Ukraine No. 2 (2023)

Digital Trade Agreement

between the United Kingdom of Great Britain and Northern Ireland
and Ukraine

London and Kyiv, 20 March, 5 and 11 May 2023

[The Agreement is not in force]

Presented to Parliament
by the Secretary of State for Foreign, Commonwealth and Development Affairs
by Command of His Majesty
May 2023

CP 837

This publication is available at www.gov.uk/official-documents

Any enquiries regarding this publication should be sent to us at Treaty Section, Foreign, Commonwealth and Development Office, King Charles Street, London, SW1A 2AH

ISBN 978-1-5286-4042-8
E02894410 05/23

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Global on behalf of the Controller of His Majesty's Stationery Office

DIGITAL TRADE AGREEMENT BETWEEN THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND UKRAINE

The United Kingdom of Great Britain and Northern Ireland ("the United Kingdom") and Ukraine (hereinafter jointly referred to as "the Parties" or individually referred to as "Party"),

Recognising the Parties' deep and longstanding relationship, underpinned by the Political, Free Trade and Strategic Partnership Agreement between the United Kingdom and Ukraine, done at London on 8 October 2020, which entered into force on 31 December 2020, as amended (the "UK-Ukraine Agreement");

Recognising the economic opportunities brought about by the digital economy to help Ukraine rebuild its economy and protect livelihoods;

Sharing a vision for greater integration and the digital transformation of the Parties' economies;

Reflecting the forward-looking nature of their partnership and commitment to deepen bilateral cooperation in new and emerging areas;

Further recognising the importance of ensuring all people and businesses of all sizes can participate in, contribute to, and benefit from the digital economy including the fundamental role of Small and Medium Sized Enterprises (SMEs) in maintaining dynamism and enhancing competitiveness;

Resolving to facilitate a trusted and secure digital environment that promotes consumer and business interests;

Desiring to establish a dynamic framework for cooperation in the fast-paced and evolving digital economy; and

Building on the Parties' rights, obligations and undertakings in the World Trade Organization ("WTO"), and other international and bilateral agreements and arrangements concerning digital trade and the digital economy,

Have agreed as follows:

ARTICLE 1

Digital Trade Agreement

For the purposes of this Digital Trade Agreement, "this Digital Trade Agreement" means this Digital Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and Ukraine.

ARTICLE 2

Amendment of UK-Ukraine Agreement

The Parties hereby agree to amend the UK-Ukraine Agreement as follows:

(a) replace the provisions of Section 6 (Electronic Commerce) of Chapter 6 (Establishment, Trade in Services and Electronic Commerce) of Title IV of the UK-Ukraine Agreement with the provisions as set out in Annex A to this Digital Trade Agreement; and

(b) amend the UK-Ukraine Agreement as set out in Annex B to this Digital Trade Agreement.

ARTICLE 3

Integral Parts

1. This Digital Trade Agreement shall form an integral part of the UK-Ukraine Agreement.

2. The Annexes and footnotes to this Digital Trade Agreement shall form an integral part thereof.

ARTICLE 4

Final Provisions

1. This Digital Trade Agreement shall enter into force on the first day of the second month following the date of the later of the Parties' written notifications certifying that they have completed their respective applicable legal requirements and procedures for the entry into force of this Digital Trade Agreement. The Parties may agree in writing on another date for entry into force, provided such date occurs after the completion of the exchange of notifications referred to above.

2. Any time after the date of entry into force of this Digital Trade Agreement, the application of this Digital Trade Agreement, or specified provisions of this Digital Trade Agreement, may be extended to Gibraltar on the first day of the second month following the United Kingdom's written notification to Ukraine certifying the completion of the applicable legal requirements and procedures for the extension of this Digital Trade Agreement, or specified provisions of this Digital Trade Agreement, in respect of Gibraltar. The Parties may agree in writing on another date, provided such date occurs after the United Kingdom's written notification referred to above.

3. Any time after the date of entry of force of this Digital Trade Agreement, the application of this Digital Trade Agreement, or specified provisions of this Digital Trade Agreement, may be extended to:

   (a) the Bailiwick of Guernsey;

   (b) the Bailiwick of Jersey; or

   (c) the Isle of Man,

   on the first day of the second month following the United Kingdom's written notification to Ukraine certifying the completion of applicable legal requirements and procedures for the extension of this Digital Trade Agreement, or specified provisions of this Digital Trade Agreement, in respect of such territory.[1] The Parties may agree in writing on another date, provided such date occurs after the date of the United Kingdom's written notification referred to above.

4. The United Kingdom shall submit notifications under this Article to the Ministry of Foreign Affairs of Ukraine or its successor. Ukraine shall submit notifications under this Article to the United Kingdom's Foreign, Commonwealth and Development Office or its successor.

5. At any time after the date that the application of this Digital Trade Agreement has been extended to a territory referred to in paragraphs 2 and 3, the United Kingdom may give written notice to Ukraine that this Digital Trade Agreement, or specified provisions of this Digital Trade Agreement, shall no longer apply to such territory. A notification pursuant to this paragraph will take effect six months after notification.

IN WITNESS WHEREOF the undersigned, duly authorised thereto by their respective Governments, have signed this Digital Trade Agreement.

[1] The Parties agree that, prior to this, the United Kingdom shall hold consultations with Ukraine concerning the application of relevant provisions of the UK-Ukraine Agreement to such territory.

