Adequate Level of Data Protection and ADR in Cross-border Data Disputes — International Trade Law Perspective

Tsai-fang Chen*

Abstract

Regulatory measures on cross-border data flows are essential to personal data protection laws. The General Data Protection Regulation ("GDPR") of the European Union ("EU") is one of such influential personal data protection regimes, which has become a model and has been adopted by many countries. The GDPR aims to ensure the protection of natural persons regarding the processing of personal data. To protect personal data outside the EU, the GDPR provides certain safeguards for its movement across the EU border. Under the GDPR, the European Commission can make a finding that a third country ensures an adequate level of protection, and the transfer of personal information to that country does not require specific authorization ("the adequacy approach"). Adequacy decisions are critical for the operation of digital trade, considering the costs and uncertainty associated with other conditions of cross-border transfer of personal data. Many countries have adopted the adequacy approach. The approach, however, creates serious trade concerns of trade barriers, discrimination, and necessity issues. While the costs of the adequacy mechanism to the free flow of data are concrete, it is questionable whether the adequacy approach would provide adequate protection for data subjects who would like to exercise their rights of data protection abroad, even in a country with adequacy status once disputes regarding the subject's data arise. This paper argues that the adequacy approach should be improved by adopting effective ADR mechanisms, including arbitration. Adopting an effective data dispute ADR mechanism would mean that the adequacy approach could be relaxed to reduce trade concerns.

* Tsai-fang Chen, Associate Professor, School of Law, National Yang Ming Chiao Tung University. WTO Co-Chair, WTO Chairs Programme; Senior Research Fellow, Asian Center for WTO & International Health Law and Policy. The author can be reached at tfc@nycu.edu.tw.

The smooth operation of the data-driven economy heavily relies on data flow. It is particularly the case for the supply of trade in services. The importance of cross-border data flows increases as technology improves.[1] Cross-border data flow through the internet has become essential for economic growth.[2] Data regulations adopted by World Trade Organization (WTO) Members could affect the free movement of data, which may result in a barrier to the supply of trade in services that requires free data flow.[3] The General Data Protection Regulation ("GDPR")[4] of the European Union ("EU") is one of such influential personal data protection regimes. Indeed, GDPR has become a model for data protection regimes and has been adopted by many countries. The GDPR aims to ensure the protection of natural persons concerning the processing of personal data. The level of protection provided under the GDPR is very high, but from the perspective of remedies afforded to the subject of personal data, it can be problematic if the personal data is transferred outside of the EU. To protect personal data, the GDPR provides certain safeguards for its movement across the EU border. Under the GDPR, the European Commission can make a finding that a third country ensures an adequate level of protection, and the transfer of personal information to that country does not require specific authorization[5]. Otherwise, stringent requirements should be met before personal data can be transferred across the national border.[6] Given the vast number of transfers involved, the adequacy decision is one of the most important decisions concerning the cross-border transfer of personal data under the GDPR. Personal protection regimes in many other countries likewise adopt the adequacy mechanism.

Under the adequacy mechanism of personal data protection regimes, a country's adequacy status would substantially impact the competitive position of its service providers supplying digital services to consumers in the EU. Foreign providers of data services may be less likely to own local data infrastructures.[7] Accordingly, services and service providers, if located in a country that does not receive the adequate decision, would be put at a competitive

[1] Dorine R. Seidman, *Transborder Data Flow: Regulation of International Information Data Flow and the Brazilian Example*, 1 J.L. & TECH. 31, 31-32 (1986).
[2] Joshua Meltzer, *the Internet, Cross-Border Data Flows and International Trade*, 2 ASIA & PAC. POL'Y STUD. 90, 90-92 (2014).
[3] *See* Daniel Crosby, *Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments* (E15 Initiative, March 2016), http://e15initiative.org/wp- content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Date Protection Regulation) [2016] 0J L 119/1 [hereinafter GDPR].
[5] GDPR, Article 45.
[6] *See* GDPR, Articles 46-49.
[7] Anupam Chander, *The Internet of Things: Both Goods and Services*, 18 WORLD TRADE REV. s9, s15 (2019).

disadvantage against those in a country that does. The process for the adequacy determination, therefore, has serious consequences and is critical in determining the EU's consistency with non-discrimination obligations under the General Agreement on Trade in Services (GATS). As other data protection regimes have adopted the adequacy decision mechanism, this issue is not only limited to the EU but also relevant to similar data regulatory regimes.

