Chapter 8: Digital Trade – Text of the 2023 Canada - Ukraine Free Trade Agreement

Article 8.1: Definitions

For the purposes of this Chapter:

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

computing facility means a computer server or storage device for processing or storing information for commercial use;

digital product means a computer program, text, video, image, sound recording, or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically;

electronic address means an address used in connection with the transmission of an electronic message to an electronic mail account, instant messaging account, telephone account, or any similar account;

electronic authentication means the process or act of verifying the identity of a party to an electronic communication or transaction and ensuring the integrity of an electronic communication;

electronic message means a message sent by any means of telecommunication, including a text, sound, voice, or image message;

electronic signature means data in electronic form that is in, affixed to, or logically associated with, an electronic document or message, and that may be used to identify the signatory in relation to the electronic document or message and indicate the signatory's approval of the information contained in the electronic document and message;

commercial electronic message means an electronic message in any form intended to directly or indirectly promote goods, works, or services, or the business reputation of a person engaged in an economic or independent professional activity;

enterprise means an entity constituted or organized under applicable law, whether or not for profit, and whether privately-owned or governmentally-owned or controlled, including a corporation, trust, partnership, sole proprietorship, joint venture, association or similar organization, and a branch of an enterprise;

government data means data held by the central government, disclosure of which is not restricted under domestic law, and which a Party makes digitally available for public access and use;

metadata means structural or descriptive information about data, such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and context;

personal data means information relating to an identified or identifiable natural person;

unsolicited commercial electronic message means an electronic message that is sent for commercial or marketing purposes to an electronic address without the consent of the recipient or against the explicit rejection of the recipient;

significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property.

Article 8.2: Scope

1. This Chapter applies to measures adopted or maintained by a Party that affect trade by electronic means.

2. This Chapter does not apply to:

- (a) government procurement; or
- (b) information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection, except for Articles 8.7(6), 8.7(7), 8.7(8), and 8.13.

3. For greater certainty, a measure that affects the supply of a service delivered or performed electronically is subject to the relevant provisions of Chapter 17 (Investment), Chapter 18 (Cross-Border Trade in Services) and Chapter 20 (Financial Services).

4. Articles 8.10 and 8.11 shall not apply to the non-conforming aspects of measures adopted or maintained in accordance with Article 17.18 (Non-Conforming Measures), Article 18.7 (Reservations), or Article 20.10 (Non-Conforming Measures).

Article 8.3: Access to and Use of the Internet for Digital Trade

1. The Parties recognize that it is beneficial for consumers in their territories to be able to:

- (a) access and use services and applications of a consumer's choice available on the Internet;
- (b) connect end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and
- (c) access information on the network management practices of a consumer's Internet access service supplier.

Article 8.4: Electronic Transactions

1. Except for circumstances provided for under its law, a Party shall not deny the legal validity of a transaction, including any document or contract related to the transaction, solely on the basis that it is in electronic form.

2. Each Party shall endeavour to avoid unnecessary regulatory burden on electronic transactions and facilitate input by interested persons in the development of its legal framework for electronic transactions.

Article 8.5: Electronic Authentication and Electronic Signatures

1. Except in circumstances provided for under its law, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.

2. A Party shall not adopt or maintain measures for electronic authentication and electronic signatures that would:

- (a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods or electronic signatures for that transaction; or
- (b) prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with a legal requirement with respect to authentication or electronic signatures.

3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the method of authentication or electronic signature meets certain performance standards or is certified by an authority accredited in accordance with its law.

4. Each Party shall encourage the use of interoperable electronic authentication.

Article 8.6: Online Consumer Protection

1. The Parties recognize the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent, misleading, or deceptive commercial activities when they engage in digital trade.

2. Each Party shall adopt or maintain consumer protection laws that address fraudulent, misleading or deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

3. The Parties recognize the importance of, and public interest in, cooperation between their respective national consumer protection authorities or other relevant bodies on activities related to cross-border digital trade, including the exchange of consumer complaints and other enforcement information as appropriate, in order to enhance consumer protection and their welfare.

Article 8.7: Personal Data Protection

1. The Parties recognize the economic and social benefits of protecting personal data of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal data of the users of

digital trade, taking into account the principles and guidelines of relevant international bodies. These principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability.

3. Each Party shall endeavour to adopt or maintain non-discriminatory practices in protecting users of digital trade from personal data protection violations within its jurisdiction.

4. Each Party shall publish information on the personal data protections it provides to users of digital trade as part of its legal frameworks, including how:

- (a) a natural person can access their own personal data;
- (b) a natural person can pursue a remedy; and
- (c) an enterprise can comply with legal requirements.

5. Recognizing that the Parties may take different legal approaches to protecting personal data, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. The Parties shall endeavour to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.