DONE at London and Kyiv, this twentieth day of March and this fifth and eleventh day of May, 2023, in two originals, in the English and Ukrainian languages, both texts being equally authentic.

For the United Kingdom of Great Britain and Northern Ireland:	**For Ukraine:**
KEMI BADENOCH	**YULIA SVYRYDENKO**

ANNEX A

SECTION 6
ELECTRONIC COMMERCE

ARTICLE 131

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

(c) "commercial information and communication technology product"[2] ("Commercial Information and Communications Technology (ICT) Product") means a product that is used 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;

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

(e) "covered person" means:

(i) an establishment of a Party as defined in Article 82(9) of this Agreement;

(ii) an investor as defined in Article 82(10) of this Agreement; or

(iii) a service supplier of a Party as defined in Article 82(16) of this Agreement;

but does not include a financial service supplier as defined in Article 119(2)(c) of this Agreement;

(f) "cryptographic algorithm" means a defined method of transforming data using cryptography;

[2] For greater certainty, for the purposes of this Section, a commercial ICT product is a good or a service, and does not include a financial instrument.

(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 principles, means or methods where one or more secret parameters, for example, crypto variables, or associated key management is required in order to transform the data or to perform a corresponding reverse transformation;

(h) "customs duty" includes a charge of any kind imposed on or in connection with importation or exportation;

(i) "electronic authentication" means an electronic process that enables the confirmation of:

(i) the electronic identification of a person; or

(ii) the origin and integrity of data in electronic form;

(j) "electronic invoicing" means the automated creation, exchange, and processing of requests for payments between suppliers and buyers using a structured digital format;

(k) "electronic registered delivery service" means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

(l) "electronic seal" means data in electronic form used by an enterprise which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

(m) "electronic signature" means data in electronic form that is in, affixed to, or logically associated with an electronic data message that may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message[3];

(n) "electronic time stamp" means data in electronic form which binds other data in electronic form to a particular time, establishing evidence that the latter data existed at that time;

[3] For greater certainty, nothing in this provision prevents a Party from according greater legal effect to an electronic signature that satisfies certain requirements, such as indicating that the electronic data message has not been altered or verifying the identity of the signatory.

(o) "electronic transferable record" means a document or instrument in electronic form which under a Party's laws or regulations is both functionally equivalent to a transferable record and satisfies quality requirements such as those referenced in Article 10 of the *UNCITRAL Model Law on Electronic Transferable Records of 2017*;

(p) "electronic transmission" or "transmitted electronically" means a transmission made using any electromagnetic means, including by photonic means;

(q) "electronic trust service" means an electronic service consisting of:

(i) the creation, verification, and validation of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, and certificates related to those services;

(ii) the creation, verification, and validation of certificates for website authentication; or

(iii) the preservation of electronic signatures, seals, or certificates related to those services.

(r) "emerging technology" means an enabling and innovative technology that has potentially significant application across a wide range of existing and future sectors, including:

(i) artificial intelligence;

(ii) distributed ledger technologies;

(iii) quantum technologies;

(iv) immersive technologies;

(v) sensing technologies;

(vi) digital twins; and

(vii) the Internet of Things;

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

(t) "end-user" means a natural person, or legal person to the extent provided for in a Party's laws and regulations, using or requesting a

public telecommunications service, either as a consumer or for trade, business, or professional purposes;

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

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

(w) "personal data" means any information, including data, about an identified or identifiable natural person;

(x) "public telecommunications service" means any telecommunications service that is offered to the public generally;

(y) "telecommunications" means the transmission and reception of signals by any electromagnetic means;

(z) "trade administration document" means the forms and documents issued or controlled by a Party that must be completed by or for an importer or exporter in connection with the import or export of goods; and

(aa) "unsolicited commercial electronic message" means an electronic message[4] that is sent for commercial or marketing purposes directly to an end-user via a public telecommunications service, without the consent of the recipient or despite the explicit rejection of the recipient.

ARTICLE 132

Objectives

1. The Parties recognise the economic benefits of, and opportunities provided by, open digital markets.

2. The Parties further recognise the importance of:

(a) avoiding unnecessary barriers to the use and development of digital trading systems;

[4] For greater certainty, an electronic message includes electronic mail and text (Short Message Service) and multimedia (Multimedia Message Service) messages.

(b) promoting the interoperability of domestic frameworks to facilitate digital trade;

(c) international cooperation with a view to developing international frameworks to govern digital trade that are free, fair and inclusive; and

(d) adopting international and domestic frameworks that:

(i) support the principle of technological neutrality;

(ii) take into account emerging technologies; and

(iii) advance the interests of consumers and businesses engaged in digital trade, whilst promoting consumer confidence in it.

ARTICLE 132-A

Scope and General Provisions

1. This Section shall apply to measures adopted or maintained by a Party affecting trade enabled by electronic means.

2. This Section shall not apply to audio-visual services.

3. Articles 132-K (Cross-Border Transfer of Information by Electronic Means) and 132-L (Location of Computing Facilities) shall not apply to information held or processed by or on behalf of a Party, or measures adopted or maintained by a Party related to that information, including measures related to its collection.

4. Articles 132-K (Cross-Border Transfer of Information by Electronic Means), 132-L (Location of Computing Facilities), [132-P] (Source Code), and 132-O (Commercial Information and Communication Technology Products that Use Cryptography) shall not apply to government procurement.

