Adequacy decisions: an opportunity for regulatory cooperation on data protection?*

Maarja Saluste (EUI)

January 18, 2021

Abstract

The European Union (EU) regulates cross-border movement of personal data generated by 447 million Europeans through several instruments, including the General Data Protection Regulation (GDPR). Companies processing or with access to personal data originating in the EU must comply with EU regulation or confront fines. For third countries, the most comprehensive and inclusive way to protect and support their businesses and their government is through negotiating an adequacy decision (Article 45 GDPR) with the EU. This paper analyses the adequacy decision framework as a form of cooperation on regulation of cross-border data flows, focusing on three cases: Australia, New Zealand and Japan. Australia was denied adequacy, while New Zealand obtained adequacy status under Directive 95/46, the predecessor to the GDPR. Japan to date is the only example of a positive adequacy decision taken under the GDPR. The analysis of the EU's determinations of adequacy and the assessment procedures used reveal an absence of transparency and lack of clarity in the processes and criteria applied. Several adjustments in this cooperation model are suggested to provide fair and equal grounds for adequacy decisions, and to bring EU practice into compliance with commitments under the World Trade Organization (WTO).

* The preparation of this research was supported by the European Union's Horizon 2020 research and innovation program under grant agreement 770680 (RESPECT). I am grateful to Bernard Hoekman for suggestions on earlier drafts.

Introduction

European Union (EU) regulation of cross-border data flows distinguishes between personal and non-personal data. The latter is unconstrained as a result of the Regulation on the free flow of non-personal data, which permits data generated by machines to move from one territory to another without restrictions.[1] Cross-border flows of personal data are regulated by several legal instruments, notably the General Data Protection Regulation (GDPR).[2] The GDPR applies to data produced by 447.7 million European individuals,[3] both online and offline. Adopted in 2018, the GDPR is considered both as ground-breaking for its coverage[4] and limiting for its restrictive impact on the movement of data flows.[5]

Access and the right to process data is an essential asset for countries and companies. In a globalized economy, data needs to 'cross' borders. Under the EU law, cross-border data flows are regulated through different transfer mechanisms. An adequacy decision by the EU gives the highest threshold of advantages for data processing.[6] Such decisions grant a 'third country, a territory or one or more specified sectors within the third country, or international organisations' the rights to transfer 'personal data which are undergoing or are intended for processing after the transfer to a third country or to an international organisation'.[7] Adequacy decisions regulated under Art. 45 of the GDPR, and previously Art. 25 of the Directive 95/46 on the processing of Personal Data (Directive)[8], are a form of regulatory cooperation in personal data protection. The EU has had this framework in place for the safe movement of data from the EU to any other third country since 1995. To date, fifteen countries have applied for an adequacy decision.

International cooperation on data protection is taking off through bilateral and plurilateral agreements to enhance safe and trustworthy movement of data to permit access to data. Examples include the Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore,[9] the Australia-

---

[1] Restrictions apply when personal and non-personal data are mixed, then data must be treated as personal data. See Articles 2(2) and 8(3) of the FDI. Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union. COM/2019/250 final, 29.5.2019.

[2] 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 Data Protection Regulation). ELI: http://data.europa.eu/eli/reg/2016/679/oj.

[3] Eurostat, 10 July 2020. Available at: https://ec.europa.eu/eurostat/documents/2995521/11081093/3-10072020-AP-EN.pdf/d2f799bf-4412-05cc-a357-7b49b93615f1:~:text=On%201%20January%202020%2C%20the,States%20on%201%20January%202019.

[4] Aaronson, S.A., Leblond, P. Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. JIEL, 2018.

[5] Meltzer, J.P., Mattoo, A. International Data Flows and Privacy: The Conflict and Its Resolution. Journal of International Economic Law, Volume 21, Issue 4, pp. 769–789, 2018.

[6] Compare Arts. 45-50 GDPR.

[7] See Arts. 44 and 45 GDPR first sentence.

[8] 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. ELI: http://data.europa.eu/eli/dir/1995/46/oj.

[9] Chile, New Zealand and Singapore DEPA (signed June 2020). Available at: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement/. Canada announced December 17, 2020 its interest to join DEPA. See: https://www.beehive.govt.nz/release/canadian-interest-digital-economy-partnership-agreement-welcomed.

Singapore Digital Economy Agreement (DEA),[10] and the Japan-US Agreement on Digital Trade.[11] This paper analyses the adequacy decisions framework, the associated assessment criteria and procedural elements to understand whether this approach could be considered as a best practice in international cooperation in data protection.

The focus of the available literature on adequacy decisions mostly has been on the EU-US case, especially the EU-US Safe Harbour and Privacy Shield, as these data flow frameworks have been challenged before the Court of Justice of the European Union (CJEU).[12] In July 2020, the CJEU invalidated the latest adequacy decision, EU-US Privacy Shield, in its ruling on *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*.[13] Studies have also begun to examine the adequacy decision for Japan, the first decision taken under the GDPR.[14] The literature has centered on specific cases. The overall legal and governance framework for adequacy decisions has not been addressed.

The shift from Directive 95/46 to the GDPR raises the question whether the adequacy decisions that have been negotiated before the GDPR came into force should be renegotiated. Questions have already been raised whether the Japanese privacy protection is at the same level as the personal data protection in the

[10] Australia and Singapore (signed December 2020). See https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement.

