Council of the
European Union

Brussels, 29 April 2022
(OR. en)

8314/22

LIMITE

DATAPROTECT 107
JAI 504
MAMA 57
AGRI 159
ACP 41
COLAC 17
COEST 325

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	7188/22
Subject:	International personal data flows and trade agreements - Report of the presidency

Delegations will find in the Annex a Presidency Report on the international personal data flows in trade agreements and international political statements.

ANNEX

International personal data flows in trade agreements and international political statements

Presidency Report

I. Introduction and context

The flow of personal data and the removal of protectionist barriers in the context of international trade is a major strategic economic issue for companies. Beyond trade activities, data flows in the world have become an essential strategic issue in a few years.

However, the facilitation of data flows, in particular for commercial purposes, must take into account the principles of the European framework and the need to ensure and promote a high level of protection of personal data.

As enshrined in Articles 7 and 8 of the European Union Charter of Fundamental Rights, respect for privacy and protection of personal data are part of the common foundations of the EU.

International trade agreements and declarations should therefore not limit the EU's autonomy as to the chosen level of protection of privacy and personal data, and personal data flows with third countries should be based on the transfer instruments provided for in Chapter V of the General Data Protection Regulation (GDPR) (e.g. adequacy decision, standard contractual clauses, binding corporate rules).

Negotiated in many and varied fora (e.g. G7, G20, WTO), international declarations and trade agreements may contain heterogeneous data protection provisions.

The French Presidency considered it useful to examine these stipulations within the Council in the Working Party “Data Protection” in order to better assess their relationship with the European legal framework on data protection.

The existence of data protection clauses or provisions in international trade agreements and declarations of political nature is of particular importance to ensure an effective link between these agreements and declarations and international flows of personal data. This report outlines the work of the working party on the subject and presents its main conclusions. It proposes the principle of informing the working party on the negotiations on data flows initiated or underway, and suggests various ways of implementing this information.

II. Work within the working party

On 2 February 2022, the Presidency presented the mapping it had drawn up to the Data Protection Working Party. This mapping listed the trade agreements negotiated in the European and WTO frameworks, as well as the initiatives developed in the framework of the G20 and G7. This document also mentioned the agreements concluded by certain third countries.

The aim of this mapping was to enable Member States to be aware of the provisions contained in these agreements negotiated in different fora, in relation to the protection of personal data and international data transfers.

The Presidency also submitted questions to the Member States on the content and architecture of this mapping, as well as on the governance and monitoring arrangements for trade agreements. Several Member States replied orally at the meetings of the Data Protection Working Party and seven Member States provided written comments.

The synthesis of these contributions and the restructured mapping were presented and discussed at the group meeting on 23 March 2022 (WK3393/22 and ST7188/22).

The new classification of trade agreements and international declarations negotiated in the European framework according to the nature of the clauses they contained (declaratory clauses, technical clauses and horizontal clauses based on the approach proposed by the Commission in 2018) was welcomed.

The Member States also considered that the establishment of this mapping was very useful.

III. Main conclusions concerning the modalities of information of the Data Protection Working Party on the negotiations on data flows

The Presidency's work indicates that:

With regard to trade negotiations, the forum for discussion within the Council remains the Trade Policy Committee of the Council of the EU, in accordance with Article 207§3 of the Treaty on the Functioning of the European Union. This article provides that trade negotiations shall be conducted by the European Commission in consultation with a special committee appointed by the Council to assist it in this task and within the framework of such directives as the Council may issue to it. There is no question of establishing parallel discussions in another preparatory body of the Council.

Likewise, the coordination at national level on this subject should be preserved. The work or discussions that take place at national level on trade negotiations should not be duplicated or exported to the European level.

However, the protection of personal data is a crosscutting subject that affects a number of sectors. An appropriate dissemination of information between the respective competent working parties seems useful and can ensure overall consistency. Furthermore, providing for the information of other Council preparatory bodies complies with the institutional rules of the Treaty on the Functioning of the European Union.

In this respect, several options on how to disseminate this information seem possible and have been defended by some Member States:

– Provide for the Data Protection Working Party to be informed only when a particular data protection issue arises in the context of a trade negotiation, or when the Council Presidency considers it necessary to draw the attention of the Member States to a trade negotiation ;

– Provide for the Data Protection Working Party to be regularly informed of the progress of trade negotiations, particularly when they begin. This information could be provided by various means: in writing, by videoconference meetings with the Commission or by the presence of one of its representatives at the meetings of the Data Protection Working Party;

– Provide for joint meetings of the Data Protection Working Party and the Trade Policy Committee to allow for the participation of experts from both subject areas in the event that complex issues relating to the protection of personal data arise during trade negotiations.

During the discussions, one delegation considered that there was no need to inform the Data Protection Working Party. Several Member States were in favour of better information for the Data Protection Working Party, without necessarily proposing any particular modalities.

It appears from these exchanges that there are different ways of providing information. The choice between them should be left to the discretion of each Presidency, depending on the current state of trade negotiations and discussions in other international fora, while respecting the prerogatives of the Trade Policy Committee and taking care to avoid to duplicate the channels of coordination and dissemination of information when they already exist elsewhere.

With regard to the scope of the information provided by the Data Protection Working Party, it should be pointed out that the Commission seems to have a specific role to play when it comes to information on political declarations, since by definition these negotiations are not followed by all EU Member States.

IV. Conclusions

The Presidency hopes that this report will contribute to the work of the Data Protection Working Party on international flows of personal data and will enable each successive Presidency to make a choice among the above-mentioned methods of disseminating information, which it deems most appropriate.

The Presidency intends to circulate this document as well as the mapping of trade agreements negotiated within the European framework, the WTO and the initiatives developed within the framework of the G20 and the G7 to the Council and the Commission so that they can use it later.

ANNEX

Mapping of trade agreements, and G20, G7 and World Trade Organisation initiatives

I- MAPPING OF BILATERAL AND MULTILATERAL TRADE AGREEMENTS EU-THIRD COUNTRIES

1- Summary of trade agreements between the European Union and third countries
2- Quotation of relevant data protection provisions

1- Summary of trade agreements between the European Union and third countries

EU bilateral (B) and multilateral (M) trade agreements classified according to the nature of the clauses they contain	
Agreement with declaratory clauses	
Southern African Development Community[1]: Signed on 10 June 2016 and entered into force on 10 October 2016 (M). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:250:TOC	Article 10 - Information exchange and confidentiality Personal data may be exchanged only where the Contracting Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Contracting Party that may supply them. To that end, Contracting Parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community.
Lebanon: Signed on 17 June 2002; entered into force on 1 March 2003 (B) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2006:143:TOC	Article 53.2 g) Proclamation of cooperation on the protection of personal data and privacy.
Algeria: Signed on 22 April 2002 and entered into force on 1 September 2005 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02005A1010%2801%29-20170201	Article 45: The Parties undertake to adopt appropriate measures to ensure the protection of personal data in order to eliminate barriers to the free movement of such data between the Parties.
Egypt: Signed on 25 April 2001 and entered into force on 1 June 2004 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1398411944881&uri=CELEX:22004A0930(03)	Joint declaration on the protection of data: The Parties agree that the protection of data will be guaranteed in all areas where the exchange of personal data is envisaged.
Jordan: Signed on 24 November 1997; entered into force on 1 May 2002 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2002:129:TOC	Joint declaration on the protection of data: The Parties agree that the protection of data will be guaranteed in all areas where the exchange of personal data is envisaged.
Palestine: Signed on 24 February 1997; entered into force on 1 July 1997 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399391758208&uri=CELEX:21997A0716(01)	Joint declaration on the protection of data: The Parties agree that the protection of data will be guaranteed in all areas where the exchange of personal data is envisaged.
Agreements with clauses providing for a personal data protection regime	

[1] South Africa, Botswana, Eswatini, Lesotho, Mozambique, Namibia.

- Harmonisation of the legislation with other existing privacy legislation at the European and international level
- Establishment of a supervisory institution/authority in charge of data protection
- Definition of personal data
- Establishment of principles governing the processing of personal data (e.g. lawfulness, fairness, transparency)
- Provision to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, including relevant instruments of the Council of Europe (Convention n° 108 of 28 January 1981)
- Regarding administrative assistance/cooperation in tax and/or customs matters, existence of specific provisions on information exchange and confidentiality (specific protocol or annex to the agreement):
    - Personal data can only be exchanged if the receiving party undertakes to protect them in a way at least equivalent to that applicable in the contracting party that may provide them;
    - The parties shall inform each other of the rules applicable on their territory, including, where appropriate, the legal rules in force in the Community's Member States;
    - The Parties shall at least ensure a level of protection based on the principles of the Council of Europe's Convention n°108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.