The adequacy approach creates trade concerns of trade barriers, discrimination, and necessity issues, which increases difficulties to the free flow of data. Therefore, it is necessary to ensure that the adequacy approach would provide adequate protection for data subjects who would like to exercise their rights of data protection abroad. However, once disputes regarding the subject's data arise, the currently available judicial remedies under adequacy mechanisms might not be sufficient even in a country with adequacy status. The trade-off in this regard is one of the most problematic areas in adequacy mechanisms. This paper argues that the adequacy approach should be improved by adopting effective ADR mechanisms, including arbitration. Adopting an effective data dispute ADR mechanism would mean that the adequacy approach could be relaxed to reduce trade concerns.

1. The Adequacy Mechanism under the GDPR

Under the GDPR, personal data can be transferred to a third country for processing only if certain conditions are satisfied.[8] The purpose of this restriction is to ensure that the level of protection of natural persons provided under the GDPR is not undermined.[9] According to Article 45.1 of the GDPR, such transfer is allowed if the Commission has decided that the destination of such transfer ensures an adequate level of protection, i.e., an adequacy decision has been made by the Commission. According to the CJEU, an adequate level of protection requires that the "level of protection" in the third country must be "essentially equivalent" to that provided in the EU.[10] The purpose of adequacy decisions by the European Commission is to formally confirm with binding effects on Member States that the level of data protection in a third country is essentially equivalent to the level of data protection in the European Union.[11]

Transferring personal information to the country with the adequacy status does not require specific authorization.[12] Free transfer of personal data is allowed, and services can be

[8] GDPR, Article 44.
[9] *Id.*
[10] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (¶¶ 73,74) [*hereinafter* Schrems I].
[11] Schrems I, ¶ 52; Article 29 Working Party, Adequacy Referential 2, WP 254 rev.01 (Feb. 6, 2018).
[12] GDPR, Article 45.

provided without restriction from data protection rules. Otherwise, stringent requirements should be met before personal data can be transferred across the national border.[13] Here, the adequacy status would have a serious impact on the condition of competition regarding service trade. The relevant rules under the GDPR that cause discriminatory treatment between origins of services can create an issue of non-discrimination obligations under international trade rules.

The rules regarding how adequacy decisions are made can also be problematic from the perspective of non-discrimination obligations under international trade rules. Article 45.2 provides the elements to be considered when making the adequacy decision. The elements to be taken into account by the Commission includes (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, data protection rules and case law, effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; [14] (b) the existence and effective functioning of one or more independent supervisory authorities in the third country with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States;[15] (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.[16] The express stipulation of the elements to be considered for an adequacy decision is an improvement over the GDPR's predecessor,[17] the data protection Directive,[18] regarding n the transparency of the decision. An independent European Data Protection Board would provide the Commission with opinions for the assessment of the adequacy of a third country's level of protection.[19]

In addition to the personal data protection rules themselves (rules *per se*), their application can also lead to potential violations of international trade norms, in particular, non-

[13] *See* GDPR, Articles 46-49.
[14] GDPR, Article 45(2)(a).
[15] GDPR, Article 45(2)(b).
[16] GDPR, Article 45(2)(c).
[17] Paul Roth, *"Adequate level of data protection" in third countries post-Schrems and under the General Data Protection*, 25(1) Journal of Law, Information, and Science 49, 55 (2017).
[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 ("Directive").
[19] GDPR, Article 70(1)(s).