5. For greater certainty, a measure that affects the supply of a service delivered or performed electronically is subject to the obligations contained in relevant provisions of Section 2 (Establishment), Section 3 (Cross-Border Supply of Services), and Section 5 (Regulatory Framework) of this Chapter, including exceptions or reservations, as set out in this Agreement, that are applicable to those obligations.

ARTICLE 132-B

Customs Duties

1. Neither Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a natural or legal person of a Party and a natural or legal person of the other Party.

2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees, or other charges on electronic transmissions, including content transmitted electronically, provided that such taxes, fees, or charges are imposed in a manner consistent with this Agreement.

ARTICLE 132-C

Domestic Electronic Transactions Framework

1. Each Party shall maintain a legal framework governing electronic transactions consistent with the principles of the *UNCITRAL Model Law on Electronic Commerce (1996) with additional Article 5 bis as adopted* in 1998, adopted by the United Nations General Assembly on 12 June 1996 (additional Article 5 *bis* adopted in 1998), or the *United Nations Convention on the Use of Electronic Communications in International Contracts*, done at New York on 23 November 2005.

2. Each Party shall endeavour to:

   (a) avoid any unnecessary regulatory burden on electronic transactions; and

   (b) facilitate input by interested persons in the development of its legal framework for electronic transactions.

3. The Parties recognise the importance of facilitating the use of electronic transferable records. To this end, each Party shall endeavour to establish a legal framework governing electronic transferable records consistent with the *UNCITRAL Model Law on Electronic Transferable Records (2017)*, adopted by the United Nations Commission on International Trade Law (UNCITRAL) on 13 July 2017.

ARTICLE 132-D

Conclusion of Contracts by Electronic Means

1. Except in circumstances otherwise provided for in its law, each Party shall ensure that:

(a) its legal framework allows for contracts to be concluded by electronic means; and

(b) its law neither creates obstacles for the use of electronic contracts nor results in electronic contracts being deprived of legal effect, enforceability, or validity, solely on the ground that the contract has been made by electronic means.

2. The Parties recognise the importance of transparency for minimising barriers to the use of electronic contracts in digital trade. To this end, each Party shall:

(a) promptly publish the circumstances referred to in paragraph 1 on a single official website hosted by the central level of government; and

(b) review those circumstances with a view to reducing them over time.

ARTICLE 132-E

Electronic Authentication and Electronic Trust Services

1. The Parties recognise the benefits of electronic authentication and electronic trust services in providing greater certainty, integrity, and efficiency in the electronic transfer of information. Accordingly, the Parties recognise the important contribution of these services to consumer and business trust in the digital economy.

2. Except in circumstances otherwise provided for under its laws and regulations, neither Party shall deny the legal effect and admissibility as evidence in legal proceedings of an electronic document, an electronic signature, an electronic seal, an electronic time stamp, the authenticating data resulting from electronic authentication, or data sent and received using an electronic registered delivery service, solely on the ground that it is in electronic form.

3. Neither Party shall adopt or maintain a measure that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication method or electronic trust service for their transaction; or

(b) prevent parties to an electronic transaction from being able to prove to judicial and administrative authorities that the use of electronic authentication or an electronic trust service in that transaction complies with the applicable legal requirements.

4. Notwithstanding paragraph 3, a Party may require that for a particular category of transactions, the method of electronic authentication or electronic trust service is certified by an authority accredited in accordance with its law or meets certain performance standards which shall be objective, transparent, and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned.

5. The Parties shall encourage the use of interoperable electronic trust services and electronic authentication, work towards the mutual recognition of electronic trust services and electronic authentication, and endeavour to engage in regulatory cooperation.

ARTICLE 132-F

Electronic Invoicing

1. The Parties recognise the importance of electronic invoicing to increase the efficiency, accuracy and reliability of commercial transactions. Each Party also recognises the benefits of ensuring that the systems used for electronic invoicing within its territory are interoperable with the systems used for electronic invoicing in the other Party's territory.

2. Each Party shall ensure that the implementation of measures related to electronic invoicing in its territory is designed to support cross-border interoperability between the Parties' electronic invoicing frameworks. To this end, each Party shall take into account international frameworks when developing measures related to electronic invoicing.

3. The Parties recognise the economic importance of promoting the global adoption of interoperable electronic invoicing systems. To this end, the Parties shall share best practices and collaborate, where appropriate, on promoting the adoption of interoperable systems for electronic invoicing.

ARTICLE 132-G

Paperless Trading

1. The Parties recognise the importance of digital connectivity in enabling trade. To this end, each Party shall:

   (a) make trade administration documents available to the public in electronic form and in English.

   (b) accept completed electronic versions of trade administration documents as the legal equivalent of paper documents, except where:

(i) that Party is subject to a domestic or international legal requirement to the contrary; or

(ii) doing so would reduce the effectiveness of the trade administration process.

2. The Parties shall, where appropriate, cooperate bilaterally and in international fora on matters related to paperless trading, including by promoting the acceptance of electronic versions of trade administration documents and supporting documents.

3. In developing initiatives concerning the use of paperless trading, each Party shall endeavour to take into account the principles and guidelines of relevant international bodies.

ARTICLE 132-H

Logistics

1. The Parties recognise the importance of efficient cross-border logistics which help lower the cost and improve the speed and reliability of supply chains.

2. The Parties shall endeavour to share best practices and general information regarding the logistics sector, including:

(a) last mile deliveries, including on-demand and dynamic routing solutions;

(b) the use of electric, remote controlled and autonomous vehicles;

(c) facilitating the availability of cross-border options for the delivery of goods, such as parcel lockers; and

(d) new delivery and business models for logistics.

