which provides for clear, specific objectives, but is flexible when it comes to the means to achieve those goals. However, being aware of the limited resources of the Member States, this Agreement should provide for the issuance of an Implementation Guide, which will recommend specific measures and scheduled steps to be undertaken regionally and nationally, to achieve those goals. In addition, a system of reporting and monitoring accomplishment of these steps and measures serve to encourage timely compliance; responding to the results of these reporting and monitoring activities with recommendations on how to remedy shortcomings further facilitates compliance.

This Agreement should recognize the importance of having institutions in place to help carry out the measures necessary to achieve its objectives. As such, an Agreement that provides for the establishment of a network of DPAs, who will share information, engage in technical assistance, participate in harmonization efforts, and cooperate for purposes of enforcement is crucial to its success.

Specific steps such as encouraging the use of PETs, aiding in the establishment of privacy management programs, and supporting a pool of trained professionals to manage these programs are also ideal measures to consider. Harmonization could be made possible by the drafting and issuance of model legislation; voluntary model codes could ease the transition into a system governed by data protection laws.

An independent DPA should ideally be in place in every Member State, to lead enforcement efforts. As for the tools necessary for enforcement, legislation, whether comprehensive or sectoral is not sufficient. Though comprehensive data protection laws are more likely to arise, given the trend in the region, and its positive characteristics, it should ideally be supplemented by a system of co-regulation, wherein both government regulators and industry stakeholders take part, both in creating industry-specific rules and guidelines, and their enforcement. Moreover, to maximize the utility of an ASEAN data protection soft law framework, it should have a mechanism in place, the purpose of which is enforcing the cross-border aspect of data protection laws.
6. A summary, conclusion, and the challenges that could be encountered in the implementation of an ASEAN Data Protection Soft Law Framework

This dissertation began with explaining the motivation behind looking for a possible strategy for promoting data protection in the Southeast Asian region. This motivation is based on the following: ASEAN has recognized that a necessary step that must be taken towards realizing the goal of an ASEAN Community is the promotion of information security and data protection. It later proposed that all Member States must have, in accordance with the Strategic Schedule for the ASEAN Economic Community, data protection legislation and regulations in line with regional best practices; the same Strategic Schedule expressed the desire of the ASEAN leadership to have a harmonized legal infrastructure for e-commerce, which includes data protection law and regulations, for the Southeast Asian region. In addition, the ASEAN Economic Community Blueprint 2025 has identified, as a measure to enhance connectivity and cooperation, putting in place a coherent and comprehensive framework for personal data protection; the same Blueprint likewise pointed out the necessity, among Member States, of equivalence in technical regulations, standards harmonization, and alignment with international standards. Furthermore, ASEAN’s intended economic integration will give rise to increased transborder data flows and various risks and challenges related to such flows. These risks and challenges must be addressed. Moreover, the numerous and varied data protection issues that have come about, and will later emerge in the region, must also be dealt with.

Considering all these, only three Member States, specifically Malaysia, the Philippines, and Singapore have enacted comprehensive data protection laws; there is no harmonized legal infrastructure for data protection in the region; there is no mechanism through which alignment with international data protection standards could be achieved by all ten Member States; and to sum it all up, there is, as of yet, no concrete comprehensive strategy or plan to achieve the above-mentioned objectives.

As such, this dissertation sought to look at a possible way to start working towards the necessary comprehensive strategy. Considering ASEAN’s strong tradition of consensus-building, the eschewal of excessive institutionalization, and the avoidance of legally-enforceable commitments, it was concluded that a soft-law approach could be a viable option. The approach commonly taken by ASEAN to achieve policy goals, and the same approach recommended in this dissertation, is characterized as soft-law because ASEAN’s legal structures and instruments lack one, two, or all of the following: (i) precision of rules; (ii) enforceable obligations; and/or (iii) delegation of authority to a third-party decision-maker to monitor, interpret, or enforce implementation.
In order to frame the discussion, this work had to provide a definition for the concept that encompasses a legal structure, the objective of which is promoting data protection in the context of a regional grouping of states, in a manner that lacks a precision of rules, enforceable obligations, or the delegation of authority to a third-party decision maker to monitor, interpret, or enforce implementation. The term “international data protection soft law framework” was the result. The definition was presented in the form of a set of elements: (i) this is a legal structure that attempts to regulate the ways in which personal information is gathered, registered, stored, used, and disseminated; (ii) the legal structure encompasses both the conduct of states with and among each other, and the conduct of private parties involved in cross-border transactions, in relation to the gathering, registering, storing, use, and dissemination of personal information; (iii) the legal structures lack one, two, or all of the following: (a) precision of rules; (b) enforceable obligations; and/or (c) delegation of authority to a third-party decision-maker to monitor, interpret, or enforce implementation; and (iv) the legal structures tend to set down diffusely formulated, general rules for gathering, registering, storing, using, and disseminating personal information, and provide for the subsequent development of more detailed rules as the need arises.