discrimination obligations (rules as applied). Even if the rules are consistent with non-discrimination obligations, their application of the rules could still violate relevant obligations. Even though the GDPR provides these elements for the Commission to consider when making adequacy decisions, the decision is still a challenging and complex process characterized by uncertainty. Currently, the European Commission only recognizes 14 jurisdictions, many of which are small in size and economic power. These jurisdictions include Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, Uruguay, and the United Kingdom.[20]

The decision may require negotiation and cooperation between authorities. Adequacy decisions are "'living' documents" that "need to be closely monitored and adopted in case of developments affecting the level of protection ensured by the third country."[21] Therefore, the adequacy status of a country may change over time.[22] Indeed, the Commission is tasked to continue monitoring the protection level in third countries.[23] The Commission shall repeal, amend or suspend an adequacy decision if the third country no longer ensures an adequate level of protection.[24] As the decision takes time, however, the adequacy status of any country may not always correspond to its actual level of protection at any given moment.

Adequacy findings can be made in light of the extent of the EU's (actual or potential) commercial relations with a given third country, including (a) the existence of a free trade agreement or ongoing negotiations; (b) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties; (c) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and (d) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.[25] These criteria suggest that when making adequacy decisions, the Commission takes into account considerations other than the strict level of data protection. For example, even though New Zealand's rules relating to the onward transfer of information were considered insufficient, the country still received adequacy status. It was because the Commission considered that it is

[20] EU, Adequacy decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[21] European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World (Communication No COM(2017) 7 Final, European Commission, 10 January 2017, 8-9.
[22] Roth, *supra* note 17, at 59.
[23] GDPR, Article 45(3), (4).
[24] GDPR, Article 45(5).
[25] European Commission, *supra* note 21, at 8.

unlikely that significant volumes of EU-sourced data would be transferred to third countries, taking into consideration "the geographical isolation of New Zealand from Europe, its size and the nature of its economy."[26] In addition, a country may receive adequacy status easier if it is an "important trade partner" with the EU, for example, in the situation of Argentina, Canada, and the United States[27]. Accordingly, political considerations could be taken into account when making adequacy decisions.[28]

Due to the existence of adequacy requirements, services and service providers originating from different countries may receive differential treatments, which affect the condition of competition to the detriment of those whose countries are not considered adequate. The consistency of such adequacy requirements with non-discrimination obligations under trade rules is therefore called into question. As the adequacy requirements under the GDPR have become a model adopted by data protection laws globally, the consistency of such rules with trade rules has become more critical.

2. Redress Mechanisms under the GDPR Adequacy Decision Making

One crucial element in determining the adequacy status of a third country is whether the third country provides adequate judicial remedies. Under GDPR Art. 45.2(a), when assessing the adequacy of the level of protection, the Commission shall consider the "effective administrative and judicial redress for the data subjects whose personal data are being transferred." This element is part of the examination of the implementation of relevant legislation in the third country.[29]

The CJEU confirmed this in its case law. In Schrems I, the CJEU ruled that "Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data,

[26] Jacob Kohnstamm, Opinion 11/2011 on the level of protection of personal data in New Zealand (Opinion No 00665/11/EN WP 182, European Commission, 4 April 2011), 10.
[27] *Id.* at 7.
[28] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW (Oxford University Press, 2013) 66 ("In practice, it can be difficult for a State or regional organization to pass judgment on a foreign regulatory system without political considerations playing some role.")
[29] GDPR Art. 45: "When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements: (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as *the implementation of such legislation, data protection rules, professional rules and security measures, including* rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, a*s well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred* . . . ." (emphasis added).

does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."[30] In Schrems II, the CJEU further stipulated that the GDPR "requires the Commission, in its assessment of the adequacy of the level of protection in a third country, to take account, in particular, of 'effective administrative and judicial redress for the data subjects whose personal data are being transferred'."[31] The Court noted that "Recital 104 of the GDPR states, in that regard, that the third country 'should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities', and adds that 'the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress'."[32] Indeed, in both decisions, the CJEU considered that the United States does not provide adequate protection of personal data from the EU, partly based on the lack of a redress mechanism addressing state actions based on state measures for the purpose of national security.[33]