ARTICLE 132-I

Standards and Conformity Assessment

1. The Parties recognise the importance and contribution of standards, technical regulations and conformity assessment procedures in fostering a well-functioning digital economy, and further recognise their role in reducing barriers to trade by increasing compatibility, interoperability and reliability.

2. The Parties shall endeavour to participate and cooperate or, where appropriate, encourage their respective bodies to participate and cooperate,

in areas of mutual interest in international fora that both Parties are party to, to promote the development of standards relating to digital trade.

3. The Parties recognise that mechanisms that facilitate the cross-border recognition of conformity assessment results can support the digital economy.

4. To this end, the Parties shall endeavour or, where appropriate, encourage their respective bodies, in areas of mutual interest, to:

   (a) exchange best practices relating to the development and application of standards, technical regulations and conformity assessment procedures that are related to the digital economy;

   (b) participate actively in international fora that both Parties or their respective bodies are party to in order to develop standards that are related to digital trade and to promote their adoption;

   (c) identify, develop, and promote joint initiatives in the field of standards and conformity assessment that are related to digital trade;

   (d) actively consider the other Party's and its respective bodies' proposals for cooperation on standards, technical regulations and conformity assessment procedures relating to digital trade; and

   (e) cooperate between governmental and non-governmental bodies, including cross-border research or test-bedding projects, to develop a greater understanding, between the Parties and industry, of standards, technical regulations and conformity assessment procedures.

5. The Parties acknowledge the importance of information exchange and transparency with regard to the preparation, adoption and application of standards, technical regulations and conformity assessment procedures for digital trade. Each Party should endeavour to, upon request, or where appropriate, encourage its respective bodies to provide information on standards, technical regulations and conformity assessment procedures relating to digital trade, in print or electronically, within a reasonable period of time agreed by the Parties and, if possible, within 60 days.

ARTICLE 132-J

Personal data Protection

1. The Parties recognise the importance of high standards of personal data protection and that protecting personal data provides economic and social benefits, which enhance confidence and trust in digital trade.

2. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal data of natural persons.

3. In the development of its legal framework for the protection of personal data, each Party shall take into account principles and guidelines of relevant international bodies. The principles underpinning each Party's personal data protection framework shall include:

   (a) collection and usage limitation;

   (b) data quality;

   (c) purpose specification;

   (d) security safeguards;

   (e) transparency;

   (f) individual participation; and

   (g) accountability.

4. Each Party shall adopt non-discriminatory practices in protecting natural persons from personal data protection violations occurring within its jurisdiction.

5. Each Party recognises that natural persons should be able to access information regarding the protection of personal data, including remedies or recourse. Accordingly, each Party shall publish information on the personal data protections it provides to natural persons, including how:

   (a) natural persons can pursue remedies, or recourse; and

   (b) businesses can comply with any legal requirements.

6. Each Party shall promote compatibility between their respective legal frameworks for protecting personal data and pursue the development of mechanisms to promote interoperability between these frameworks. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks.

7. To this end, the Parties shall exchange information on any mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote interoperability and compatibility between them.

ARTICLE 132-K

Cross-Border Transfer of Information by Electronic Means

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

2. Neither Party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal data, if 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 a measure 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 132-L

Location of Computing Facilities

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. Neither 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 a measure 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.

ARTICLE 132-M

Open Government Information

1. For the purposes of this Article, "government information" means non-proprietary information held by the central level of government and, to the extent provided for under a Party's laws and regulations, by other levels of government.[5]

2. The Parties recognise that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation. To this end, each Party is encouraged to expand the coverage of government information digitally available for public access and use, through engagement and consultation with interested stakeholders.

3. Each Party shall provide interested persons with a mechanism to request the disclosure of specific government information.

4. To the extent that a Party chooses to make government information available to the public, it shall endeavour to ensure that the information is:

   (a) in a machine-readable and open format, and can be searched, retrieved, used, reused, and redistributed;

   (b) accompanied by metadata that is, to the extent possible, based on commonly used formats that allow the user to understand and utilise the data; and

   (c) to the extent practicable, made available in a spatially enabled format with reliable, easy to use, and freely available Application Programming Interfaces, and is regularly updated.

5. To the extent that a Party chooses to make government information available to the public, it shall endeavour to avoid imposing conditions[6] that unduly prevent or restrict the user of that information from:

   (a) reproducing, redistributing, or republishing the information;

   (b) regrouping the information; or

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

[5] This Article is without prejudice to a Party's laws pertaining to intellectual property and personal data protection.

[6] For greater certainty, nothing in this paragraph prevents a Party from requiring a user of that information to link to original sources.

6. The Parties shall endeavour to cooperate to identify ways in which each Party can expand access to and use of government information that the Party has made public, with a view to enhancing and generating business opportunities, especially for Small and Medium Sized Enterprises (SMEs).

ARTICLE 132-N

Data Innovation

1. The Parties recognise that digitalisation and the use of data promote economic growth. To support the cross-border transfer of information by electronic means and promote data-driven innovation, the Parties further recognise the need to create an environment that enables, supports, and is conducive to, experimentation and innovation, including through the use of regulatory sandboxes where applicable.

2. The Parties shall endeavour to support data innovation through:

   (a) collaborating on data sharing projects, including projects involving researchers, academics and industry, using regulatory sandboxes as required to demonstrate the benefits of the cross-border transfer of information by electronic means;

   (b) cooperating on the development of policies and standards for data mobility, including consumer data portability; and

   (c) sharing policy approaches and industry practices related to data sharing, such as data trusts.

ARTICLE 132-O

Commercial Information and Communication Technology Products that Use Cryptography

1. Neither Party shall require a manufacturer or supplier of a commercial ICT product that uses cryptography[7] to, at any time prior to or post market entry, as a condition for the manufacture, sale, distribution, import or use of the commercial ICT product:

   (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;

[7] For the purposes of this Article, a commercial ICT product does not include a financial instrument.

(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.

2. Paragraph 1 shall not apply to:

(a) the regulation of financial instruments;

(b) a requirement that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by that Party and are exclusively for use in the exercise of government functions, including those of central banks;

(c) a measure adopted or maintained by a Party in the exercise of supervisory, investigatory or examination authority relating to financial service suppliers or financial markets;

(d) the manufacture, sale, distribution, import or use of a commercial ICT product by or for a Party;

(e) a requirement imposed or enforced, or a commitment or undertaking enforced, by a judicial authority, a regulatory body, or a competition authority pursuant to a Party's competition law, to prevent or remedy a restriction or a distortion of competition; or

(f) a decision, by a regulatory body or a judicial authority of a Party, requiring a manufacturer or supplier of a commercial ICT product that uses cryptography to preserve and make available[8] any information to which subparagraph (a) of paragraph 1 applies in furtherance of an investigation, inspection, examination, enforcement action or a judicial proceeding.

3. Where proprietary information relating to cryptography of a commercial ICT product that uses cryptography has been revealed to a Party upon its request, that Party shall adopt or maintain measures to prevent the unauthorised disclosure of proprietary information contained in or related to a commercial ICT product that uses cryptography. To this end, each Party shall provide for appropriate safeguards against that disclosure, including by limiting the access to and use of that information to those who are essential to the performance of those activities only.

4. Nothing in this Article shall be construed to:

[8] 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.

(a) affect the rights and obligations of a Party under Article 132-P (Source Code) of this Agreement; or

(b) preclude a Party's law enforcement authorities from requiring a service supplier using encryption to provide, pursuant to that Party's legal procedures, access to encrypted and unencrypted communications.

ARTICLE 132-P

Source Code

1. Neither Party shall require the transfer of, or access to, source code[9] of software owned by a person of the other Party.

2. Nothing in this Article shall be construed to:

(a) preclude a regulatory body or a judicial authority of a Party, or a designated conformity assessment body operating in a Party's territory, from requiring a person of the other Party to preserve and make available[10] the source code of software in furtherance of an investigation, inspection, examination, enforcement action, or judicial proceedings; or

(b) apply to a remedy imposed, enforced, or adopted by a regulatory body or a judicial authority of a Party, in accordance with a Party's law following an investigation, inspection, examination, enforcement action, or judicial proceeding.

3. Where source code of software owned by a person of the other Party has been revealed to a Party, or to a designated conformity assessment body operating in a Party's territory, on its request, that Party shall adopt or maintain measures to prevent the unauthorised disclosure of source code of software. To this end, each Party shall provide for appropriate safeguards against that disclosure, including by limiting the access to and use of that source code of software to those who are essential to the performance of that activity only.

4. This Article shall not apply to the voluntary transfer of, or granting of access to, source code of software by a person of the other Party:

[9] For the purposes of this Article, a reference to "source code" includes an algorithm embedded in the source code, but does not include the expression of that algorithm in any other form, including in prose.

[10] The Parties understand that this making available shall not be construed to negatively affect the status of the source code of software as a trade secret.

(a) on a commercial basis, such as in the context of a freely negotiated contract; or

(b) under open source licences, such as in the context of open source coding.

ARTICLE 132-Q

Cyber Security

1. The Parties recognise that threats to cyber security undermine confidence in digital trade. The Parties also recognise the importance of:

   (a) workforce development in the area of cyber security, including through training and development, and possible initiatives relating to mutual recognition of qualifications; and

   (b) enhancing the cyber security capability of businesses, including SMEs, and enabling greater cyber security resilience within industry.

2. The Parties shall endeavour to:

   (a) build the capabilities of their respective national entities responsible for cyber security incident response, taking into account the evolving nature of cyber security threats;

   (b) maintain cooperation to anticipate, identify, and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and to swiftly address cyber security incidents;

   (c) cooperate by sharing information and best practices on matters related to cyber security, which may include measures and non-legal interventions; and

   (d) support the development of open, transparent, industry-led, multi-stakeholder and consensus-based technical standards.

3. Given the evolving nature of cyber security threats, the Parties recognise that risk-based approaches may be more effective than prescriptive approaches in addressing those threats. Accordingly, each Party shall endeavour to employ, and shall encourage enterprises within its jurisdiction to use, risk-based approaches to:

   (a) manage cyber security risks and to detect, respond to and recover from cyber security events; and

   (b) improve their cyber resilience.

ARTICLE 132-R

Online Consumer Protection

1. The Parties recognise the importance of transparent and effective measures that enhance consumer trust in digital trade.

2. To this end, each Party shall adopt or maintain measures that protect consumers engaged[11] in online commercial activities, including laws and regulations that proscribe misleading, deceptive, fraudulent, and unfair commercial practices that cause harm or potential harm to consumers.

