5. This Section does not apply to gambling and betting services, broadcasting services, audio-visual services, services of notaries or equivalent professions, and legal representation services.

6. In the event of any inconsistency between the provisions of this Section and the other provisions of this Agreement, those other provisions shall prevail to the extent of the inconsistency.

ARTICLE 8.71

Definitions

For the purposes of this Section:

(a) "algorithm" means a defined sequence of steps, taken to solve a problem or obtain a result;

(b) "cipher" or "cryptographic algorithm" means a mathematical procedure or formula for combining a key with data (plaintext) to create a ciphertext;

(c) "ciphertext" means data in a form that cannot be easily understood without subsequent decryption;

(d) "commercial information and communication technology product" (commercial ICT product) means a product, including software, that is designed for commercial applications and whose intended function is information processing and communication by electronic means, including transmission and display, or electronic processing applied to determine or record physical phenomena, or to control physical processes;

(e) "computing facilities" means computer servers and storage devices for processing or storing information for commercial use;

(f) "covered person" means:

(i) a covered enterprise;

(ii) an entrepreneur of a Party; and

(iii) a service supplier of a Party,

but does not include a financial service supplier of a Party;

(g) "cryptography" means the principles, means or methods for the transformation of data in order to conceal or disguise its content, prevent its undetected modification or prevent its unauthorised use; and is limited to the transformation of information using one or more secret parameters, for example, crypto variables or associated key management;

(h) "electronic authentication" means the electronic process or act of verifying the identity of a party to an electronic communication or transaction, or ensuring the origin and integrity of an electronic communication;

(i) "electronic signature" means data in electronic form which is in, affixed to or logically associated with other electronic data and that may be used to:

(i) identify the person in relation to the electronic data;

(ii) indicate the person's approval of the information contained in the electronic data; and

(iii) confirm that the information in the electronic data has not been altered;

(j) "encryption" means the conversion of data (plaintext) through the use of a cryptographic algorithm into a ciphertext using the appropriate key;

(k) "government information" means non-proprietary information, including data, held by the central government;

(l) "key" means a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that a person with knowledge of the key can reproduce or reverse the operation, but a person without knowledge of the key cannot;