Since the effectiveness of an international data protection soft law framework to achieve ASEAN’s data protection goals must be evaluated, it is necessary to first look at previous, analogous cases of success, to find out what contributed to their ability to accomplish certain objectives. Possible pitfalls, weaknesses, and challenges must also be looked into, so that these may be avoided or remedied. Hence, several ASEAN soft law instruments were reviewed. The aspects looked into were each instrument’s major objectives; the measures prescribed by these instruments to be enacted in order to achieve its objectives; the positive outcomes of these measures; and the shortcomings of, or difficulties encountered in implementing, these instruments.

In order to see, not only the effective soft law measures that could work in the ASEAN, but in particular, effective soft law measures aimed at promoting data protection, this work had to study existing international data protection soft law frameworks: the OECD Privacy Guidelines and the APEC Privacy Framework. The approach taken was that of looking at the measures implemented in connection with these frameworks, and their features and characteristics. The advantages and disadvantages of their features and characteristics, and the successes of, and challenges involved in the implementation of the measures they recommended were illustrated.

The result was a set of recommendations for what could be considered ideal features and characteristics of an ASEAN data protection soft law framework. Specific measures that could be implemented, due to their likelihood of success in achieving policy goals were also presented.
It was concluded that soft law, which comes in the form of international guidance and non-legal instruments, could be an effective form of regulation and tool for promoting data protection. It was found out that harmonization or convergence of national laws could result from soft law measures, such as privacy principles, Implementing Guidelines, codes, standards, and best practices. The exchange of information, development of collective standards, provision of training and technical assistance, ongoing monitoring and support, and cooperation for purposes of cross-border enforcement of data protection laws can be facilitated through government networks; these networks can also give government officials in countries with fewer resources the help they need to achieve the data protection objectives of the ASEAN.

It was likewise concluded that an ASEAN Data Protection Agreement that provides for clear, specific objectives, but is flexible when it comes to the means to achieve those goals could serve as the foundation of an ASEAN data protection soft law framework. The issuance of an Implementation Guide, which will recommend specific measures and scheduled steps to be undertaken regionally and nationally; a system of reporting and monitoring the accomplishment of steps and measures suggested in the Implementation Guide; and responding to the results of these reporting and monitoring activities with recommendations on how to remedy shortcomings facilitates compliance, and ultimately contributes to the promotion of data protection in the region.

The necessity of an Agreement that encourages the establishment of a network of DPAs, who will share information, engage in technical assistance, participate in harmonization efforts, and cooperate for purposes of enforcement was likewise found to be crucial. Other specific steps such as encouraging the use of PETs, aiding in the establishment of privacy management programs, and supporting a pool of trained professionals to manage these programs were also found to be effective measures. In addition, it was established that harmonization could be made possible through various steps such as the drafting and issuance of model legislation and voluntary model codes, which could likewise ease the transition into a system governed by data protection laws.

Furthermore, an independent DPA was found to be an important element in any data protection soft law framework. Additionally this dissertation further confirms that legislation, whether comprehensive or sectoral is not sufficient - it should ideally be supplemented by a system of co-regulation, wherein both government regulators and industry stakeholders take part, both in creating industry-specific rules and guidelines, and their enforcement.

Finally, to maximize the utility of an ASEAN data protection soft law framework, it should have a mechanism in place, the purpose of which is facilitating the cross-border aspect of data protection laws. This mechanism,
which is primarily an accreditation system, should have an accrediting body deemed credible by regulators, businesses, and consumers; and a network of independent DPAs who are authorized to participate in cross-border enforcement of data protection laws, and have authority over, ideally, all sectors that engage in the cross-border transfer of data. This mechanism should also be transparent and provide a venue for participation of stakeholders. Any seal of accreditation that it might give to companies that are found compliant with the standards and program requirements set by ASEAN should also be able to clearly communicate the extent and limits of the said accreditation. Finally, and of utmost importance, is an accessible mechanism for filing complaints and dispute resolution, and the existence of a referral system that would have the system’s accrediting body, or AA, refer matters to DPAs who are empowered to investigate and prosecute violations, and authorized to impose sanctions.

As promising an ASEAN data protection soft law framework with these features and characteristics might be in achieving the Association’s objective of promoting data protection in the region, it is still important to identify the possible challenges the ASEAN will likely encounter in working towards implementing this framework.

The first challenge involves human rights concerns, particularly in connection with possible violations that could be committed by government instrumentalities. Only six ASEAN Member States’ constitutions mention the right to privacy. In addition, the extent to which the right is protected is not uniform across these States, and protections against searches of the home, residence, or property, the individual’s person, undue exploitation of personal data, and protections of honor, dignity and reputation, correspondence and other communications, and the right to family life are neither consistently protected, procedurally or substantively. Additionally, at present, only one ASEAN Member State has a comprehensive data protection law that covers both the private and public sector – the Philippines. Although Singapore and Malaysia have comprehensive data protection laws, these do not apply to the public sector. More concerning is the fact that in these two latter countries, there are no statutory provisions that ensure the independence of their DPAs.

