ARTICLE 8.85

Location of computing facilities

1. A Party shall not require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

2. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 that are necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.

3. This Article does not apply to:

(a) government procurement; or

(b) information held or processed by or on behalf of a Party, or measures by a Party related to that information, including measures related to its collection.

ARTICLE 8.86

Commercial information and communication technology products that use cryptography[1]

1. A Party shall not require a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import or use of the commercial ICT product, to:

(a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, to that Party or a person in the territory of that Party;

(b) partner or otherwise cooperate with a person in the territory of that Party in the development, manufacture, sale, distribution, import or use of the commercial ICT product; or

(c) use or integrate a particular cryptographic algorithm or cipher.

2. This Article shall not preclude a regulatory body or judicial authority of a Party from requiring a manufacturer or supplier of a commercial ICT product that uses cryptography:

(a) to preserve and make available[1] any information to which subparagraph 1(a) applies for an investigation, inspection, examination, enforcement action or judicial proceeding, subject to safeguards against unauthorised disclosure; or

(b) to transfer or provide access to any information to which subparagraph 1(a) applies for the purpose of imposing or enforcing a remedy granted in accordance with that Party's competition law following an investigation, inspection, examination, enforcement action or judicial proceeding.

3. Notwithstanding paragraph 4 of Article 8.70, this Article applies to commercial ICT products that use cryptography.[2] This Article does not apply to:

(a) a Party's law enforcement authorities requiring service suppliers using encryption to provide access to encrypted and unencrypted communications pursuant to that Party's legal procedures;

(b) the regulation of financial instruments;

---

[1] For greater certainty, this Article does not affect the rights and obligations of a Party under Article 8.73.

[1] The Parties understand that this making available shall not be construed to negatively affect the status of any proprietary information relating to cryptography as a trade secret.

[2] For greater certainty, for the purposes of this Article, a commercial ICT product does not include a financial instrument.