Agreements	Specific provisions /observations
Serbia: Signed on 1 February 2010 and entered into force on 1 September 2013 (consolidated version as of 1 February 2015) (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02013A1018%2801%29-20150201	
Cameroon: Signed on 15 January 2009 and entered into force on 4 August 2014 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02009A0228%2801%29-20190218	
Bosnia and Herzegovina: Signed on 16 June 2008 and entered into force on 1 July 2008 (goods) and 1 June 2015 (services) (B) http://europa.ba/wp-content/uploads/2015/05/delegacijaEU_201112140506368 6eng.pdf	
Montenegro: Signed on 15 October 2007 and entered into force on 1 January 2008 (goods) and 1 May 2010 (services) (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1474016437229&uri=CELEX:02010A0429(01)-20150201	

Albania: Signed on 1 December 2006 and entered into force on 1 April 2009 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2009.107.01.0165.01.ENG&toc=OJ%3AL%3A2009%3A107%3ATOC#L_2009107EN.01016601	
Faroe Islands: Signed on 6 December 1996 and entered into force on 1 January 1997 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1398412647857&uri=CELEX:21997A0222(01)	Article 10 – Information exchange and confidentiality 2. Personal data may be exchanged only where the receiving Contracting Party undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the supplying Contracting Party Has an adequacy decision issued before the GDPR: Decision 2010/146 of 5 March 2010 (updated version as of 17 December 2016) https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32010D0146
Morocco: Signed on 26 February 1996 and entered into force on 1 March 2000 (consolidated version as of 19 July 2019) (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399391205944&uri=CELEX:22000A0318(01)	
Tunisia: Signed on 7 July 1995 and entered into force on 1 March 1998 (B) (consolidated version as of 1 July 2013) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399544134573&uri=CELEX:21998A0330(01)	
Israel: Signed on 20 November 1995; entered into force on 1 June 2000 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22000A0621%2801%29&qid=1612177181225	Article 10 - Obligation to observe confidentiality 2. Personal data may only be transmitted if the level of personal protection afforded by the legislations of the Parties is equivalent. The Parties shall ensure at least a level of protection based on the principles of Council of Europe Convention No 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Has an adequacy decision issued before the GDPR: Decision 2011/61 of 31 January 2011 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061
Andorra: Signed on 28 June 1991 and entered into force on 1 July 1991 (consolidated version of 1 January 2016) (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1398350679054&uri=CELEX:21990A1231(02)	Has an adequacy decision issued before the GDPR: Decision 2010/625 of 19 October 2010 (updated version as of 17 December 2016) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0625

Norway: Signed on 14 May 1973 and entered into force on 1 July 1973 (consolidated version as of 1 May 2015) (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399391371763&uri=CELEX:21973A0514(01)	The GDPR applies in Norway since 20 July 2018 in accordance with the Joint Committee Decision integrating the General Data Protection Regulation (GDPR) (EU) 2016/679 into the EEA Agreement, which was adopted by the EEA Joint Committee on 6 July 2018. Part of the European Economic Area and member of the Free Trade Association
Iceland: Signed on 19 December 1972 and entered into force on 1 April 1973 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399389051991&uri=CELEX:21972A0722(05)	The GDPR applies in Iceland since 20 July 2018 in accordance with the Joint Committee Decision integrating the General Data Protection Regulation (GDPR) (EU) 2016/679 into the EEA Agreement, which was adopted by the EEA Joint Committee on 6 July 2018. Part of the European Economic Area and member of the Free Trade Association
Switzerland – Liechtenstein: Signed on 22 July 1972; entered into force on 1 January 1973 (consolidated version as of 1 February 2015) (M) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399542828541&uri=CELEX:21972A0722(03)	Implementation of the GDPR. Part of the European Economic Area and member of the Free Trade Association Has an adequacy decision issued before the GDPR: decision 2000/518 of 26 July 2000: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518

Agreements containing the EU horizontal clauses on cross-border data flows (Clause A) and protection of personal data and privacy (Clause B) proposed in 2018[2]

- Clause A ""Cross-border data flows"": prohibition of the following unjustified restrictions
  - Obligation to use computer facilities in the territory of a party, including by imposing certification requirements for such facilities ;
  - Forced localisation of data in the territory of a party;
  - Prohibition of storage and processing of data in the territory of the other party;
  - Restrictions making cross-border transfers conditional on the use of computer facilities in the territory of the party;
  - Clause on review of the list of prohibited restrictions and requirement to evaluate its operation after three years;
- Clause B "Protection of personal data and privacy" including the following elements
  - Explicit recognition that high standards and rules for privacy and protection of personal data are fundamental for the parties;
  - Opportunity for the parties to adopt and maintain safeguards for privacy and protection of personal data, including for transfers of personal data;
  - Non-circumvention clause of the EU acquis: provision stating that the agreement does not affect the protection of personal data and privacy as guaranteed by the laws of the parties;

Agreements	**Specific provisions /observations**

[2] **The bilateral agreements with the United Kingdom and Chile contain the structure and content of the horizontal clauses proposed in 2018 fully**
The other bilateral agreements include clauses on personal data flows and privacy exceptions

United Kingdom: Signed on 30 December 2020 and entered into force on 1 January 2021 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22021A0430%2801%29&qid=1625583778831	CHAPTER 2 - DATA FLOWS AND PERSONAL DATA PROTECTION Article 201 - Cross-border data flows 1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by a Party: (a)requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party; (b) requiring the localisation of data in the Party's territory for storage or processing; (c)prohibiting the storage or processing in the territory of the other Party; or (d)making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory 2. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the date of entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in paragraph 1. Such a request shall be accorded sympathetic consideration. Article 202 - Protection of personal data and privacy 1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standard in this regard contribute to trust in the digital economy and to the development of trade. 2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application (34) for the protection of the data transferred. 3. Each Party shall inform the other Party about any measure referred to in paragraph 2 that it adopts or maintains. Has an adequacy decision issued after the GDPR: Decision of 28 June 2021. https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of

	personal data by the united kingdom - general data protection regulation en.pdf
Vietnam: Signed on 30 June 2019; entered into force on 1 August 2020 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2020:186:TOC	Article 8.45 – Data Processing 1. Each Party shall adopt or maintain appropriate safeguards to protect personal data and privacy, including individual records and accounts […] 3. Nothing in this Article restricts the right of a Party to protect personal data and privacy, so long as such right is not used to circumvent this Agreement. Article 8.53 – General Exceptions Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination against the other Party where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by a Party of measures: [..] e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Singapore: Signed on 19 October 2018; entered into force on 21 November 2019 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2019:294:TOC	ARTICLE 8.54 - Data Processing 1. Each Party shall, subject to appropriate safeguards on privacy and confidentiality, permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing, where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt or maintain appropriate safeguards to protect privacy and personal data, including individual records and accounts, as long as these safeguards are not used to circumvent the provisions of this Agreement. ARTICLE 8.62 – General Exceptions Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination against the other Party where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or

	enforcement by a Party of measures: [..] e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Japan: Signed on 17 July 2018; entered into force on 1er February 2019 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2018:330:TOC	ARTICLE 8.63 – General Exceptions 1. A Party shall not take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, if those transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. 2. Nothing in paragraph 1 restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as that right is not used to circumvent Sections B to D and this Sub-Section. ARTICLE 18.1 – Objectives and general principles 2. Nothing in this Section shall affect the right of a Party to define or regulate its own level of protection in pursuit or furtherance of its public policy objectives in areas such as: h) personal data and cybersecurity; Has an adequacy decision issued after the GDPR: Decision 2019/419 of 23 January 2019 : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC
Armenia: Signed on 24 November 2017 and entered into force on 1 June 2018 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22018A0126(01)	Article 13 - Protection of personal data The Parties agree to cooperate in order to ensure a high level of protection of personal data in accordance with the international legal instruments and standards of the European Union, Council of Europe and other international bodies. Article 185 - Data processing 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial

	service supplier. 2. Nothing in paragraph 1 restricts the right of a Party to protect personal data and privacy, so long as such right is not used to circumvent this Agreement. 3. Each Party shall adopt or maintain adequate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data. Article 200 - General exceptions 2. Subject to the requirement that such measures not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed as preventing the adoption or enforcement by a Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with this Chapter including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Canada: Signed on 30 October 2016; entered into force on 21 September 2017 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2017:011:TOC	Article 28.3 - General exceptions 2. For the purposes of Chapters Nine (Cross-Border Trade in Services), Ten (Temporary Entry and Stay of Natural Persons for Business Purposes), Twelve (Domestic Regulation), Thirteen (Financial Services), Fourteen (International Maritime Transport Services), Fifteen (Telecommunications), Sixteen (Electronic Commerce), and Sections B (Establishment of investments) and C (Non-discriminatory treatment) of Chapter Eight (Investment), subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by a Party of measures necessary: c) to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;

	Has an adequacy decision issued before the GDPR: Decision 2002/02 of 20 December 2001.https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002
Ghana: Signed on 28 July 2016 and entered into force on 15 December 2016 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.287.01.0003.01.ENG&toc=OJ:L:2016:287:TOC	Article 68 -General exception clause Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in goods, services or establishment, nothing in this Agreement shall be construed to prevent the adoption or enforcement by the Parties of measures which: c) are necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Republic of Moldova: Signed on 27 June 2014 and entered into force on 1 September 2014 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2014:260:TOC	Article 13 - Protection of personal data 1. The Parties agree to cooperate in order to ensure a high level of protection of personal data in accordance with EU, Council of Europe and international legal instruments and standards. 2. Any processing of personal data shall be subject to the legal provisions referred to in Annex I to this Agreement. The transfer of personal data between the Parties shall only take place if such transfer is necessary for the implementation, by the competent authorities of the Parties, of this or other agreements concluded between the Parties. Article 261 - General exceptions 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by any Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to : (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.
Ukraine: Signed on 27 June 2014, entered into force on 23 April 2014 (B)	Article 15 – Protection of personal data

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2014:161:TOC	The Parties agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, including the relevant Council of Europe instruments. Cooperation on personal data protection may include, inter alia, the exchange of information and of experts. Section 7 - Exceptions Article 141 – General exceptions 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed in such a way as to prevent the adoption or enforcement by any Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Georgia: Signed on 27 June 2014 and entered into force on 1 September 2014 (B) https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2014:261:FULL&from=EN	Article 14 - Protection of personal data The Parties agree to cooperate in order to ensure a high level of protection of personal data in accordance with the EU, Council of Europe and international legal instruments and standards referred to in Annex I to this Agreement. Article 134 – General exceptions 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by any Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.
Costa Rica; El Salvador; Guatemala; Honduras; Nicaragua; Panama: Signed on 29 June 2012; entered into force on 1 August 2013 (M) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2012:346:TOC	Article 34 – Personal Data Protection 1. The Parties agree to cooperate in order to improve the level of protection of personal data to the highest international standards, such as the Guidelines for the Regulation of

	Computerised Personal Data Files, modified by the General Assembly of the United Nations on December 14th 1990, and to work towards the free movement of personal data between the Parties, with due regard to their domestic legislation. 2. Cooperation on protection of personal data may include, inter alia, technical assistance in the form of exchange of information and expertise taking into account the laws and regulations of the Parties Article 203 – General exceptions 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Title shall be construed to prevent the adoption or enforcement by any Party of measures which are: e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Colombia and Peru: Signed on 26 June 2012; entered into force on 1 March 2013 (M) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399559825164&uri=CELEX:22012A1221(01)	Article 157 Data Processing 1. Each Party shall permit a financial service supplier of another Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of the right to privacy and the freedom from interference with the privacy, family, home or correspondence of individuals, in particular with regard to the transfer of personal data. Article 164 - Protection of Personal Data The Parties shall endeavour, insofar as possible, and within their respective competences, to develop or maintain, as the case may be, regulations for the protection of personal data. Article 167 - General Exceptions