The effective judicial and administrative redress afforded to data subjects is therefore centered on the administrative and judicial authorities within the jurisdiction of the third country.[34] Specifically, under Schrems II, the CJEU specified the rationales for this requirement and held that "The existence of such effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since . . . data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects' complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country."[35] GDPR provides a strong remedies mechanism under Art. 77

[30] Schrems I, ¶ 95.
[31] Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18, EU:C:2020:559, ¶ 188 [*hereinafter* Schrems II].
[32] *Id.*
[33] Schrems I, ¶¶ 90, 95; Schrems II, ¶¶ 191-92.
[34] This can also be the case when the transfer of personal data to a third country is pursuant to an international agreement, as discussed under CJEU's PNR Opinion, which provides that "As regards air passengers' right to redress, Article 14(2) of the envisaged agreement provides that Canada is to ensure that any individual who is of the view that their rights have been infringed by a decision or action in relation to their PNR data may seek effective judicial redress, in accordance with Canadian law, or such other remedy which may include compensation." Opinion pursuant to Article 218(11) TFEU — Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada — Appropriate legal bases — Article 16(2), point (d) of the second subparagraph of Article 82(1) and Article 87(2)(a) TFEU — Compatibility with Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union), Opinion 1/15, ¶ 226 (26 July 2017) [*hereinafter* PNR Opinion].
[35] *Schrems II*, ¶ 189.

(Right to lodge a complaint with a supervisory authority), Art. 78 (Right to an effective judicial remedy against a supervisory authority), Art. 79 (Right to an effective judicial remedy against a controller or processor), Art. 82 (Right to compensation and liability), Article 83 (General conditions for imposing administrative fines), and Article 84 (Penalties), among other provisions. The basic structure is composed of administrative authorities and courts. The rulings regarding third countries focusing on national authorities and courts reflect the redress mechanisms envisioned under GDPR.

While redress mechanisms are considered necessary for an adequacy status, the CJEU did not limit the dispute resolution to courts. The CJEU in Schrems I analyzed procedures before the Federal Trade Commission under safe harbour and held that they are limited to commercial disputes and cannot be applied in disputes relating to the legality of interference with fundamental rights that result from measures originating from the States.[36] In Schrems II, the CJEU analyzed the Ombudsperson mechanism under the U.S. State Department and held that the mechanism did not provide a sufficient redress mechanism.[37] While the CJEU did not discuss private dispute resolutions, it is the result of the focus on the redress mechanism addressing U.S. intelligence services.

3. The Costs to Trade and the WTO Consistency of the Adequate Mechanisms

Restriction on data transfer across borders strongly impacts services and service providers originating from Members that do not receive an adequacy status. Therefore, for such Members, their services and service suppliers may be put at a competitive disadvantage. Even so, the inconsistency of the adequacy mechanism with trade rules under the WTO, particularly the GATS, is uncertain. One of the biggest hurdles and the resulting uncertainty for a claim of violation of MFN principles under the GATS for the disparate treatment under data protection law based on adequacy decisions is to establish likeness between services and service suppliers originating from different Members with different statuses under the decisions.

Article II:1 of the GATS provides that for measures affecting trade in services, "each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country." The application of the MFN obligation does not require a specific commitment in a given service sector and requires non-discriminatory treatment to be

[36] *Schrems I*, ¶ 89.
[37] *Id.* ¶¶ 195-97.

afforded to "like services" and "like service suppliers." Therefore, it is an obligation applicable to all measures affecting trade in services.