Hence, in the ASEAN’s efforts to promote data protection in the region, it should consider encouraging the recognition of privacy as a human right in the Member States’ constitutions. This will help ensure that victims of privacy violations who have no recourse in legislative enactments, will, at the very least, be able to invoke such offenses as violations of their constitutional rights. This, in turn, will allow them to seek some redress for possible violations that may be

772 Id.
committed both by private or state actors. Such an approach is being suggested, given the unlikely prospect of having states such as Singapore or Brunei, taking a liberal approach in exposing their governments to liability resulting from incursions into their citizens’ private matters.

The second challenge is the slow legislative process in certain ASEAN Member States. This was most evident in Cambodia and in the Lao People’s Democratic Republic when they were attempting to enact the measures suggested by the ASEAN e-commerce framework Agreement.\footnote{Review of e-commerce Legislation in the Association of Southeast Asian Nations, by the United Nations Conference on Trade and Development, p. 11 (2013).} Should the ASEAN embark on encouraging a legislative approach to promoting data protection in the region, one way to remedy this problem is by assisting national legislators in the drafting process. A previously-suggested approach, the drafting and publication by the ASEAN of a model law, would be helpful. Another approach is to reach out to legislators, through established legislative networks, and convincing them of the value of data protection legislation. The importance of government networks is quite apparent in this regard, since it could be an effective way to communicate the necessity of enacting the necessary legislation.

Third, it is expected that there will be relatively low levels of data protection awareness among government officials and employees in most of the ASEAN Member States. This was the experience of representatives who participated in the ASEAN e-commerce and cyberlaw workshops, and it is likely that the same will be true for data protection matters. As such, maximizing the potential of information networks, and information-sharing and capacity-building efforts, is key in order to raise the levels of awareness among the individuals who will be tasked to implement and enforce the ASEAN’s data protection Agreement, and its resulting policies and recommended measures.

It should also be noted that this lack of awareness, specifically awareness about the benefits of having, and the risks of not having a national data protection strategy, could be a factor in the seeming lack of will among legislators and other government officials to respond to the need for a national policy to promote data protection. Hence, raising awareness will also likely lead to an increase in willingness and a sense of urgency to consider various approaches to promote data protection in their respective countries.

Fourth, a lack of continuity in personnel with relevant technology and policy knowledge\footnote{See Id.} about data protection is a problem that should be anticipated by ASEAN. This could slow down the progress of the development of various enforcement, legislative, harmonization, and reporting and monitoring efforts that may have already been initiated. This explains the
necessity of having a national focal point, such as a DPA, who can lead a country’s data protection strategy. Having a DPA will ensure the existence of institutional knowledge and the presence of experts who have built up the relevant skills and information necessary to carry out the continuous work of promoting data protection locally and regionally.

Fifth, data protection is a constantly evolving field with continuously emerging innovations that must be dealt with constantly. The international data protection legal environment changes quickly, and new PETs swiftly emerge, alongside means of circumventing these technologies. As such, the ASEAN and its Member States should equip themselves with the necessary capabilities to keep up with emerging developments. A possible way to do this is by regularly revisiting data protection strategies, issuing updated versions of Implementation Guides and Checklists, encouraging research and the sharing of research results, and strengthening information-sharing and capacity building efforts.

Sixth, the drafting of legislation, deploying PETs, training law enforcement, and gaining technical knowledge and expertise in order to enforce the Agreement’s or a law’s provisions entail significant resources and expense. The ASEAN Member States’ governments are not on equal footing when it comes to the ability to shoulder these expenses. This could greatly hinder the progress of implementing the measures recommended by an ASEAN Data Protection Agreement. As such, it would be necessary to foster an environment wherein resource-sharing and capacity-building could be an option to respond to the lack of resources in certain ASEAN countries.

Finally, a situation wherein multiple government agencies have overlapping or conflicting roles in implementing and enforcing data protection legislation should be anticipated. Such a situation could arise when, in trying to fill legislative gaps, various regulatory or government bodies begin issuing regulations pertaining to data protection. Worse, there may be agency rules and regulations that may later on conflict with legislation. When faced with multiple data protection regulations, a government may have to grapple with several government agencies that have taken on the role of enforcing certain data protection policies and adjudicating related controversies. These powers may be inconsistent with the powers of a later-established DPA.

This may cause confusion among businesses and consumers who have little legal expertise to aid them in reconciling these conflicts on their own. Hence, when an ASEAN Member State enacts a data protection law, and establishes a DPA (or designates an existing government agency to take on the responsibilities commonly associated with DPAs), it should take steps to streamline, coordinate, and reconcile all relevant laws, rules, regulations, and the various responsibilities that may have been allocated to certain government agencies. Moreover, it should educate the public on the result of this streamlining and coordinating process.