	1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties, or a disguised restriction on establishment or cross-border supply of services, nothing in this Title and Title V (Current Payments and Capital Movements) shall be construed to prevent the adoption or enforcement by any Party of measures: e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title and Title V (Current Payments and Capital Movements) including those relating to: […] ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Republic of Korea: Signed on 6 October 2010; entered into force on 1 July 2011 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399390040762&uri=CELEX:22011A0514(01)	Article 7.43 -Data processing No later than two years after the entry into force of this Agreement, and in no case later than the effective date of similar commitments stemming from other economic integration agreements: (a) each Party shall permit a financial service supplier of the other Party established in its territory to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier; and (b) each Party, reaffirming its commitment (41) to protect fundamental rights and freedom of individuals, shall adopt adequate safeguards to the protection of privacy, in particular with regard to the transfer of personal data Article 7.50 - Exceptions Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by either Party of measures: [...] (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;

	Has an adequacy decision issued after the GDPR: Decision of 17 December 2021.https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf
States of Southern and Eastern Africa[3]: Signed on 29 August 2009 and entered into force on 14 May 2012 (M) https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2012.111.01.0001.01.FRA	Article 56 -General exception clause Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on international trade, nothing in this Agreement shall be construed to prevent the adoption or enforcement by the EC Party, the ESA States or a Signatory ESA State of measures which: c) are necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement, including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Papua New Guinea, Fiji, Samoa, Solomon Islands: Signed on 30 July 20019 and entered into force on 20 December 2009 (M) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399391908038&uri=CELEX:22009A1016(01)	Article 42 – General exception clause Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in goods, services or establishment, nothing in this Agreement shall be construed to prevent the adoption or enforcement by the EC Party or Pacific States of measures which: c) are necessary to secure compliance with laws or regulations not inconsistent with the provisions of this Agreement, including those relating to (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
CARIFORUM States: Signed on 15 October 2008; entered into force on 29 December 2008 (M) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1398342443880&uri=CELEX:22008A1030(01)	Chapter 6 : Protection of Personal Data Article 197 – General objective 1. The Parties and the Signatory CARIFORUM States, recognising: (a) their common interest in protecting fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, (b) the importance of maintaining effective data protection regimes as a means of

[3] Comoros, Madagascar, Mauritius Island, Seychelles, Zimbabwe.

	protecting the interests of consumers, stimulating investor confidence and of facilitating transborder flows of personal data; (c) that the collection and processing of personal data should be accomplished in a transparent and fair manner, with due respect accorded to the data subject, agree to establish appropriate legal and regulatory regimes, as well as appropriate administrative capacity to implement them, including independent supervisory authorities, in order to ensure an adequate level of protection of individuals with regard to the processing of personal data, in line with existing high international standards. Article 224 – General exception clause 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in goods, services or establishment, nothing in this Agreement shall be construed to prevent the adoption or enforcement by the EC Party, the CARIFORUM States or a Signatory CARIFORUM State of measures which: c) are necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: […] (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Ivory Coast: Signed on 26 November 2008 and entered into force on 3 September 2016 (B) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1398352060784&uri=CELEX:22009A0303(01)	Article 68 - General exception clause Subject to the requirement that such measures not be applicable in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in goods, services or establishment, this Agreement shall not be construed as preventing the adoption or enforcement by the Parties of measures which: […] c) are necessary to ensure compliance with laws and regulations and which are not incompatible with the provisions of this Agreement, including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Chile: Signed on 18 November 2002; entered into force on 1 February 2003 (goods) and le 1 March 2005 (services) (B) https://eur-lex.europa.eu/resource.html?uri=cellar:f83a503c-fa20-4b3a-9535-	Article 135 - Exceptions 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties

f1074175eaf0.0004.02/DOC_2&format=PDF	where like conditions prevail, or a disguised restriction on trade in services, financial services or establishment, nothing in this Title shall be construed to prevent the adoption or enforcement by either Party of measures : (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to : (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; Article 202 - Data Protection The Parties agree to accord a high level of protection to the processing of personal and other data, compatible with the highest international standards.
Mexico: Signed on 1 July 2000; entered into force on 1 October 2000 (B) https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2001:070:FULL&from=EN	Article 27 – Exceptions 2. Subject to the requirement that such measures are not arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Title shall be construed to prevent the adoption or enforcement by any Party of measures: c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;

The trade agreements signed with Northern Macedonia (signed on 1 June 2001 and entered into force on 1 April 2004), Turkey (signed on 6 March 1995 and entered into force on 1 January 1996), San Marino (signed on 16 December 1991 and entered into force on 1 April 2002) and Syria (signed on 18 January 1977 and entered into force on 1 July 1977) do not contain any specific provisions on personal data protection.

2- Citation des dispositions pertinentes en matière de protection de données à caractère personnel

Agreement	Relevant extracts on data protection
BILATERAL TRADE AGREEMENTS BETWEEN EUROPEAN UNION – THIRD EUROPEAN COUNTRIES	
Albania	Article 79 - Protection of personal data Albania shall harmonise its legislation concerning personal data protection with Community law and other European and international legislation on privacy upon the date of entry into force of this Agreement. Albania shall establish independent supervisory bodies with sufficient financial and human resources in order to efficiently monitor and guarantee the enforcement of national legislation on personal data protection. The Parties shall cooperate to achieve this goal. Protocol 6 on mutual administrative assistance in customs matters Article 10 Information exchange and confidentiality 1. Any information communicated in whatsoever form pursuant to this Protocol shall be of a confidential or restricted nature, depending on the rules applicable in each of the Parties. It shall be covered by the obligation of official secrecy and shall enjoy the protection extended to similar information under the relevant laws of the Party that received it and the corresponding provisions applying to the Community authorities. 2. Personal data may be exchanged only where the Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Party that may supply them. To that end, Parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community.
Andorra	Article 12h - Protection of professional secrecy and personal data The information exchanged by the Contracting Parties as part of the measures provided for in this Title shall enjoy the protection extended to professional secrecy and personal data as defined in the relevant laws applicable in the territory of the recipient Contracting Party. In particular, that information may not be transferred to persons other than the competent bodies in the Contracting Party concerned, nor may it be used by those bodies for purposes other than those provided for in this Agreement.
Armenia	Article 13 - Protection of personal data The Parties agree to cooperate in order to ensure a high level of protection of personal data in accordance with the international legal instruments and standards of the European Union, Council of Europe and other international bodies. Article 185 - Data processing 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for

	data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Nothing in paragraph 1 restricts the right of a Party to protect personal data and privacy, so long as such right is not used to circumvent this Agreement. 3. Each Party shall adopt or maintain adequate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data. Article 200 - General exceptions 2. Subject to the requirement that such measures not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed as preventing the adoption or enforcement by a Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with this Chapter including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Bosnia and Herzegovina	Article 79 - Protection of personal data Bosnia and Herzegovina shall harmonise its legislation concerning personal data protection with Community law and other European and international legislation on privacy upon the entry into force of this Agreement. Bosnia and Herzegovina shall establish independent supervisory bodies with sufficient financial and human resources in order to efficiently monitor and guarantee the enforcement of national personal data protection legislation. The Parties shall cooperate to achieve this goal. » Protocol 5 on mutual administrative assistance in customs matters Article 10 - Information exchange and confidentiality 2. Personal data may be exchanged only where the Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Party that may supply them. To that end, Parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community.
Georgia	Article 14 - Protection of personal data The Parties agree to cooperate in order to ensure a high level of protection of personal data in accordance with the EU, Council of Europe and international legal instruments and standards referred to in Annex I to this Agreement. Article 118 - Data processing 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data.

	Article 127 – Objective and principles 2. The Parties agree that the development of electronic commerce must be compatible with the international standards of data protection in order to ensure the confidence of users of electronic commerce. Article 134 – General exceptions 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by any Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.
Faroe Islands	Protocol 5 on mutual assistance between administrative authorities in customs matters Article 10 – Information exchange and confidentiality 2. Personal data may be exchanged only where the receiving Contracting Party undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the supplying Contracting Party.
Iceland	No specific provision
North Macedonia	Protocol 5 on mutual assistance between administrative authorities in customs matters Article 1-Definitions For the purposes of this Protocol: (d) 'personal data' shall mean all information relating to an identified or identifiable individual; Article 10 - Information exchange and confidentiality 1. Any information communicated in whatsoever form pursuant to this Protocol shall be of a confidential or restricted nature, depending on the rules applicable in each of the Contracting Parties. It shall be covered by the obligation of official secrecy and shall enjoy the protection extended to similar information under the relevant laws of the Contracting Party that received it and the corresponding provisions applying to the Community authorities. 2. Personal data may be exchanged only where the Contracting Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Contracting Party that may supply them. To that end, Contracting Parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community.
Montenegro	Article 81 – Protection of personal data Montenegro shall harmonise its legislation concerning personal data protection with Community law and other European and international legislation on privacy upon the entry into force of this Agreement. Montenegro shall establish one or more independent supervisory bodies with sufficient financial and

	human resources in order to efficiently monitor and guarantee the enforcement of national personal data protection legislation. The Parties shall cooperate to achieve this goal. Protocol 6 on mutual administrative assistance in customs matters Article 10 - Information exchange and confidentiality 2. Personal data may be exchanged only where the Contracting Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Contracting Party that may supply them. To that end, contracting parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community.
Norway	No specific provision
Republic of Moldova	Article 10- Information exchange and confidentiality 1. Any information communicated in whatsoever form pursuant to this Protocol shall be of a confidential or restricted nature, depending on the rules applicable in each of the Parties. It shall be covered by the obligation of official secrecy and shall enjoy the protection extended to similar information under the relevant laws of the Party that received it and the corresponding provisions applying to the institutions of the Union. 2. Personal data may be exchanged only where the Party which may receive it undertakes to protect such data in a manner that is considered adequate by the Party that may supply them. 4. The information obtained under this Protocol shall be used solely for the purposes of this Protocol. Where one of the Parties wishes to use such information for other purposes, it shall obtain the prior written consent of the authority which provided the information. Such use shall then be subject to any restrictions laid down by that authority. Article 13 - Protection of personal data 1. The Parties agree to cooperate in order to ensure a high level of protection of personal data in accordance with EU, Council of Europe and international legal instruments and standards. 2. Any processing of personal data shall be subject to the legal provisions referred to in Annex I to this Agreement. The transfer of personal data between the Parties shall only take place if such transfer is necessary for the implementation, by the competent authorities of the Parties, of this or other agreements concluded between the Parties. Article 99 – Cooperation may cover the following subjects: d) enhancing the level of security of personal data and the protection of privacy in electronic communications. Article 197 - Customs cooperation […] In order to ensure compliance with the provisions of this Chapter the Parties shall, inter alia: (d) exchange, where appropriate, information and data subject to respect of the confidentiality of data and standards and regulations on protection of personal data. Article 245 – Data processing