The Appellate Body has held that the concept of "likeness" of services and service suppliers under Articles II:1 of the GATS is concerned with the competitive relationship of services and service suppliers.[38] The determination of likeness can only be made on a case-by-case basis, taking into account the specific circumstances of the particular case.[39] When analyzing likeness for services and service suppliers, the criteria for assessing "likeness" employed traditionally as analytical tools in the context of trade in goods, if relevant for assessing the competitive relationship of services and service suppliers, may also be employed, provided that they are adapted as appropriate to account for the specific characteristics of trade in services.[40] Accordingly, the Appellate Body noted that the characteristics of services and service suppliers or consumers' preferences in respect of services and service suppliers might be relevant for determining "likeness" under the GATS.[41] The Appellate Body stressed that the fundamental purpose of the comparison to determine "likeness" in the context of trade in services is to assess whether and to what extent the services and service suppliers at issue are in a competitive relationship.[42] The existence of a competitive relationship is a precondition for the subsequent analysis under the requirement of "treatment no less favourable" of whether the conditions of competition have been modified.[43]

Depending on how the service is provided, trade in services might be affected by a limitation on the transfer of personal data. Adequacy decisions under the GDPR determine whether personal data can be transferred to a specific country, which may affect the competitive conditions of services and service suppliers originating from different countries.[44] For example, for data storage services, a prohibition on the transfer of data to the country where the server of the service provider is located could arguably hinder its supply of services under Mode I. Competitive conditions between service suppliers located in countries with different adequacy status could be disrupted under the GDPR. In this regard, there are situations where adequacy decisions might violate MFN principles under Article II:1 of the GATS. Accordingly, a WTO

[38] Appellate Body Report, *Argentina – Measures Relating to Trade in Goods and Services*, ¶ 6.25, WTO Doc. WT/DS453/AB/R (adopted May 9, 2016) [hereinafter *Argentina – Financial Services* Appellate Body Report].
[39] *Id.* ¶ 6.26.
[40] *Id.* ¶ 6.31.
[41] *Id.* ¶ 6.32.
[42] *Id.* ¶ 6.34.
[43] *Id.*
[44] *See* Daniel Crosby, *supra* note 3, at 8.

Member who does not receive adequacy status might argue that its services or service suppliers are discriminated against vis-à-vis services or service suppliers originating from a jurisdiction where adequacy status has been granted. To deal with this claim, a panel would have to determine whether services and service suppliers originating from jurisdictions with different adequacy statuses are "like."

The mechanism of adequacy decision works similarly to the measures in the *Argentina – Financial Services* in that they distinguish different jurisdictions and provide differential treatment to services and service supplies based on the classification. Under the GDPR, whether the transfer of personal data to a particular jurisdiction is allowed depends on the adequacy status of the destination. In this context, the differential treatment between services and service suppliers is "due to origin" but is not "based exclusively on origin." Similarly, here, the classification of a country as adequacy or non-adequacy is not based on "origin *per se*" but on "the regulatory framework inextricably linked to such origin."[45] Accordingly, even though the mechanism of adequacy decisions distinguishes services and service suppliers based on their origin, the situations here do not support a presumption of likeness. A likeness analysis is still required. For the purpose of the article, we assume that nothing specific would undermine likeness between services or service providers in question other than the level of protection of personal data. Under the likeness analysis, it is the claimant that should demonstrate likeness between the services or service suppliers situated in countries belonging to different classifications despite various levels of protection for personal data. If the *prima facie* case was made, it is then for the respondent to demonstrate the lack of likeness between the services or service suppliers due to various levels of protection for personal data of their origins.

Identical services and service suppliers originating from different jurisdictions with various levels of protection for personal data could be unlike if the consumer preferences are indeed clear and strong enough due to this factor. However, this determination has to be made based on consumer preferences concerning the safety characteristics of the services or the service suppliers themselves. It should not simply be made based on whether the origin of the services or the service suppliers has received the adequacy decisions. Otherwise, a country could easily manipulate the status of the origin of the services or service suppliers to affect the outcome of the likeness analysis. In this regard, the adequacy decision is like a label that affects consumer preferences, the effect of which should be separated from the likeness analysis.

[45] Panel Report, *Argentina – Measures Relating to Trade in Goods and Services*, ¶ 7.166, WTO Doc. WT/DS453/R (adopted May 9, 2016) [hereinafter *Argentina – Financial Services* Panel Report].