6. A Party shall not use the personal data of natural persons obtained from an enterprise operating within its jurisdiction in a manner that constitutes targeted discrimination on manifestly wrongful grounds such as race, colour, sex, sexual orientation, gender, language, religion, political or other opinion, national or social origin, property, medical, birth, or other status, genetic identity, age, ethnicity, or disability.

7. Each Party shall endeavour to ensure that any personal data disclosed to a government authority by an enterprise is protected against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

8. Each Party shall ensure that any personal data disclosed to a government authority by an enterprise is not collected, created, accessed, disclosed, used, retained or modified by a government authority in a manner that can reasonably be expected to cause significant harm to a natural person.[Footnote 1]

9. The Parties acknowledge that their respective legal frameworks provide a suitable level of protection for personal information, including for personal information transferred between their jurisdictions.

10. Unless a modification to the other Party's existing measures results in a materially lower standard of protection of personal

information, a Party shall not adopt or maintain a measure for the protection of personal information that applies solely to cross-border transfers of personal information required for the conduct of business between the jurisdictions of the Parties, in a manner that modifies the conditions of competition to the detriment of service suppliers or enterprises of the other Party.

Article 8.8: Unsolicited Commercial Electronic Messages

1. Each Party shall adopt or maintain measures providing for the limitation of unsolicited commercial electronic messages.

2. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that:

- (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent the ongoing reception of those messages; or
- (b) require the consent, as specified in the measures of each Party, of recipients to receive commercial electronic messages.

3. The Parties shall endeavour to cooperate in cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

Article 8.9: Prohibition of Customs Duties on Digital Products Transmitted Electronically

1. A Party shall not impose customs duties on a digital product transmitted electronically between a person of one Party and a person of another Party.

2. For greater certainty, paragraph 1 does not prevent a Party from imposing internal taxes, fees, or other charges on a digital product transmitted electronically, provided that those taxes, fees, or charges are imposed in a manner consistent with this Agreement.

Article 8.10: Cross-Border Transfer of Information by Electronic Means

1. A Party shall not restrict the cross-border transfer of information by electronic means, including personal data if such activity is for the conduct of the business of an enterprise.

2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is 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. Paragraph 1 does not apply to a financial institution of the other Party or a cross-border financial service supplier of the other Party as defined in Chapter 20 (Financial Services).

Article 8.11: Location of Computing Facilities

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

2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is 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. Paragraph 1 does not apply to a financial institution of the other Party or a cross-border financial service supplier of the other Party as defined in Chapter 20 (Financial Services).

Article 8.12: Source Code

1. A Party shall not require the transfer of, or access to, source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, for a specific investigation, inspection, examination enforcement action, or judicial proceeding [Footnote2] , subject to safeguards against unauthorized disclosure.

Article 8.13: Open Government Data

1. The Parties recognize the benefit of making data held by a regional or local government digitally available for public access and use in a manner consistent with paragraphs 2 to 4.

2. The Parties recognise that facilitating public access to and use of government data fosters economic and social development,

competitiveness, and innovation. To this end, each Party shall endeavour to expand the coverage of such data, such as through engagement and consultation with interested stakeholders.

3. To the extent that a Party chooses to make government data digitally available for public access and use, each Party shall endeavour, to the extent practicable, to ensure that such data is:

- (a) made available in a machine-readable and open format;
- (b) searchable and retrievable;
- (c) updated, as applicable, in a timely manner; and
- (d) accompanied by metadata that is, to the extent possible, based on commonly used formats that allow the user to understand and utilise the data.

A Party shall further endeavour to make this data generally available at no or reasonable cost to the user.

4. To the extent that a Party chooses to make government data digitally available for public access and use, it shall endeavour to avoid imposing conditions [Footnote 3] that unduly prevent or restrict the user of such data from:

- (a) reproducing, redistributing, or republishing the data;
- (b) regrouping the data; or

- (c) using the data for commercial and non-commercial purposes, including in the process of production of a new product or service.

5. The Parties shall endeavour to cooperate in matters that facilitate and expand public access to and use of government data, including exchanging information and experiences on practices and policies, with a view to encouraging the development of digital trade and creating business opportunities, especially for small and medium-sized enterprises (SMEs).

Footnotes

Footnote 1

For greater certainty, the public disclosure of personal data that can reasonably be expected to cause significant harm does not constitute a violation of this obligation provided that it is not inconsistent with paragraph 6 of this Article and that it is done for the purposes of legitimate law enforcement activities, judicial proceedings, compliance with regulatory requirements, or national security.

Return to footnote1referrer

Footnote 2

This disclosure shall not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner.

Return to footnote2referrer

Footnote 3

For greater certainty, this paragraph does not prevent a Party from requiring a user of such data to link to original sources.

Return to footnote3referrer