	2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights and freedoms of individuals, in particular with regard to the transfer of personal data. Article 261 - General exceptions 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by any Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to : (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts. Article 321 - Right of information 3. Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which: (e) govern the protection of confidentiality of information sources or the processing of personal data. Article 423 - Exchange of information and further cooperation at operational level 3. For the transfer and processing of personal data, Article 13 of Title III (Freedom, Security and Justice) of this Agreement shall apply.
United Kingdom of Great Britain and Northern Ireland	TITLE III - DIGITAL TRADE CHAPTER 2 - DATA FLOWS AND PERSONAL DATA PROTECTION Article 201 - Cross-border data flows 1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by a Party: (a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party; (b) requiring the localisation of data in the Party's territory for storage or processing; (c) prohibiting the storage or processing in the territory of the other Party; or (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory. 2. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the date of entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in paragraph 1. Such a request shall be accorded sympathetic consideration.

	Article 202 - Protection of personal data and privacy 1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade. 2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data transferred. 3. Each Party shall inform the other Party about any measure referred to in paragraph 2 that it adopts or maintains. Article 412 - General exceptions 1. Nothing in Chapter 1 and Chapter 5 of Title I, Chapter 2 of Title II, Title III, Title VIII and Chapter 4 of Title XI shall be construed as preventing a Party from adopting or maintaining measures compatible with Article XX of GATT 1994. To that end, Article XX of GATT 1994, including its Notes and Supplementary Provisions, is incorporated into and made part of this Agreement, mutatis mutandis. 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on investment liberalisation or trade in services, nothing in Title II, Title III, Title IV, Title VIII and Chapter 4 of Title XI shall be construed to prevent the adoption or enforcement by either Party of measures: c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to (ii)the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts Article 523 Definitions For the purposes of this Part, the following definitions apply (b) "special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; (f) "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed Article 525 Protection of personal data 1. The cooperation provided for in this Part is based on the Parties' long-standing commitment to ensuring a high level of protection of personal data 2. To reflect that high level of protection, the Parties shall ensure that personal data processed under this Part is subject to effective safeguards in the Parties' respective data protection regimes, including that: (a) personal data is processed lawfully and fairly, in compliance with the principles of data minimisation, purpose limitation, accuracy and storage limitation; (b) processing of special categories of personal data is only permitted to the extent necessary and subject to appropriate safeguards adapted to the specific

	risks of the processing; (c) a level of security appropriate to the risk of the processing is ensured through relevant technical and organisational measures, in particular as regards the processing of special categories of personal data; (d) data subjects are granted enforceable rights of access, rectification and erasure, subject to possible restrictions provided for by law which constitute necessary and proportionate measures in a democratic society to protect important objectives of public interest; (e) in the event of a data breach creating a risk to the rights and freedoms of natural persons, the competent supervisory authority is notified without undue delay of the breach; where the breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subjects are also notified, subject to possible restrictions provided for by law which constitute necessary and proportionate measures in a democratic society to protect important objectives of public interest; (f) onward transfers to a third country are allowed only subject to conditions and safeguards appropriate to the transfer ensuring that the level of protection is not undermined; (g) the supervision of compliance with data protection safeguards and the enforcement of data protection safeguards are ensured by independent authorities; and (h) data subjects are granted enforceable rights to effective administrative and judicial redress in the event that data protection safeguards have been violated. 3. The United Kingdom, on the one side, and the Union, also on behalf of any of its Member States, on the other side, shall notify the Specialised Committee on Law Enforcement and Judicial Cooperation of the supervisory authorities responsible for overseeing the implementation of, and ensuring compliance with, data protection rules applicable to cooperation under this Part. The supervisory authorities shall cooperate to ensure compliance with this Part 4. The provisions on the protection of personal data set out in this Part apply to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 5. This Article is without prejudice to the application of any specific provisions in this Part relating to the processing of personal data. Article 570 restrictions on access to and further use of transferred personal data 1. The transferring competent authority may indicate, at the moment of transferring personal data, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its onward transfer, erasure or destruction after a certain period of time, or its further processing. Where the need for such restrictions becomes apparent after the personal data have been transferred, the transferring competent authority shall inform the receiving competent authority accordingly. 2. The receiving competent authority shall comply with any restriction on access or further use of the personal data indicated by the transferring competent authority as described in paragraph 1. 3. Each Party shall ensure that information transferred under this Title was collected, stored and transferred in accordance with its respective legal framework. Each Party shall ensure, as far as possible, that such information has not been obtained in violation of human rights. Nor shall such information be transferred if, to the extent reasonably foreseeable, it could be used to request, hand down or execute a death penalty or any form of cruel or inhuman treatment

	Article 769 - Personal data protection 1. The Parties affirm their commitment to ensuring a high level of personal data protection. They shall endeavour to work together to promote high international standards. 2. The Parties recognise that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade, and are a key enabler for effective law enforcement cooperation. To that end, the Parties shall undertake to respect, each in the framework of their respective laws and regulations, the commitments they have made in this Agreement in connection with that right. 3. The Parties shall cooperate at bilateral and multilateral levels, while respecting their respective laws and regulations. Such cooperation may include dialogue, exchanges of expertise, and cooperation on enforcement, as appropriate, with respect to personal data protection. 4. Where this Agreement or any supplementing agreement provide for the transfer of personal data, such transfer shall take place in accordance with the transferring Party's rules on international transfers of personal data. For greater certainty, this paragraph is without prejudice to the application of any specific provisions in this Agreement relating to the transfer of personal data, in particular Article 202 and Article 525, and to Title I of Part Six. Where needed, each Party will make best efforts, while respecting its rules on international transfers of personal data, to establish safeguards necessary for the transfer of personal data, taking into account any recommendations of the Partnership Council under point (h) of Article 7(4). ARTICLE 782 – Interim provision for transmission of personal data to the United Kingdom 1. For the duration of the specified period, transmission of personal data from the Union to the United Kingdom shall not be considered as a transfer to a third country under Union law, provided that the data protection legislation of the United Kingdom on 31 December 2020, as it is saved and incorporated into United Kingdom law by the European Union (Withdrawal) Act 2018 and as modified by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) (88) (the "applicable data protection regime"), applies and provided that the United Kingdom does not exercise the designated powers without the agreement of the Union within the Partnership Council.
Republic of San Marino	No specific provision
Serbia	Article 81 – Protection of personal data Serbia shall harmonise its legislation concerning personal data protection with Community law and other European and international legislation on privacy upon the entry into force of this Agreement. Serbia shall establish one or more independent supervisory bodies with sufficient financial and human resources in order to efficiently monitor and guarantee the enforcement of national personal data protection legislation. The Parties shall cooperate to achieve this goal. Protocol 6 on Mutual administrative assistance in customs matters Article 1 - Definitions For the purposes of this Protocol: (d) ‘personal data’ shall mean all information relating to an identified or identifiable individual; Article 10 - Information exchange and confidentiality

	2. Personal data may be exchanged only where the Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Party that may supply them. To that end, the Parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community.
Turkey	ANNEXE 7 on mutual assistance between administrative authorities in customs matters Article 1 - Definitions For the purposes of this Annex: (e) 'personal data' shall mean all information relating to an identified or identifiable individual. Article 10 – obligation to observe confidentiality 2. Personal data may only be transmitted if the level of personal protection afforded by the legislation of the Parties is equivalent. The Parties shall ensure at least a level of protection based on the principles of Council of Europe Convention No 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.
Ukraine	Article 15 – Protection of personal data The Parties agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, including the relevant Council of Europe instruments. Cooperation on personal data protection may include, inter alia, the exchange of information and of experts. Article 129 – Data processing (inserted sub-section 6 - Financial services) 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. 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. Section 7 – Exceptions Article 141 – General exceptions 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed in such a way as to prevent the adoption or enforcement by any Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;

	ANNEX XLIII TO TITLE VI - FINANCIAL COOPERATION, WITH ANTI-FRAUD PROVISIONS Control and anti-fraud measures Article 1 - Exchange of information and enhanced cooperation at operational level Article 10 – Data protection 1. The communication of personal data shall only take place if such communication is necessary for the implementation of this Agreement by the competent authorities of Ukraine or the EU as the case may be. When communicating, processing or treating personal data in a particular case, in line with Article 15 the competent authorities of Ukraine shall abide by the relevant legislation of Ukraine, and the EU Authorities shall abide by the provisions of the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the EU institutions and bodies and on the free movement of such data. 2 In particular, the standards of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed on 28 January 1981 (ETS No. 108) and of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No. 181) shall apply to such communication. 3.In addition, the following principles shall apply: (a) both the communicating authority and the receiving authority shall take every reasonable step to ensure as appropriate the rectification, erasure or blocking of personal data where the processing does not comply with the provisions of this Article, in particular because those data are not adequate, relevant, accurate, or they are excessive in relation to the purpose of processing. This includes the notification of any rectification, erasure or blocking to the other Party; (b) upon request, the receiving authority shall inform the communicating authority of the use of the communicated data and of the results obtained there from; (c) personal data may only be communicated to the competent authorities. Further communication to other bodies requires the prior consent of the communicating authority; (d) the communicating and the receiving authorities are under an obligation to make a written record of the communication and receipt of personal data. PROTOCOL II on mutual administrative assistance in customs matters Article 1 - Definitions For the purposes of this Protocol:(d) 'personal data' means any information relating to an identified or identifiable natural person. Article 10 - Information exchange and confidentiality 2. Personal data may be exchanged only where the Party which may receive them undertakes to afford such data an adequate level of protection in