Accordingly, the label that a Member puts on the origin of the services and service suppliers should not be considered as the factor for likeness determination.

Services and service suppliers from different jurisdictions could be like in every other regard, but different levels of protection could mean that the possibility for the occurrence of a breach of personal data can be different, and the remedies available against the breach can also be different. In this regard, if consumers consider this difference to be important, there is a possibility that it could render the services and service suppliers unlike. It is a difficult task for both the claimant and the respondent, and the allocation of the burden of proof would dictate the outcome of the case.

In addition, this analysis involves complex factual analysis, which was why the Panel in *Argentina – Financial Services*[46] tried to avoid this step,[47] which the Appellate Body reversed.[48] It is a difficult and time-consuming process that a panel is ill-suited to perform. A panel would need to determine the level of protection of personal data of the exporting countries involved and whether the difference is indeed so significant that it could render the services or service suppliers unlike. As noted, a panel tasked to compare services and service suppliers based on their respective level of protection should not simply rely on adequacy decisions made by the importing Member but may need to conduct its own process of adequacy decisions. However, WTO panels are not well suited to make such determinations.

Adequacy mechanisms create trade barriers and potential costs to adjudicating bodies of the WTO. As its inconsistency with the current rules under the WTO is not clear-cut, there is no sound basis to call for its abolishment. However, considering the costs to trade this mechanism creates for the free flow of data and international trade, its design should be carefully crafted to avoid unnecessary costs to trade. Indeed, if WTO adjudicating bodies consider that an adequacy mechanism violates obligations under the GATS, the measure can nonetheless be justified under Article XIV of the GATS. The obvious exception would be Article XIV:(c)(ii) which provides that a measure could be justified if it is "necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this

[46] *Id.*
[47] The Panel considered that the factual situation in the present case made it "extremely difficult" to undertake such likeness analysis when taking into consideration the factor regarding the possibility for Argentina to have access to the service suppliers' tax information.[47] Indeed, here, the Panel considered that "the current circumstances make it impossible" for it "to compare relevant services and service suppliers in order to evaluate relevant 'other factor(s)' in addition to their origin." *Id.* ¶ 7.184.
[48] Appellate Body Report, *Argentina – Measures Relating to Trade in Goods and Services*, ¶ 6.25, WTO Doc. WT/DS453/AB/R (adopted May 9, 2016) [hereinafter *Argentina – Financial Services* Appellate Body Report].

Agreement including those relating to . . . the protection of the privacy of individuals in relation to the processing and dissemination of personal data . . . .” In this case, the measure must pass the “necessity” test. Below this paper examines one of the redress requirements that may be questionable in light of the necessity test.

4. The Development in RTAs

In light of the limit of the GATS provision, facing difficulty in multilateral negotiations, some WTO Members seek to deal with the issue in regional trade agreements (RTAs). Through RTAs, some countries have established rules that provide direct regulation on restrictions on data transfer. RTAs such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[49] the United States-Mexico-Canada Agreement (USMCA),[50] and U.S.-Japan Digital Trade Agreement,[51] and the Digital Economy Partnership Agreement (DEPA)[52] has provided direction obligation that ensures cross-border data flow. Certainly, as the EU is not a party to these RTAs, GDPR is not subject to these rules. They are nonetheless an important indication that could influence the direction of future trade rules, such as the WTO electronic commerce negotiations under the Joint Statement Initiative on Electronic Commerce (JSI).[53] The negotiators of these FTAs do not choose to impose a non-discriminatory obligation on personal data protection regimes directly.[54] Recognizing the importance of cross-border data transfer in digital trade, these FTAs provide an obligation to ensure free cross-border data flow. A personal data protection law restricting cross-border data flow would then need to be justified under an exception that would require, among others, that the measure does not

[49] Article 14.11.2 of the CPTPP (providing that “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.”).
[50] Article 19.11.1 of the USMCA (providing that “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.”).
[51] Article 11.1 of the U.S.-Japan Digital Trade Agreement (providing that “Neither 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.”).
[52] Article 4.3.2 of the DEPA (providing that “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.”).
[53] WTO, Joint Statement on Electronic Commerce”, WT/L/1056 (25January2019).
[54] Article 14.8.3 of the CPTPP provides a soft approach on the non-discriminatory practices of personal information protection laws (providing that “Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.”). Similar provision can be found at Article 19.8.4 of the USMCA and Article 11.2.(a) of the U.S.-Japan Digital Trade Agreement. Article 4.2.4 of the DEPA provides a harder obligation by providing “Each Party shall adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.” The point of these rules are encouragement or requirement for parties to provide protection for users of electronic commerce and do not, at least not explicitly, impose non-discriminatory obligations on cross-border data transfer.

constitute discrimination. The difference from the GATS here is that there is no need to prove likeness and discrimination in the first place.[55] Therefore, this approach that ensures the free flow of data that is justifiable by a non-discriminatory requirement is a correct approach that would ensure a non-discriminatory personal data protection regime.

Article 14.11.3(a) of the CPTPP, for example, provides that "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 . . . is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade . . . ." The exceptions to the cross-border data flow are modeled to the chapeau of the general exceptions under GATT and GATS. Under the current interpretation of these provisions under the WTO, which an interpretation of the FTA provisions could seek guidance from,[56] these exceptions that are currently provided under the FTAs, together with a prohibition to restrict cross-border data flow, are sufficient to ensure the personal data protection regimes would be consistent with the MFN principle. The Appellate Body has held that whether a measure is applied in a particular manner "can most often be discerned from the design, the architecture, and the revealing structure of a measure."[57] This review of the design, the architecture, and revealing the structure of a measure to determine whether its actual or expected application would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail would involve "a consideration of "both substantive and procedural requirements" under the measure at issue.[58]

In addition to the obligation of non-discrimination, the provision requires that the measure at issue should "achieve a legitimate public policy objective." This is arguably a lower threshold than the necessity test under the general exception under the GATS. Nonetheless, it provides an important element when determining the consistency of the personal data protection law with the trade rules—the law must be able to achieve their stated objectives.

---

[55] *See* Article 14.11.3(a) of the CPTPP (providing that "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 . . . is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade . . . ."). For similar provisions see also Article 19.11.2(a) of the USMCA and Article 4.3.3 of the DEPA.

[56] Shin-yi Peng & Han-wei Liu, *The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?*, 51 J. WORLD TRADE 2, 21 (2017).

[57] Appellate Body Report, European Communities – Measures Prohibiting the Importation and Marketing of Seal Products, ¶ 5.302, WTO Doc. WT/DS400/AB/R / WT/DS401/AB/R (adopted on June 18, 2014) [hereinafter *EC – Seal Products* Appellate Body Report].

[58] *Id.*

5. Data Disputes Regarding Third Countries

Personal protection laws such as GDPR guarantees the protection of personal data. Data subjects have various rights concerning their personal data, including the right to the informed,[59] right to access,[60] right to rectification,[61] right to erasure,[62] right to restriction of processing,[63] right to data portability,[64] right to object,[65] and rights related to automated decision-making and profiling.[66] In light of the digital age and "datafication" of transactions, data disputes will become more widespread and prevalent, once more countries adopt GDPR-type personal data protection laws and people are more educated about their data-related rights. Such disputes are complicated and require special knowledge about the data platforms or the relevant data system to participate in dispute resolution.[67]

As many of the critical rights of data subjects are not absolute, the exercise of the rights is often subject to complex balancing acts with other rights recognized in the EU. For example, in *Google Inc. v. AEPD*, the CJEU ruled that each request for erasure needs a case-by-case assessment to balance the fundamental rights to personal data protection and private life of the data subject and the legitimate interests of all internet users.[68] The other rights and legitimate interests may include freedom of expression, right to access to documents, professional secrecy, freedom of religion and belief, freedom of arts and science, protection of IP, and economic interests.[69] The nature of the data disputes arising from personal data protection law indicates that both the complexity and the potential volume of such disputes will require a unique design and structure of the dispute resolution mechanism. Therefore, Werra called for adopting a Global ADR Mechanism to address the challenges of "massive online micro-justice."[70]