3. While recognising that the form of protection may be different as between online and other forms of commerce, each Party shall provide consumers engaged in online commercial activities with a level of protection that is, in its effect, not less than that provided under its law to consumers engaged in other forms of commerce.

4. The Parties recognise the importance of online consumer protection and, as appropriate, shall promote cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to online consumer protection. To this end, the Parties affirm that cooperation under Chapter 19 (Consumer Protection) of Title V (Economic and Sector Cooperation) includes cooperation with respect to online consumer protection.

5. The Parties further recognise the importance of improving awareness of and providing access to consumer redress mechanisms to protect consumers engaged in online commercial activities, including for consumers of a Party transacting with suppliers of the other Party.

6. The Parties shall endeavour to explore the benefits of mechanisms, including alternative dispute resolution, to facilitate the resolution of claims concerning online commercial activities.

ARTICLE 132-S

Unsolicited Commercial Electronic Messages

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

[11] For the purposes of this Article, the term 'engaged' includes the pre-transaction phase of online commercial activities.

(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or

(b) require the consent, as specified in the laws and regulations of that Party, of recipients to receive commercial electronic messages.

2. Each Party shall ensure that unsolicited commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and contain the necessary information to enable end-users to request cessation free of charge and at any time.

3. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained in accordance with paragraphs 1 and 2.

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

ARTICLE 132-T

Digital Inclusion

1. The Parties recognise the importance of digital inclusion, that all people and businesses can participate in, contribute to, and benefit from the digital economy. To this end, the Parties recognise the importance of expanding and facilitating opportunities in the digital economy by removing barriers to participation in the digital economy, and that this may require tailored approaches, developed in consultation with businesses, individuals and other groups that disproportionately face such barriers. The Parties also recognise the importance of adopting or maintaining labour policies that promote decent conditions of work for workers who are engaged in or support the digital economy, in accordance with each Party's laws and regulations.

2. The Parties shall cooperate on matters relating to digital inclusion, including the participation of women and other groups and individuals that may disproportionately face barriers to digital trade. Such cooperation may include:

(a) sharing experiences and best practices, including the exchange of experts, with respect to digital inclusion;

(b) identifying and addressing barriers in accessing digital trade opportunities;

(c) sharing methods and procedures for developing datasets and conducting analysis in relation to the participation in digital trade by women and other groups that may disproportionately face barriers to participation in the digital economy;

(d) improving digital skills and access to online business tools;

(e) promoting labour protection for workers who are engaged in or support digital trade; and

(f) other areas as jointly agreed by the Parties.

3. Cooperation activities relating to digital inclusion may be carried out through the coordination, as appropriate, of the Parties' respective agencies and stakeholders.

4. The Parties also recognise the digital divide between countries, and the role for digital trade in promoting economic development and poverty reduction. To that end, the Parties shall endeavour to undertake and strengthen cooperation, including through existing mechanisms, to promote the participation in digital trade of countries who face barriers to such participation. This may include sharing best practices, collaborating on capacity building initiatives, active engagement in international fora and promoting countries' participation in, and contribution to, the global development of rules on digital trade.

5. The Parties shall also participate actively at the WTO and in other international fora to promote initiatives for advancing digital inclusion in digital trade.

ARTICLE 132-U

Small and Medium Sized Enterprises

1. The Parties recognise the fundamental role played by SMEs in economic growth and job creation, and the need to address the barriers to participation in the digital economy for such entities. To this end, the Parties shall, subject to their available resources, seek opportunities to:

(a) promote close cooperation on digital trade between SMEs of the Parties and cooperate in promoting jobs and growth for SMEs;

(b) encourage SMEs' participation in platforms that help link SMEs with international suppliers, buyers and other potential business partners; and

(c) exchange information and share best practices in improving digital skills and leveraging digital tools and technology to improve access to capital and credit, participation in government procurement opportunities, and other areas that could help SMEs adapt to digital trade.

2. The Parties recognise the integral role played by the private sector in the Parties' implementation of this Article.

ARTICLE 132-V

Emerging Technology

1. The Parties recognise that emerging technologies play important roles in promoting economic competitiveness and facilitating international trade and investment flows, and that coordinated action across multiple trade policy areas helps to maximise the economic and social benefits of those technologies.

2. The Parties shall endeavour to develop governance and policy frameworks for the trusted, safe, and responsible use of emerging technologies. In developing those frameworks, the Parties recognise the importance of:

(a) taking into account the principles and guidelines of relevant international bodies;

(b) utilising risk-based approaches to regulation that are based on industry-led standards and risk management best practices; and

(c) having regard to the principles of technological interoperability and technological neutrality.

3. The Parties shall endeavour to cooperate on matters related to emerging technologies with respect to digital trade. This cooperation may include:

(a) exchanging information and sharing experiences and best practices on laws, regulations, policies, enforcement and compliance;

(b) cooperating on issues and developments relating to emerging technologies, such as ethical use, human diversity and unintended biases, industry-led technical standards and algorithmic transparency;

(c) promoting collaboration between each Party's governmental and non-governmental entities in relation to research and development opportunities and opportunities for investment in emerging technologies;

(d) playing an active role, including through international fora, in the development of international standards, regulations and conformity assessment procedures that provide clear expectations for businesses and support the growth of emerging technologies; and

(e) participating actively in international fora on matters concerning the interaction between trade and emerging technologies.