	accordance with the standards and legal instruments referred to in Article 15 of Title III Justice, Freedom and Security of this Agreement.
EU-MIDDLE EAST AGREEMENTS	
Agreements	**Relevant extracts on data protection**
Israel	PROTOCOL 5 on mutual assistance between administrative authorities in customs matters Article 1 - Definitions For the purposes of this Protocol: (e) "personal data" shall mean all information relating to an identified or identifiable individual. Article 10 - Obligation to observe confidentiality 2. Personal data may only be transmitted if the level of personal protection afforded by the legislations of the Parties is equivalent. The Parties shall ensure at least a level of protection based on the principles of Council of Europe Convention No 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.
Jordan	JOINT DECLARATION ON THE PROTECTION OF DATA The Parties agree that the protection of data will be guaranteed in all areas where the exchange of personal data is envisaged. PROTOCOL 4 on mutual assistance between administrative authorities in customs matters Article 1 – Definitions For the purposes of this Protocol: (d) 'personal data' shall mean all information relating to an for suspecting that they are intended to supply operations identified or identifiable individual. Article 10 – Information exchange and confidentiality 2. Personal data may be exchanged only where the receiving Party undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the supplying Party.
Lebanon	Article 53 information society and telecommunications 1. The Parties recognise that information and communication technologies constitute a key element of modern society, vital to economic and social development, and a cornerstone of the emerging information society. 2. Cooperation in this field shall aim at: [...] g) a dialogue on regulatory cooperation on international services, including aspects relating to protection of data and privacy. PROTOCOL 5 on mutual administrative assistance in customs matters

	Article 1 - Definitions For the purposes of this Protocol: (d) 'personal data' shall mean all information relating to an identified or identifiable individual; Article 10 – Information exchange and confidentiality 2. Personal data may be exchanged only where the Contracting Party which may receive it undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Contracting Party that may supply it. To that end, contracting parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community.
Palestine	Joint Declaration on data protection The Parties agree that the protection of data will be guaranteed in all areas where the exchange of personal data is envisaged.
EU-EASTERN ASIA AGREEMENTS	
Agreements	**Relevant extracts on data protection**
Republic of Korea	Article 6.8 – Confidentiality 2. Personal data may be exchanged only where the Party receiving the data undertakes to protect such data in a manner at least equivalent to that applicable to that particular case in the Party that may supply them. The person providing information shall not stipulate any requirements which are more onerous than those applicable to it in its own jurisdiction. 6. The requesting Party shall, unless otherwise agreed by the person who provided the information, wherever appropriate, use all available measures under the applicable laws and regulations of that Party to maintain the confidentiality of information and to protect personal data in case of applications by a third party or other authorities for the disclosure of the information concerned. Article 7.43 – Data processing [...] b) each Party, reaffirming its commitment to protect fundamental rights and freedom of individuals, shall adopt adequate safeguards to the protection of privacy, in particular with regard to the transfer of personal data. Article 7.50 - Exceptions Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by either Party of measures: [..] (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual

	records and accounts;
Japan	ARTICLE 8.3 – General Exceptions 2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or trade in services, nothing in Sections B to F shall be construed as preventing a Party from adopting or enforcing measures which are: c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ARTICLE 8.78 Consumer protection 3. The Parties recognise the importance of adopting or maintaining measures, in accordance with their respective laws and regulations, to protect the personal data of electronic commerce users. ARTICLE 18.1 Objectives and general principles 2. Nothing in this Section shall affect the right of a Party to define or regulate its own levels of protection in pursuit or furtherance of its public policy objectives in areas such as: (h) personal data and cybersecurity;
Singapore	ARTICLE 8.54 - Data Processing 1. Each Party shall, subject to appropriate safeguards on privacy and confidentiality, permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing, where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt or maintain appropriate safeguards to protect privacy and personal data, including individual records and accounts, as long as these safeguards are not used to circumvent the provisions of this Agreement. ARTICLE 8.62 – General Exceptions Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination against the other Party where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by a Party of measures: [..] e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; UNDERSTANDING 3 – CUSTOMS-RELATED PROVISIONS ARTICLE 9 – Information Exchange and Confidentiality 2. Personal data may be exchanged only where the Party which may receive them undertakes to protect such data in a manner that is considered adequate

	by the Party that may supply them.
Vietnam	Article 8.45 – Data Processing 1. Each Party shall adopt or maintain appropriate safeguards to protect personal data and privacy, including individual records and accounts. 2. No later than two years from the date of entry into force of this Agreement, each Party shall permit financial service suppliers of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service suppliers. 3. Nothing in this Article restricts the right of a Party to protect personal data and privacy, so long as such right is not used to circumvent this Agreement. Article 8.53 – General Exceptions Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination against the other Party where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by a Party of measures: [..] e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
EU-PACIFIC STATES AGREEMENTS	
Papua New Guinea, Fiji, Samoa, Solomon Islands	Article 42 – General exception clause Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in goods, services or establishment, nothing in this Agreement shall be construed to prevent the adoption or enforcement by the EC Party or Pacific States of measures which: c) are necessary to secure compliance with laws or regulations not inconsistent with the provisions of this Agreement, including those relating to (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
EU - NORTH AMERICA AGREEMENT	
Canada	Article 21.7 Further cooperation between the Parties 5. Before the Parties conduct the first exchange of information provided for under paragraph 4, they shall ensure that the Committee on Trade in Goods endorse the measures to implement these exchanges. The Parties shall ensure that these measures specify the type of information to be exchanged, the modalities for the exchange and the application of confidentiality and personal data protection rules Article 28.3 - General exceptions

	2. For the purposes of Chapters Nine (Cross-Border Trade in Services), Ten (Temporary Entry and Stay of Natural Persons for Business Purposes), Twelve (Domestic Regulation), Thirteen (Financial Services), Fourteen (International Maritime Transport Services), Fifteen (Telecommunications), Sixteen (Electronic Commerce), and Sections B (Establishment of investments) and C (Non-discriminatory treatment) of Chapter Eight (Investment), subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by a Party of measures necessary: c) to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Mexico	Article 22 – Data processing 2. As far as the transfer of personal data is concerned, each Party shall adopt adequate safeguards to the protection of privacy and fundamental rights, and freedom of individuals in accordance with Article 41 of the Agreement. Article 27 – Exceptions 2. Subject to the requirement that such measures are not arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Title shall be construed to prevent the adoption or enforcement by any Party of measures: c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
EU – CENTRAL AMERICA AGREEMENTS	
Costa Rica; El Salvador; Guatemala; Honduras; Nicaragua; Panama:	Article 34 – Personal Data Protection 1. The Parties agree to cooperate in order to improve the level of protection of personal data to the highest international standards, such as the Guidelines for the Regulation of Computerised Personal Data Files, modified by the General Assembly of the United Nations on December 14th 1990, and to work towards the free movement of personal data between the Parties, with due regard to their domestic legislation. 2. Cooperation on protection of personal data may include, inter alia, technical assistance in the form of exchange of information and expertise taking into account the laws and regulations of the Parties Article 198- Data Processing 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of the financial service supplier 2. Each Party shall adopt or maintain adequate safeguards to the protection of privacy and fundamental rights, and freedom of individuals, in particular with

	regard to the transfer of personal data Article 203 – General exceptions 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Title shall be construed to prevent the adoption or enforcement by any Party of measures which are: e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ANNEX III Article premier - Definitions For the purposes of this Annex: e) "personal data" means all information relating to an identified or identifiable individual; Article 10 – Information Exchange and Confidentiality 1. Personal data may be exchanged, in accordance with each Party's legislation, only where the Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Party that may supply them.
EU - SOUTH AMERICA AGREEMENTS	
Chile	Article 30 - Data protection 1. The Parties agree to cooperate on the protection of personal data in order to improve the level of protection and avoid obstacles to trade that requires transfers of personal data. 2. Cooperation on personal data protection may include technical assistance in the form of exchange of information and experts and the establishment of joint programmes and projects. Article 122 - Data processing in the financial services sector 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Where the information referred to in paragraph 1 consists of or contains personal data, the transfer of such information from the territory of one Party to the territory of the other Party shall take place in accordance with the domestic law regulating the protection of individuals with respect to the transferring and processing of personal data of the Party out of whose territory the information is transferred. Article 135 - Exceptions

	1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in services, financial services or establishment, nothing in this Title shall be construed to prevent the adoption or enforcement by either Party of measures : (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to : (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; Article 202 - Data Protection The Parties agree to accord a high level of protection to the processing of personal and other data, compatible with the highest international standards.
Colombia and Peru	Article 109 Working Groups To the extent necessary and justified, the Trade Committee may establish a working group with the aim of performing, among others, the following tasks: (b) proposing guidelines and strategies enabling the signatory Andean Countries to become a safe harbour for the protection of personal data. To this end, the working group shall adopt a cooperation agenda that shall define priority aspects for accomplishing that purpose, especially regarding the respective homologation processes of data protection systems; Article 157 Data Processing 1. Each Party shall permit a financial service supplier of another Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of the right to privacy and the freedom from interference with the privacy, family, home or correspondence of individuals, in particular with regard to the transfer of personal data Article 163 Regulatory Aspects of Electronic Commerce 1. The Parties shall maintain a dialogue on regulatory issues arising from electronic commerce which shall inter alia address the following issues: (e) the protection of personal data; Article 164 - Protection of Personal Data The Parties shall endeavour, insofar as possible, and within their respective competences, to develop or maintain, as the case may be, regulations for the protection of personal data. Article 167 - General Exceptions 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties, or a disguised restriction on establishment or cross-border supply of services, nothing in this Title and Title V (Current Payments and Capital Movements) shall be construed to prevent the adoption or enforcement by any Party of measures: e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title and Title V (Current Payments and Capital Movements) (55) including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of

	individual records and accounts; ANNEX V - MUTUAL ADMINISTRATIVE ASSISTANCE IN CUSTOMS MATTERS Article 1 – Definitions 'personal data' means any information relating to an identified or identifiable individual and may mean, if the legislation of the Party so provides, any information relating to an identified or identifiable legal person; Article 10 – Information Exchange and Confidentiality 2. Personal data may be exchanged only where the Party which may receive them undertakes to protect such data in at least an equivalent way to that applicable in that particular case in the Party that may supply them.
EU–CARIFORM STATES AGREEMENTS	
Antigua and Barbuda, Bahamas, Barbados, Belize, Cuba, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, Trinidad and	Article 107 – Data processing 2. The EC Party and the Signatory CARIFORUM States shall adopt adequate safeguards to the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data. Article 197 – General objective 1. The Parties and the Signatory CARIFORUM States, recognising: (d) their common interest in protecting fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, (e) the importance of maintaining effective data protection regimes as a means of protecting the interests of consumers, stimulating investor confidence and of facilitating transborder flows of personal data; (f) that the collection and processing of personal data should be accomplished in a transparent and fair manner, with due respect accorded to the data subject, agree to establish appropriate legal and regulatory regimes, as well as appropriate administrative capacity to implement them, including independent supervisory authorities, in order to ensure an adequate level of protection of individuals with regard to the processing of personal data, in line with existing high international standards. Article 198 - Definitions For the purposes of this Chapter: (a) 'personal data' means any information relating to an identified or identifiable individual (data subject); (b) 'processing of personal data' means any operation or set of operations which is performed upon personal data, such as collection, recording,

Tobago	organisation, storage, alteration, retrieval, consultation, use, disclosure, combination, blocking, erasure or destruction, as well as transfers of personal data across national borders; (c) 'Data Controller' means the natural or legal person, authority or any other body which determines the purposes and means of the processing of personal data. Article 199 – Principles and general rules The Parties agree that the legal and regulatory regimes and administrative capacity to be established shall, at a minimum, include the following content principles and enforcement mechanisms: a) Content principles: vi)restrictions on onward transfers — as a matter of principle, further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection; PARTIE IV GENERAL EXCEPTIONS Article 224 – General exception clause 1. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in goods, services or establishment, nothing in this Agreement shall be construed to prevent the adoption or enforcement by the EC Party, the CARIFORUM States or a Signatory CARIFORUM State of measures which: c) are necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (i) the protection of the privacy of individuals in relation to the processing and dissemination of personal data (ii)the protection of confidentiality of individual records and accounts;
EU – AFRICA AGREEMENTS	
Agreements	**Relevant extracts on data protection**
South Africa	PROTOCOL 2 on mutual administrative assistance in customs matters Article 10 - Information exchange and confidentiality Personal data may be exchanged only where the Contracting Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Contracting Party that may supply them. To that end, Contracting Parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community. Article 91 - Data protection The Parties shall cooperate to improve the level of protection to the processing of personal data, taking into account international standards.

Algeria	Article 45: The Parties undertake to adopt appropriate measures to ensure the protection of personal data in order to eliminate barriers to the free movement of such data between the Parties. Protocol 7 on mutual administrative assistance in the field of customs Article 1 d) 'personal data' shall mean all information relating to an identified or identifiable individual Article 10 - Exchange of information and confidentiality 2. Personal data may be exchanged only where the Contracting Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Contracting Party that may supply them. To that end, the Contracting Parties shall inform each other of their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community.
Cameroon	CHAPITRE 6 - Protection of personal data Article 61 - Overall objective The Parties, recognising: a) their common interest in protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data; b) the importance of maintaining effective data protection regimes as a means of protecting the interests of consumers, stimulating investor confidence and facilitating cross-border flows of personal data; c) the need to collect and process personal data in a transparent and fair manner, with due respect accorded to the data subject, agree to establish appropriate legal and regulatory regimes, and the appropriate administrative capacity to implement them, including independent supervisory authorities, in order to ensure an adequate level of protection of individuals with regard to the processing of personal data, in line with the highest international standards: i) Guidelines on computerised personal data files, as amended by the United Nations General Assembly on 20 November 1990. ii) Recommendation of the OECD Council of 23 September 1980 concerning guidelines governing the protection of privacy and trans-border flows of personal data. Article 62 - Definitions For the purposes of this Chapter: (a) 'personal data' shall mean any information relating to an identified or identifiable natural person (data subject); (b) 'processing of personal data' shall mean any operation or set of operations which is performed upon personal data, such as collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, combination, blocking, erasure or destruction, as well as transfers of personal data across national borders; (c) 'data controller' shall mean the natural or legal person, authority or any other body which determines the purposes and means of the processing of personal data.

	Article 63 - Principles and general rules The Parties agree that the legal and regulatory regimes and administrative capacity to be established shall, at a minimum, include the following content principles and enforcement mechanisms: (a) Content principles: (i) The purpose limitation principle — data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to these rights should be those provided for in legislation and necessary in a democratic society for the protection of important public interests. (ii) The data quality and proportionality principle — data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed. (iii) The transparency principle — individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions to these rights should be those provided for in legislation and necessary in a democratic society for the protection of important public interests. (iv) The security principle — the data controller should take technical and organisational security measures that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller. (v) The rights of access, rectification and opposition — the data subject should have the right to obtain a copy of all data relating to him/her that are processed, and the right to rectify those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be those provided for in legislation and necessary in a democratic society for the protection of important public interests. (vi) Restrictions on onward transfers — as a matter of principle, further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. (vii) Sensitive data — where special categories of data are involved, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, data concerning health and sex, and data relating to offences, criminal convictions or security measures, additional safeguards should be in place. (b) Enforcement mechanisms Appropriate mechanisms should be in place to ensure that the following objectives are achieved: (i) to ensure a good level of compliance with the rules, including a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them; the existence of effective and dissuasive sanctions; and systems of verification by authorities, auditors or independent data protection officials; (ii) to provide support and help to individual data subjects in the exercise of their rights, which they must be able to enforce rapidly and effectively, and without prohibitive cost, including through an appropriate institutional mechanism allowing independent investigation of complaints; (iii) to provide appropriate redress to the injured party where rules are not complied with, allowing compensation to be paid and sanctions imposed where

	appropriate. Article 64 - Consistency with international commitments 1. The Parties shall keep each other informed, via the EPA Committee, of the multilateral commitments and agreements with third countries in which they may participate, or of any obligation by which they may be bound and which could be relevant to the application of this Chapter, and in particular of any agreement providing for the processing of personal data, such as personal data being collected, stored or accessed by third parties or transferred to third parties. 2. The Parties may request consultations to discuss any matter which may arise.
Ivory Coast	Article 10 - Exchange of information and confidentiality 2. Personal data may be exchanged only where the Party which may receive it undertakes to protect such data in at least an equivalent way to that applicable to that particular case in the Party which may supply it. To that end, the Parties shall inform each other of their applicable rules, including, where appropriate, legal provisions in force in the Member States of the Community. Article 68 - General exception clause Subject to the requirement that such measures not be applicable in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in goods, services or establishment, this Agreement shall not be construed as preventing the adoption or enforcement by the Parties of measures which: […] c) are necessary to ensure compliance with laws and regulations and which are not incompatible with the provisions of this Agreement, including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Southern African Development Community (South Africa, Botswana, Eswatini, Lesotho, Mozambique, Namibia)	Article 10 - Information exchange and confidentiality 2. Personal data may be exchanged only where the Party which may receive them agrees to ensure an adequate level of protection of such data. To that end, the Parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the European Union.
Egypt	JOINT DECLARATION ON THE PROTECTION OF DATA The Parties agree that the protection of data will be guaranteed in all areas where the exchange of personal data is envisaged.

States of Southern and Eastern Africa (Comoros, Madagascar, Mauritius Island, Seychelles, Zimbabwe)	Article 56 -Clause General exception clause Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on international trade, nothing in this Agreement shall be construed to prevent the adoption or enforcement by the EC Party, the ESA States or a Signatory ESA State of measures which: c) are necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement, including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Ghana	Article 10 - Information exchange and confidentiality 2. Personal data may be exchanged only where the Party which may receive them undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Party that may supply them. To that end, the Parties shall communicate to each other information on their applicable rules, including, where appropriate, legal provisions in force in the Member States of the European Community. Article 68 - General exception clause Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in goods, services or establishment, nothing in this Agreement shall be construed to prevent the adoption or enforcement by the Parties of measures which: c) are necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Morocco	Article 1 - Definitions For the purposes of this Protocol: d) "personal data" shall mean any data relating to an identified or identifiable natural person. Annex FUNDAMENTAL PRINCIPLES APPLICABLE TO DATA PROTECTION 1. Personal data undergoing computer processing must be: (a) obtained and processed fairly and lawfully; (b) kept for explicit and legitimate purposes and not further used in a way incompatible with those purposes; (c) appropriate, relevant and not excessive in relation to the purposes for which they are collected; (d) accurate and, where necessary, kept up to date; (e) kept in a form which permits identification of the person concerned for no longer than is necessary for the procedure for which the data were collected. 2. Personal data revealing racial origin, political or religious opinions or other beliefs, and data concerning a person's health or sex life, may not undergo computer processing except where suitable safeguards are provided by national law. These provisions apply also to personal data relating to criminal

	convictions. 3. Appropriate security measures must be taken to ensure that personal data recorded in computer filing systems are protected against unlawful destruction or accidental loss and against unauthorised alteration, disclosure or access. 4. Any person must have the right to: (a) establish whether personal data relating to him are kept in a computer filing system, the purposes for which they are mainly used and the identity and normal place of residence or work of the person responsible for the filing system; (b) obtain at reasonable intervals, and without excessive delay or expense, confirmation as to the existence of a computer filing system containing personal data relating to him and communication of such data in an intelligible form; (c) obtain, as appropriate, the rectification or erasure of such data where they have been processed in violation of the provisions laid down by the national legislation applying the fundamental principles contained in paragraphs 1 and 2 of this Annex; (d) have access to legal remedies if no action is taken on a request for communication or, where appropriate, the communication, rectification or erasure referred to in points (b) and (c) above. 5.1. Derogations from the provisions of paragraphs 1, 2 and 4 of this Annex are allowed only in the cases below. 5.2. Derogations from the provisions of paragraphs 1, 2 and 4 of this Annex may be allowed where provided for in the legislation of the Contracting Party and where such derogation constitutes a necessary measure in a democratic society and is intended to: (a) safeguard national security, public order or a State's financial interests or prevent criminal offences; (b) protect the data subjects or the rights and freedoms of others. 5.3. In the case of computerised filing systems containing personal data used for statistical purposes or scientific research, the rights referred to in paragraphs 4(b), (c) and (d) of this Annex may be restricted by law where such use is clearly unlikely to constitute an invasion of privacy of the data subjects. 6. No provision in this Annex is to be interpreted as restricting or prejudicing a Contracting Party's power to grant data subjects wider protection than that provided for in this Annex.
Tunisia	Article 10 - Obligation to observe confidentiality 2. Personal data may be communicated only where the level of protection granted to persons laid down in the legislation of the Contracting Parties is equivalent. The Contracting Parties must ensure at least a level of protection based on the principles contained in the Annex to this Protocol. Annex FUNDAMENTAL PRINCIPLES APPLICABLE TO DATA PROTECTION 1. Personal data undergoing computer processing must be: (a) obtained and processed fairly and lawfully; (b) kept for explicit and legitimate purposes and not further used in a way incompatible with those purposes; (c) appropriate, relevant and not excessive in relation to the purposes for which they are collected;

	(d) accurate and, where necessary, kept up to date; (e) kept in a form which permits identification of the person concerned for no longer than is necessary for the procedure for which the data were collected. 2. Personal data revealing racial origin, political or religious opinions or other beliefs, and data concerning a person's health or sex life, may not undergo computer processing except where suitable safeguards are provided by national law. These provisions apply also to personal data relating to criminal convictions. 3. Appropriate security measures must be taken to ensure that personal data recorded in computer filing systems are protected against unlawful destruction or accidental loss and against unauthorised alteration, disclosure or access. 4. Any person must have the right to: (a) establish whether personal data relating to him are kept in a computer filing system, the purposes for which they are mainly used and the identity and normal place of residence or work of the person responsible for the filing system; (b) obtain at reasonable intervals, and without excessive delay or expense, confirmation as to the existence of a computer filing system containing personal data relating to him and communication of such data in an intelligible form; (c) obtain, as appropriate, the rectification or erasure of such data where they have been processed in violation of the provisions laid down by the national legislation applying the fundamental principles contained in paragraphs 1 and 2 of this Annex; (d) have access to legal remedies if no action is taken on a request for communication or, where appropriate, the communication, rectification or erasure referred to in paragraphs (b) and (c) above. 5.1. Derogations from the provisions of paragraphs 1, 2 and 4 of this Annex are allowed only in the cases below. 5.2. Derogations from the provisions of paragraphs 1, 2 and 4 of this Annex may be allowed where provided for in the legislation of the Contracting Party and where such derogation constitutes a necessary measure in a democratic society and is intended to: (a) safeguard national security, public order or a State's financial interests or prevent criminal offences; (b) protect the data subjects or the rights and freedoms of others. 5.3. In the case of computerised filing systems containing personal data used for statistical purposes or scientific research, the rights referred to in paragraphs 4(b), (c) and (d) of this Annex may be restricted by law where such use is clearly unlikely to constitute an invasion of privacy of the data subjects. 6. No provision in this Annex is to be interpreted as restricting or prejudicing a Contracting Party's power to grant data subjects wider protection than that provided for in this Annex.

II-MAPPING OF G7 ET G20 AND WORLD TRADE ORGANISATION INITIATIVES

G20	
Declarations/ Statement	**Relevant extracts on data protection**
7/8 July 2017- Germany (Hamburg) Leaders' Declaration – 8 July 2017	Trust in digital technologies requires effective consumer protection, intellectual property rights, transparency, and security in the use of ICT. We support the free flow of information while respecting applicable legal frameworks for privacy, data protection and intellectual property rights. The G20 Roadmap for Digitalisation will help us guide our future work
Digital Economy Ministerial Declaration – 7 April 2017	Users can increasingly benefit from the digital world. G20 countries will support the free flow of information while respecting applicable domestic and/or international legal frameworks for privacy and data protection, and strengthening security in the use of ICT as well as transparency and consumer protection. We reaffirm support for ICT policies that preserve the global nature of the Internet, promote the flow of information across borders, and allow Internet users to lawfully access online information, knowledge and services of their choice. At the same time the G20 recognizes that applicable frameworks for privacy and personal data protection, as well as intellectual property rights, have to be respected as they are essential to strengthening confidence and trust in the digital economy. We further recognize that there is also a need to meet certain legitimate policy objectives to take advantage of the benefits of digitalisation. Furthermore, we encourage international co-operation among the G20 in the above mentioned policy objectives, while also supporting cooperation efforts at the broader international level and including to assist countries to bridge the digital divide.
30 November – 1 December 2018 - Argentina (Buenos Aires) Leaders' Declaration - 1 December 2018	To maximize the benefits of digitalization and emerging technologies for innovative growth and productivity, we will promote measures to boost micro, small and medium enterprises and entrepreneurs, bridge the digital gender divide and further digital inclusion, support consumer protection, and improve digital government, digital infrastructure and measurement of the digital economy. We reaffirm the importance of addressing issues of security in the use of ICTs. We support the free flow of information, ideas and knowledge, while respecting applicable legal frameworks, and working to build consumer trust, privacy, data protection and intellectual property rights protection. [...]
Digital Economy Ministerial Declaration - 24 August 2018	We encourage G20 members to continue their actions to i) develop comprehensive, high-quality data infrastructures for measuring the use and consequences of digital technologies, such as the Internet of things and big data, at the individual and business levels; (ii) actively participate in actions for the development and improvement of international measurement standards for the digital economy; iii) work collaboratively to bridge existing measurement gaps in key dimensions such as capturing the creation of economic value in the digital economy, measuring data flows, the interface between trade and the digital economy, skills and education; including breakdowns by sex, age, business size, sector, and location where appropriate;

	iv) build capacity to improve data collection and dissemination, and research data quality; and v) explore more diverse sources of data and tools that could be used to improve digital economy measurement, allow a better use of available data, and enable the conversation between businesses, government and other actors from civil society to strengthen the evidence base and complement current statistics. To avoid fragmentation of statistical efforts, we encourage IOs, where appropriate, to consider examples of digital economy measurement efforts by G20 countries
28/29 June 2019 - Japan (Osaka) Leaders' Declaration – 29 June 2019 Digital Economy Ministerial Declaration – 9 June 2018	Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. Such data free flow with trust will harness the opportunities of the digital economy. We will cooperate to encourage the interoperability of different frameworks, and we affirm the role of data for development. We also reaffirm the importance of interface between trade and digital economy, and note the ongoing discussion under the Joint Statement Initiative on electronic commerce, and reaffirm the importance of the Work Programme on electronic commerce at the WTO. Reaffirming the commitments made in Hangzhou, Dusseldorf, and Salta, we share the understanding that digitalization gives us the opportunity to promote inclusive and sustainable economic growth. Digitalization also promotes social and cultural progress and development, fosters innovation, and empowers individuals and businesses, including micro, small, and medium-sized enterprises (MSMEs) to benefit from emerging technologies and data. Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development. At the same time, we recognize that the free flow of data raises certain challenges. By continuing to address challenges related to privacy, data protection, intellectual property rights, and security, we can further facilitate data free flow and strengthen consumer and business trust. In order to build trust and facilitate the free flow of data, it is necessary that legal frameworks both domestic and international should be respected. Such data free flow with trust will harness the opportunities of the digital economy. We will cooperate to encourage the interoperability of different frameworks, and we affirm the role of data for development
20/21 November 2020 – South Arabia (Riyadh) Leaders' Declaration - 21 November 2020	Connectivity, digital technologies, and policies have played a key role in strengthening our response to the pandemic and facilitating the continuation of economic activity. We take note of the Policy Options to Support Digitalization of Business Models during COVID-19. We acknowledge that universal, secure, and affordable connectivity, is a fundamental enabler for the digital economy as well as a catalyst for inclusive growth, innovation and sustainable development. We acknowledge the importance of data free flow with trust and cross-border data flows. We reaffirm the role of data for development. We support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these

	challenges, in accordance with relevant applicable legal frameworks, we can further facilitate data free flow and strengthen consumer and business trust. We recognize the importance of working with stakeholders to connect humanity by accelerating global internet penetration and bridging digital divides. We recognize the importance of promoting security in the digital economy and welcome the G20 Examples of Practices Related to Security in the Digital Economy. We will continue to promote multi-stakeholder discussions to advance innovation and a human-centered approach to Artificial Intelligence (AI), taking note of the Examples of National Policies to Advance the G20 AI Principles. We welcome both the G20 Smart Mobility Practices, as a contribution to the well-being and resilience of smart cities and communities, and the G20 Roadmap toward a Common Framework for Measuring the Digital Economy
30/31 October 2021- Italy (Roma) Digital Economy Ministerial Declaration - 5 August 2021	Digital Economy Ministers, in 2020, recognised the opportunities and challenges of data free flow with trust and cross-border data flows and the need to address these challenges such as those related to privacy, data protection, intellectual property rights and security, in accordance with the relevant applicable legal frameworks, including by identifying commonalities between existing approaches and instruments used to enable data to flow with trust across borders. Against this backdrop, building upon and recognising the work and achievements of the Japanese and Saudi Presidencies, we acknowledge the work of the OECD on *Mapping Commonalities in Regulatory Approaches to Cross-border Data Transfers* which identifies the "commonalities, complementarities and elements of convergence"across different approaches. Such commonalities can foster future interoperability
G7	
Declarations/ Statement	**Relevant extracts on data protection**
26/27 May 2017 (Italy) Leaders' Communiqué - 27 May 2017	No specific provision/commitment
8/9 June 2018 (Canada) Leaders' Communiqué - 9 June 2018	No specific provision/commitment
24/26 August 2019 (France) Leaders' Communiqué - 26 August 2019 Declaration "Biarritz strategy for an Open, Free and Secure digital transformation" - 26 August 2019	We recognize that cross-border flow of data, information, ideas and knowledge generate higher productivity, greater innovation, and improved sustainable development, while it can raise issues related to privacy, data protection, intellectual property rights, and security. Data free flow with trust will harness the opportunities of the digital transformation. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. We will cooperate to encourage interoperability of different frameworks, and we affirm the role of data for development
10/12 June 2020 (US)	No specific provision/commitment

