MODULE 4

DATA ISSUES

Article 4.1: Definitions

For the purposes of this Module:

computing facilities means computer servers and storage devices for processing or storing information for commercial use.

Article 4.2: Personal Information Protection

1. The Parties recognise the economic and social benefits of protecting the personal information of participants in the digital economy and the importance of such protection in enhancing confidence in the digital economy and development of trade.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce and digital trade. In the development of its legal framework for the protection of personal information, each Party shall take into account principles and guidelines of relevant international bodies.[11]

3. The Parties recognise that the principles underpinning a robust legal framework for the protection of personal information should include:

(a) collection limitation;

(b) data quality;

(c) purpose specification;

(d) use limitation;

(e) security safeguards;

(f) transparency;

(g) individual participation; and

(h) accountability.

[11] For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering data protection or privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to data protection or privacy.

4. Each Party shall adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.

5. Each Party shall publish information on the personal information protections it provides to users of electronic commerce, including how:

(a) individuals can pursue remedies; and

(b) businesses can comply with any legal requirements.

6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall pursue the development of mechanisms to promote compatibility and interoperability between their different regimes for protecting personal information. These mechanisms may include:

(a) the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement;

(b) broader international frameworks;

(c) where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or

(d) other avenues of transfer of personal information between the Parties.

7. The Parties shall exchange information on how the mechanisms in paragraph 6 are applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.

8. The Parties shall encourage adoption of data protection trustmarks by businesses that would help verify conformance to personal data protection standards and best practices.

9. The Parties shall exchange information on and share experiences on the use of data protection trustmarks.

10. The Parties shall endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information.

Article 4.3: Cross-Border Transfer of Information by Electronic Means

The Parties affirm their level of commitments relating to cross-border transfer of information by electronic means, in particular, but not exclusively:

"*1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.*

2. *Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.*

3. *Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:*

   (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

   (b) does not impose restrictions on transfers of information greater than are required to achieve the objective."

Article 4.4: Location of Computing Facilities

The Parties affirm their level of commitments relating to location of computing facilities, in particular, but not exclusively:

"*1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.*

2. *No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.*

3. *Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:*

   (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

   (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective."