ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN)

FRAMEWORK ON PERSONAL DATA PROTECTION

The Telecommunications and IT Ministers of Brunei Darussalam, the Kingdom of Cambodia, the Republic of Indonesia, the Lao People's Democratic Republic, Malaysia, the Republic of the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Kingdom of Thailand, and the Socialist Republic of Viet Nam (hereinafter referred to *collectively* as "ASEAN Member States" or "Participants"; or *individually* as "ASEAN Member State" or "Participant");

COMMITTED to an inclusive and integrated ASEAN through cooperation in the field of Information and Communications Technology (ICT) and to propel ASEAN towards a digitally-enabled economy that is secure, sustainable and transformative;

RECOGNISING the importance in strengthening personal data protection with a view to contributing to the promotion and growth of trade and flow of information within and among ASEAN Member States in the digital economy;

RECALLING the ASEAN Economic Community (AEC) Blueprint 2025 adopted by the ASEAN Leaders at the 27th ASEAN Summit on 22 November 2015 in Kuala Lumpur, Malaysia, which called for the establishment of a coherent and comprehensive framework for personal data protection;

FURTHER RECALLING the ASEAN ICT Masterplan 2020 (AIM2020) adopted at the 15th ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) on 27 November 2015 in Da Nang, Viet Nam, which called for greater cooperation and the development of a regional framework on personal data protection;

HAVING REGARD to the Asia-Pacific Economic Cooperation forum (APEC) Privacy Framework (2015) as well as other internationally recognised standards or frameworks on personal data protection;

DESIRING to foster closer understanding, information sharing, exchange of good practices, joint activities and cooperation in ASEAN in the area of personal data protection in accordance with the domestic laws, policies and regulations of ASEAN Member States;

HAVE REACHED the following understanding on this ASEAN Framework on Personal Data Protection (hereinafter referred to as "Framework"):

Objectives

1. This Framework serves to strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants, with a view to contribute to the promotion and growth of regional and global trade and the flow of information.

Effect of the Framework

2. This Framework serves only as a record of the Participants' intentions and does not constitute or create, and is not intended to constitute or create, obligations under domestic or international law and will not give rise to any legal process and will not be deemed to constitute or create any legally binding or enforceable obligations, express or implied.

Scope of the Framework

3. The Participants will endeavour to cooperate, promote and implement in their domestic laws and regulations the Principles of Personal Data Protection as set out in Paragraph 6 of this Framework (herein referred to as "Principles") while continuing to ensure and facilitate the free flow of information among the ASEAN Member States.

4. This Framework will not apply to:

   (a) Measures adopted by a Participant to exempt any areas, persons or sectors from the application of the Principles; and

   (b) Matters relating to national sovereignty, national security, public safety, public policy and all government activities deemed suitable by a Participant to be exempted.

5. Recognising the importance of cooperation, two or more Participants may enter into separate agreements to further strengthen collaboration on personal data protection in furtherance of the objectives of this Framework where practicable.

Principles of Personal Data Protection

6. The Participants recognise the need to protect and prevent misuse of an individual's personal data and will endeavour to take into account and implement in their domestic laws and regulations the following Personal Data Protection Principles (the "Principles") in accordance with this Framework:

Consent, Notification and Purpose

(a) An organisation should not collect, use or disclose personal data about an individual unless:

(i) the individual has been notified of and given consent to the purpose(s) of the collection, use or disclosure of his/her personal data; or

(ii) the collection, use or disclosure without notification or consent is authorised or required under domestic laws and regulations.

(b) An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.

Accuracy of Personal Data

(c) The personal data should be accurate and complete to the extent necessary for the purpose(s) for which the personal data is to be used or disclosed.

Security Safeguards

(d) The personal data should be appropriately protected against loss and unauthorised access, collection, use, disclosure, copying, modification, destruction or similar risks.

Access and Correction

(e) Upon request by an individual, an organisation should:

(i) provide the individual access to his/her personal data which is in the possession or under the control of the organisation within a reasonable period of time; and

(ii) correct an error or omission in his personal data, unless domestic laws and regulations require or authorise the organisation not to provide access or correct the personal data in the particular circumstances.

Transfers to Another Country or Territory

(f) Before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles.

Retention

(g) An organisation should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes.

Accountability

(h) An organisation should be accountable for complying with measures which give effect to the Principles.

(i) An organisation should, on request, provide clear and easily accessible information about its data protection policies and practices with respect to personal data in its possession or under its control. An organisation should also make available information on how to contact the organisation about its data protection policies and practices.

Implementation

7 Recognising the different levels of development of the Participants, a Participant may delay the application of this Framework until such time that it is ready to implement it by informing the other Participants in writing.

8 The Participants may undertake joint activities to strengthen cooperation and collaboration in the area of personal data protection which could include the following activities:

(a) Information sharing and exchange;

(b) Workshop, seminar or other capacity building activity; and

(c) Joint research in areas of mutual interest.

9 The implementation of joint activities, including the objectives, expected outcomes and work schedule, should be provided in separate project document(s) to be agreed upon by the Participants.

Financial Arrangements for Activities under the Framework

10. The financial arrangements to cover expenses for the joint activities under this Framework will be mutually agreed upon by the Participants. This Framework does not in any manner represent any commitment with regards to funding on the part of any Participant.

Confidentiality

11. A Participant will not communicate, disseminate, disclose or release to any third party any confidential document, information, or data received from the other Participant(s) in the course of the implementation of this Framework except to the extent as authorised in writing to do so by the other Participant providing such document, information or data. The Participants agree that the provisions of this Paragraph will continue to apply notwithstanding the termination of this Framework.

Amendments

12. This Framework may be amended at any time by mutual agreement of the Participants.

Settlement of Disputes

13. In the event of any dispute, Participants will resolve the dispute amicably through consultation or negotiations, without any reference to any third party or international tribunal.

Representation and Address of the Participants

14. The Participants agree to designate their respective data protection or privacy authorities, to be responsible for coordinating, implementing and managing activities relating to this Framework.

Final Provisions

15. This Framework will commence on the date of its adoption at the ASEAN Telecommunications and IT Ministers Meeting.

16. A Participant may at any time withdraw from this Framework by giving at least six (6) months written notice to the other Participants. Such withdrawal will not affect the implementation of any ongoing projects, programmes and/or activities, which have been jointly decided upon by Participants.

17. This Framework may be terminated by mutual written agreement of all Participants.

ADOPTED AT Bandar Seri Begawan, Brunei Darussalam, this twenty fifth day of November in the year two thousand and sixteen in one (1) original copy in the English language.