Road to the US summit	
11/13 June 2021 (UK)	
Trade Ministers' Communiqué: 27/28 May 2021	We are united in our opposition to digital protectionism. We agree on the importance of data free flow with trust, and in this regard, we welcome and support the OECD's work on digital trade and data flows. We recognise that data localisation can impact data flows, with possible consequences for businesses, particularly micro, small, and medium-sized enterprises. We recognise the importance of unlocking the power of data in our economies and our societies, while continuing to address challenges related to privacy, data protection, intellectual property rights, and security
Digital and Technology Ministers' Declaration - 28/04/2021	We believe that it is vital we work together to better leverage the potential of valuable data-driven technologies, promote international cooperation to drive benefits for our economies and societies, and ensure personal data are appropriately protected, while recognising our varied approaches to data governance.[…] we endorse a Roadmap for Cooperation on Data Free Flow with Trust which sets out our plan for delivering tangible progress on this agenda, building confidence for businesses and individuals to use technology, as well as driving economic and social value. As part of this Roadmap, we will work to accelerate the development of mutually acceptable data sharing practices for agreed priority sectors, and we will build evidence on the economic and societal impacts of data localisation measures. We will also champion progress of the OECD's work on 'Mapping commonalities in regulatory approaches to cross-border data transfers' and on trusted 'Government access to personal data held by the private sector'
Leaders' Communiqué – 13/06/2021	Championing data free flow with trust, to better leverage the potential of valuable data-driven technologies while continuing to address challenges related to data protection. To that end we endorse our Digital Ministers' Roadmap for Cooperation on Data Free Flow with Trust.
Roadmap for cooperation on data free flow with trust (Annex 2 of Digital Ministers' Declaration – 28 April 2021)	Data Localisation: Build an evidence base on the impact of data localisation measures and alternative policy responses to these approaches (recognising consistency with the Trade Ministerial Track). This will bring together evidence from national authorities and external stakeholders, such as academia and business groups, with information from other fora to help inform future multilateral and plurilateral discussions. These will include the G20 Digital Economy Task Force, the Working Party on Data Governance and Privacy in the Digital Economy of the OECD Committee on Digital Economy Policy, and the Working Party of the OECD Trade Committee, as well as the Internet and Jurisdiction Policy Network Regulatory cooperation: Differences in domestic approaches can impact cross-border data flows, creating uncertainty (including legal uncertainty) for governments, businesses and individuals. The G7 Digital and Tech officials will promote work to identify commonalities in regulatory approaches to cross-border data transfers, as well as good regulatory practices and

	cooperation between nations Government Access to Data: We are committed to maintaining domestic data protection and privacy standards, reasonable principles underpinning lawful access regimes, as well as legal powers and arrangements that facilitate access across borders. Support the aims and objectives of the OECD's drafting group working on trusted 'Government access to personal data held by the private sector. Data Sharing for Priority Sectors: The G7 is collaborating on interoperability and standards for health data as part of the Health Ministerial Track. We will work to meaningfully accelerate the development of mutually acceptable data sharing practices for a broader set of priority sectors.
Trade Ministers' Communiqué - 22 October 2021	Data free flow with trust -To harness the opportunities of the digital economy and support the trade of goods and services, data should be able to flow freely across borders with trust, including the trust of individuals and businesses. - We are concerned about situations where data localisation requirements are being used for protectionist and discriminatory purposes, as well as to undermine open societies and democratic values, including freedom of expression. - We should address unjustified obstacles to cross-border data flows, while continuing to address privacy, data protection, the protection of intellectual property rights, and security. - Personal data must be protected by high enforceable standards, including when it is transferred across borders. We recognise the importance of enhancing cooperation on data governance and data protection and identifying opportunities to overcome differences. We will cooperate to explore commonalities in our regulatory approaches and promote interoperability between G7 members. - Non-personal data should benefit from protection, including all applicable protection as intellectual property, such as the protection of trade secrets. - Achieving consensus on common principles for trusted government access to personal data held by the private sector will help to provide transparency and legal certainty. It will support the transfer of data between jurisdictions by commercial entities and result in positive economic and social impacts. We support the OECD's work on developing these principles, recognising the importance of legitimate access to protect citizens and safeguard national security. - Open government data can play an important role in digital trade. Where appropriate, public sector datasets should be published in anonymised, open, interoperable, and accessible forms.

World Trade Organisation	
Agreements	**Relevant extracts on data protection**
General Agreement on Trade in Services https://www.wto.org/french/docs_f/legal_f/26-gats_01_f.htm	Article XIV: General Exceptions Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
Round of negotiations on Electronic Commerce **Joint Statement on Electronic Commerce of 26 April 2019 – Communication presented by the European Union** https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/22.pdf&Open=True	**2.7 Cross-border data flows:** 1. Members are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted by: (a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member; (b) requiring the localization of data in the Member's territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localization requirements in the Member's territory. **2.8 Protection of personal data and privacy:** 1. Members recognize that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade. 2. Members may adopt and maintain the safeguards they deem appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in the agreed disciplines and commitments shall affect the protection of personal data and privacy afforded by the Members respective safeguards. 3. Personal data means any information relating to an identified or identifiable natural person.
Understanding on commitments in financial services	**B. Transfers of Information and Processing of Information**

https://www.wto.org/french/tratop_f/serv_f/21-fin_f.htm	8. No Member shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this paragraph restricts the right of a Member to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of the Agreement.

III-MAPPING OF BILATERAL AND MULTILATERAL TRADE AGREEMENTS BETWEEN THIRD COUNTRIES

Third countries agreements	Relevant extracts on data protection
Canada – United States – Mexico Agreement (CUSMA) – Free Trade Agreement Signed on 30 November 2018 – Entered into force on 1 July 2020 Canada – United States – Mexico Agreement - Table of contents (international.gc.ca)	**Article 19.11: Cross-Border Transfer of Information by Electronic Means** 1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person. 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: (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 necessary to achieve the objective. **Article 32.8: Personal Information Protection** 1. For the purposes of this Article: personal information means information, including data, about an identified or identifiable natural person. 2. Each Party shall adopt or maintain a legal framework that provides for the protection of personal information. In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). 3. The Parties recognize that, pursuant to paragraph 2 key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. 4. Each Party shall endeavor to adopt non-discriminatory practices in protecting natural persons from personal information protection violations occurring within its jurisdiction. 5. Each Party shall publish information on the personal information protections it provides, including how: (a) individuals can pursue a remedy; and (b) an enterprise can comply with legal requirements. 6. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. The Parties shall endeavor 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. The Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal

	information. 7. The Parties shall endeavor to foster cooperation between appropriate government agencies regarding investigations on matters involving personal information protection and encourage the development of mechanisms to assist users to submit cross-border complaints regarding protection of personal information. **Article 32.9: Access to Information** Each Party shall maintain a legal framework that allows a natural person in its territory to obtain access to records held by the central level of government subject to reasonable terms and limitations specified in the Party's law, provided that the terms and limitations applying to natural persons of another Party in the Party's territory are no less favorable than those applying to natural persons of the Party, or of another country, in the Party's territory.
Comprehensive and Progressive Trans-Pacific Partnership (Canada, Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam) Signed on 8 March 2018 and entered into force on 30 December 2018 https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/toc-tdm.aspx?lang=fra	**Chapter 11 – Financial services** **Article 11.8: Treatment of Certain Information** Nothing in this Chapter shall require a Party to furnish or allow access to: (a) information related to the financial affairs and accounts of individual customers of financial institutions or cross-border financial service suppliers; **Annexe 11-B** **Specific Commitments** **Section B: Transfer of Information** Each Party shall allow a financial institution of another Party to transfer information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business. Nothing in this Section restricts the right of a Party to adopt or maintain measures to: (a) protect personal data, personal privacy and the confidentiality of individual records and accounts; or (b) require a financial institution to obtain prior authorisation from the relevant regulator to designate a particular enterprise as a recipient of such information, based on prudential considerations, provided that this right is not used as a means of avoiding the Party's commitments or obligations under this Section. **Section D: Electronic Payment Card Services** 3. Nothing in this Section shall be construed to prevent a Party from adopting or maintaining measures for public policy purposes, provided that these measures are not used as a means to avoid the Party's obligation under this Section. For greater certainty, such measures may include:

	(a) measures to protect personal data, personal privacy and the confidentiality of individual records, transactions and accounts, such as restricting the collection by, or transfer to, the cross-border services supplier of another Party, of information concerning cardholder names; **Chapter 14 - Electronic Commerce** **Article 14.8: Personal Information Protection** 1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce. 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. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies. Footnote 6 3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction. 4. Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) business can comply with any legal requirements. 5.Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. **Article 14.11: 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. 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.
Regional Comprehensive Economic Partnership Agreement (Burma, Brunei, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Vietnam, Australia, China, Japan, South Korea et New Zealand). Signed on 15 November 2020. https://rcepsec.org/legal-text/	**CHAPTER 1- INITIAL PROVISIONS AND GENERAL DEFINITIONS** **Article 1.2: General definitions** (u) personal information means any information, including data, about an identified or identifiable individual; **Chapter 12 – Electronic commerce** **Article 12.8: Online Personal Information Protection** 1. Each Party shall adopt or maintain a legal framework which ensures the protection of personal information of the users of electronic commerce. 2. In the development of its legal framework for the protection of personal information, each Party shall take into account international standards, principles, guidelines, and criteria of relevant international organisations or bodies[4]. 3. Each Party shall publish information on the personal information protection it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) business can comply with any legal requirements. 4. The Parties shall encourage juridical persons to publish, including on the internet, their policies and procedures related to the protection of personal information. 5. The Parties shall cooperate, to the extent possible, for the protection of personal information transferred from a Party.

[4] Footnote n 8: "For greater certainty, a Party may comply with the obligation under this paragraph by adopting or maintaining measures such as comprehensive privacy or personal information protection laws and regulations, sector-specific laws and regulations covering the protection of personal information, or laws and regulations that provide for the enforcement of contractual obligations assumed by juridical persons relating to the protection of personal information."