The issue became more acute regarding redress mechanisms in third countries. The basic structure of the adequacy approach is that the third country should provide the

[59] GDPR, Art. 12.
[60] GDPR, Art. 15(1).
[61] GDPR, Art. 16.
[62] GDPR, Art. 17(1).
[63] GDPR, Art. 18(1), 19.
[64] GDPR, Art. 20.
[65] GDPR, Art. 21(1).
[66] GDPR, Art. 22, 21, 13(2)(f).
[67] JEF AUSLOSS, THE RIGHT TO ERASURE IN EU DATA PROTECTION LAW, 426-27.
[68] CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014, ¶¶. 81-83.
[69] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW, 52-53 (2018).
[70] Jacques de Werra, *Alternative Dispute Resolution in Cyberspace: The Need to Adopt Global ADR Mechanisms for Addressing the Challenges of Massive Online Micro-Justice*, in SWISS REVIEW OF INTERNATIONAL AND EUROPEAN LAW 289 (2016).

administrative and judicial redress mechanism, as discussed above. While it may seem plausible on paper, the redress mechanism of third countries may not actually provide an adequate level of protection for transferred personal data. Even if a third country provides both substantive and procedural protection regarding personal data that is similar to that of GDPR, the level of protection afforded to data subjects in the EU may not be substantially equivalent to the GDPR. For example, if personal data is transferred to Japan, any remedies will have to be provided by the Japanese administrative authority and/or Japanese courts. Considering the language barriers and associated costs for such redress, it is difficult to claim that the redress through Japanese data protection rules would be equivalent to those available under the GDPR. In addition, as the personal data dispute often involves a complex balancing between fundamental rights, the differences in these rights between jurisdictions in actual disputes could lead to various levels of protection for personal data. An adequate level of protection cannot be fully expected in disputes resolved in third countries.

This flaw in the adequacy mechanism is critical as it raises questions about the basis of the adequacy approach. It is especially problematic from the trade law perspective, as it calls into question the non-discrimination and necessity aspect of the GDPR. If one of the critical elements of the adequacy determination does not guarantee adequate protection, the legitimacy of the personal data protection law will suffer with respect to its consistency with relevant trade rules. Uncertainty and dispute would ensue.

6. Concluding Remarks — Need for the Development of ADR for Personal Data Disputes

The flaw discussed in the previous section could be addressed with arbitration and ADR mechanisms. This paper calls for a distinct redress mechanism that is independent of the redress mechanism from third countries in adequacy determinations. A relevant mechanism is the arbitration system established under Privacy Shield System.[71] While this arbitration system does not provide its function as expected due to the invalidity of the system, the idea of the utilization of arbitration for personal data disputes should be considered.[72] Such a mechanism should be binding and user-friendly, providing adequate protection for data subjects from different jurisdictions.

[71] U.S. Dep't of Commerce, E.U.-U.S. Privacy Shield Framework Principles, Annex I (Introduction), https://www.privacyshield.gov/article?id=ANNEX-I-introduction.
[72] Jacques de Werra, *Using Arbitration and ADR for Disputes About Personal and Non-Personal Data: What Lessons from Recent Development in Europe?* 30(2) AM. REV. INT'L ARB. 195, 205-07 (2019).

As this mechanism can be independent of the jurisdiction of the third country to which the data is transferred, the impact of the laws in third countries, both personal data protection laws and laws protecting other balancing rights, could be reduced. A well-functioning ADR that replaces the redress mechanism under the current adequacy approach could ultimately reduce or even remove the need to require adequacy in substantive personal protection law. This would further the objectives of non-discrimination and reduces the unnecessary burden on international trade.