ARTICLE 132-W

Digital Identities

1. Recognising that cooperation between the Parties on digital identities will increase regional and global connectivity, and recognising that each Party may take different legal and technical approaches to digital identities, the Parties shall pursue the development of mechanisms to promote compatibility and interoperability between their respective digital identity regimes.

2. To this end, the Parties shall endeavour to facilitate initiatives to promote such compatibility and interoperability, which may include:

(a) developing appropriate frameworks and common standards to foster technical interoperability between each Party's implementation of digital identities;

(b) developing comparable protection of digital identities under each Party's respective legal frameworks, or the recognition of their legal effects, whether accorded autonomously or by agreement;

(c) supporting the development of international frameworks on digital identity regimes;

(d) identifying and implementing use cases for the mutual recognition of digital identities; and

(e) exchanging knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation and security standards, and the promotion of the use of digital identities.

ARTICLE 132-X

Cooperation on Competition Policy

1. Recognising that the Parties can benefit by sharing their experiences in enforcing competition law and in developing and implementing competition

policies to address the challenges that arise from the digital economy, the Parties shall consider undertaking agreed technical cooperation activities, including:

(a) exchanging information and experiences on the development of competition policies for digital markets;

(b) sharing best practices on the enforcement of competition law and the promotion of competition in digital markets;

(c) providing advice or training, including through the exchange of officials, to assist a Party to build necessary capacities to strengthen competition policy development and competition law enforcement in digital markets; and

(d) any other form of technical cooperation agreed by the Parties.

2. The Parties shall endeavour to cooperate, where practicable, on issues of competition law enforcement in digital markets between their respective authorities, including through notification, consultation and the exchange of information.

3. Any cooperation under paragraphs 1 and 2 shall be in a manner compatible with each Party's domestic law and important interests, and within their available resources.

ARTICLE 132-Y

Stakeholder Engagement

1. The Parties shall seek opportunities to convene a Digital Economy Dialogue (the "Dialogue") at times agreeable to the Parties, to promote the benefits of the digital economy. The Parties shall promote relevant collaboration efforts and initiatives between the Parties through the Dialogue.

2. Where appropriate, and as may be agreed by the Parties, the Dialogue may include participation from other interested stakeholders, such as researchers, academics, and industry. The Parties may collaborate with such stakeholders in convening the Dialogue.

3. To encourage inclusive participation by the Parties' stakeholders and increase the impact of outreach, the Parties may consider organising the Dialogue in connection with, or as a part of, existing bilateral initiatives.

4. The Parties may consider relevant technical or scientific input, or other information arising from the Dialogue, for the purposes of implementation

efforts and further modernisation of this Section and other relevant articles in this Agreement.

ARTICLE 132-Z

Open Internet Access

Subject to its applicable policies, laws and regulations, each Party shall endeavour to adopt or maintain appropriate measures to ensure that end-users in its territory may:

(a) access, distribute, and use services and applications of their choice available on the Internet, subject to reasonable, transparent, and non-discriminatory network management;

(b) connect devices of their choice to the Internet, provided that these devices do not harm the network; and

(c) access information on the network management practices of their Internet access service supplier.

ARTICLE 132-AA

Cooperation

1. The Parties recognise the fast-paced and evolving nature of digital trade, and the role of cooperation between the Parties in increasing and enhancing opportunities for businesses, consumers, and society at large.

2. In addition to areas of cooperation between the Parties identified in other parts of this Section, the Parties shall exchange information on, and share experiences and best practices on laws, regulations, policies, enforcement, and compliance relating to digital trade.

3. The Parties shall, where appropriate, cooperate and actively participate in international fora, including the WTO, to promote the development and adoption of international frameworks for digital trade.

4. The Parties shall encourage the development, by the private sector, of methods of self-regulation that foster digital trade, including codes of conduct, model contracts, guidelines and compliance mechanisms.

5. The Parties shall endeavour to:

(a) work together to address challenges for SMEs in the use of digital trade;

(b) promote and facilitate collaboration between government entities, enterprises, and other non-governmental entities on digital technologies, including digital innovation and emerging technologies, relating to trade, investment, and research and development opportunities; and

(c) facilitate gender equality and equal opportunities for women and men in digital trade, acknowledging the objectives established in Chapter 20 (Cooperation on Employment, Social Policy and Equal Opportunities) of Title V (Economic and Sector Cooperation).

ANNEX B

The UK-Ukraine Agreement shall be amended as follows:

Amendments to Title IV (Trade and Trade Related Matters), Chapter 6 (Establishment, Trade in Services and Electronic Commerce), Section 1 (General Provisions):

1. The title of Article 81 (Objective, Scope and Coverage) shall be substituted with "Objective, Scope and Coverage of Sections 1 to 5".

2. In paragraph 1 of Article 81, the words "and for cooperation on electronic commerce" shall be omitted.

3. In paragraph 2 of Article 81, the words "Sections 1 to 5 of" shall be inserted after the words "nothing in".

4. In paragraph 3 of Article 81, the words "Sections 1 to 5 of" shall be inserted after the words "the provisions of".

5. In paragraph 4 of Article 81, the words "Sections 1 to 5 of" shall be inserted after the words "compatible with".

6. In paragraph 5 of Article 81, the words "This Chapter" shall be substituted with "Sections 1 to 5 of this Chapter".

7. In the unnumbered paragraph following paragraph 5 of Article 81, the words "Sections 1 to 5 of" shall be inserted after both instances of the words "this Chapter".

Amendments to Title IV (Trade and Trade Related Matters), Chapter 6 (Establishment, Trade in Services and Electronic Commerce), Section 5 (Regulatory Framework), Sub-Section 6 (Financial Services):

8. Article 119 (Scope and Definitions) shall be replaced by the following:

"ARTICLE 119
Scope and Definitions

1. This Sub-Section sets out the principles of the regulatory framework for all financial services liberalised pursuant to Sections 2, 3 and 4 of this Chapter.

2. For the purposes of this Sub-section and of Sections 2, 3 and 4 of this Chapter:

(a) "financial service" means any service of a financial nature offered by a financial service supplier of a Party. Financial services include the following activities:

(i) insurance and insurance-related services:

1. direct insurance (including co-insurance):

(a) life;

(b) non-life;

2. reinsurance and retrocession;

3. insurance intermediation, such as brokerage and agency; and

4. services auxiliary to insurance, such as consultancy, actuarial, risk assessment and claim settlement services;

(ii) banking and other financial services (excluding insurance):

1. acceptance of deposits and other repayable funds from the public;

2. lending of all types, including consumer credit, mortgage credit, factoring and financing of commercial transactions;

3. financial leasing;

4. all payment and money transmission services, including credit, charge and debit cards, travellers' cheques and bankers' drafts;

5. guarantees and commitments;

6. trading for own account or for account of customers, whether on an exchange, in an over-the-counter market or otherwise, the following:

(a) money market instruments (including cheques, bills, certificates of deposit);

(b) foreign exchange;

(c) derivative products including, but not limited to, futures and options;

(d) exchange rate and interest rate instruments, including products such as swaps and forward rate agreements;

(e) transferable securities; and

(f) other negotiable instruments and financial assets, including bullion;

7. participation in issues of all kinds of securities, including underwriting and placement as agent (whether publicly or privately) and provision of services related to such issues;

8. money broking;

9. asset management, such as cash or portfolio management, all forms of collective investment management, pension fund management, custodial, depository and trust services;

10. settlement and clearing services for financial assets, including securities, derivative products, and other negotiable instruments;

11. provision and transfer of financial information, and financial data processing and related software;

12. advisory, intermediation and other auxiliary financial services concerning all the activities listed in subparagraphs (1) to (11), including credit reference and analysis, investment and portfolio research and advice, advice on acquisitions and on corporate restructuring and strategy;

(b) "financial service computing facility" means a computer server or storage device for the processing or storage of information relevant for the conduct of the ordinary business of a financial service supplier;

(c) "financial service supplier" means any natural or legal person of a Party that seeks to provide or provides financial services. The term "financial service supplier" does not include a public entity;

(d) "public entity" means:

(i) a government, central bank or a monetary authority, of a Party, or an entity owned or controlled by a Party, which is principally engaged in carrying out governmental functions or activities for governmental purposes, not including an entity principally engaged in supplying financial services on commercial terms; or

(ii) a private entity, performing functions normally performed by a central bank or monetary authority, when exercising those functions; and

(e) "new financial service" means a service of a financial nature, including services related to existing and new products or the manner in which a product is delivered, which is not supplied by any financial service supplier in the territory of a Party but which is supplied in the territory of the other Party."

9. Article 122 (New Financial Services) shall be replaced by the following:

"ARTICLE 122
New Financial Services[12]

1. Each Party shall permit a financial service supplier of the other Party established in the territory of that Party to provide any new financial service of a type similar to those services that the Party would permit its own financial service suppliers to provide under its domestic law in like circumstances. A Party may determine the juridical form through which the service may be provided and may require authorisation for the provision of the service. Where such authorisation is required, a decision shall be made within a reasonable time and the authorisation may only be refused for prudential reasons.

2. To support innovation in financial services, the Parties shall endeavour to collaborate, share knowledge, experiences and developments in financial services, to advance financial integrity,

[12] Nothing in this Article shall be construed as preventing a financial service supplier of a Party from applying to the other Party to request that it authorises the supply of a financial service that is not supplied in the territory of either Party. That application shall be subject to the domestic law of the Party to which the application is made and, for greater certainty, shall not be subject to this Article.

consumer wellbeing and protection, financial inclusion, competition, financial stability and facilitate cross-border development of new financial services."

10. Article 123 (Data Processing) shall be replaced by the following:

"ARTICLE 123
Financial Information

1. Neither Party shall restrict a financial service supplier of the other Party from transferring information, including transfers of data by electronic means, where such transfers are for the conduct of the ordinary business of the financial service supplier.

2. Subject to paragraph 3, neither Party shall require a financial service supplier of the other Party to use or locate financial services computing facilities in the Party's territory as a condition for conducting business in the Party's territory.[13]

3. Each Party has the right to require a financial service supplier of the other Party to use or locate financial services computing facilities its territory, where it is not able to ensure access to information required for the purposes of financial regulation and supervision, provided that to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information.

4. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights and the freedom of individuals, in particular with regard to the transfer of personal data. Nothing in this Article shall restrict the right of a Party to adopt or maintain measures to protect personal data, personal privacy, and the confidentiality of individual records and accounts, provided that such measures are not used to circumvent the provisions of this Agreement."

[13] For greater certainty, this prohibition also applies to circumstances in which a financial service supplier of the other Party uses the services of an external business for such use, storage or processing of information.

E02894410

978-1-5286-4042-8