[11] The agreement bans data localization, barriers to cross-border data flows and conditioning access to the market on transfer of source code or algorithms, and covers financial services (signed October 2019). See: https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

[12] See for example: Shaffer, G. Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards. Yale Journal of International Law, 25(1), 1-88, 2000; Greer, D. Tomorrow's Privacy. Safe Harbor – a framework that works. International Data Privacy Law. Vol. 1. No.3. 2011; Schwartz, P. M. The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. 126(7) Harv. L. Rev. 1966, 2013; Linn, E. A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement. Vanderbilt Journal of Transnational Law, 50(5), 1311-1358, 2017. Puccio, L., Monteleone, S. From Safe Harbour to Privacy Shield. Advances and shortcomings of the new EU-US data transfer rules. EPRS, 2017. The previous agreement with US was called the Safe Harbour Agreement that came into force 26 July 2000. However, it has been invalidated in the *Schrems* v. *Ireland*. The new Privacy Field Framework came into force 12 July 2016. C-362/14 *Maximillian Schrems* v. *Data Protection Commissioner, Joined Party Digital Rights Ireland Ltd.*, ECLI:EU:C:2015:650. Weber, R.H. Free flow of data and digital trade from an EU perspective in Ed. Peng, S. *et al*. (Eds.) Governing Science and Technology under the International Economic Order. Regulatory Divergence and Convergence in the Age of Megaregionals. Edward Elgar Publishing, 2018, p. i52. Several cases have been taken to the CJEU that were about the EU-US privacy matters. C-131/12 *Google Spain SL, Google Inc.* v. *Agencia Española de Protección de Datos (es), Mario Costeja González*, ECLI:EU:C:2014:317. T-670/16 *Digital Rights Ireland v Commission*, ECLI:EU:T:2017:838. Kuner, C. *et al*. (eds.) The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020.

[13] Case C-311/18 *Data Protection Commissioner* v *Facebook Ireland and Maximillian Schrems*. Judgement of 16 July 2020, ECLI:EU:C:2020:559.

[14] Greenleaf, G. Japan: EU Adequacy Discounted. 155 Privacy Laws & Business International Report 8-10; UNSW Law Research Paper No. 19-5, 2018. Greenleaf, G. Japan and Korea: Different Paths to EU Adequacy. 156 Privacy Laws & Business International Report, 9-11, 2018. Miadzvetskaya, Y. What are the pros and cons of the Adequacy decision on Japan? KU Leuven. Centre for IT & IP Law. Available at: https://www.law.kuleuven.be/citip/blog/what-are-the-pros-and-cons-of-the-adequacy-decision-on-japan/.

EU[15] and the previous Directive does not have the same threshold as the GDPR. Greenleaf argues that Art. 45 of the GDPR "explicitly requires 'effective and enforceable data subject rights' and 'effective judicial and administrative redress' and notes that these points are ignored in the adequacy decision for Japan.[16]

This paper analyses the legal texts and relevant documents linked to adequacy decisions to understand the assessment and process for the application of an adequacy decision. It is organized as follows. Section 1 gives an overview on the overall EU data protection framework for cross-border data flows. It highlights the extensive nature and importance of the liberties associated with obtaining an adequacy decision given to third countries compared to non-EU companies that need to seek compliance with the GDPR themselves. Section 2 examines the assessment and procedural elements of the cooperation between the EU and third countries. It focuses on available information on the evaluation of equivalency of the data protection regime in opinions pertaining to the adequacy of data regimes in Australia, New Zealand and Japan. Section 3 discusses the compatibility of the data adequacy decisions with the EU's international legal commitments in the General Agreement of Trade in Services (GATS). It argues that the EU could be challenged under the GATS by World Trade Organization (WTO) members, and briefly makes a case for the EU to consider using an open plurilateral agreement as a framework to address concerns regarding the potential discriminatory nature of data adequacy decisions. Section 4 concludes.

1. EU´s legislative framework for cross-border movement of personal data

Since 1995, the EU has implemented privacy rules on the movement of personal data across EU members states. First through Directive 95/46 on the processing of Personal Data (Directive) and since 2018 through the comprehensive General Data Protection Regulation (GDPR).[17] However, the Directive in the past and now the GDPR also have an extraterritorial outreach: determining how personal data that belong to EU citizens should be treated not only within the EU, but also when they move outside of its borders.

For the movement of data, third countries, companies based in those countries, and international organizations must meet GDPR criteria to show that the transborder data flows are and will remain secured.[18] Chapter 5 (Arts. 44-50) of the GDPR covers cases where personal data of EU citizens, that are undergoing processing or will be processed or stored, move out from the EU to a third country or to an international organization.[19] Arts. 44-50 of the GDPR set up three different means to ensure that data are moving safely. Transfers of personal data outside of the EU can be made either based on (1) an adequacy decision[20], (2) appropriate safeguards, like standard contractual clauses (SCCs), binding corporate rules (BCRs) etc.[21] or (3) derogations[22].

---

[15] Miadzvetskaya, Y. What are the pros and cons of the Adequacy decision on Japan? KU Leuven, CiTiP, 4 April 2019. Available at: https://www.law.kuleuven.be/citip/blog/what-are-the-pros-and-cons-of-the-adequacy-decision-on-japan/.

[16] Greenleaf, G. Japan: EU Adequacy Discounted. 155 Privacy Laws & Business International Report 8-10; UNSW Law Research Paper No. 19-5, 2018, p. 8.

[17] The GDPR came into force May 24, 2018. Data protection in the EU. European Commission. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.
A Directive: does not have a direct effect in an EU member state, but the EU member states has to incorporate the rules into their legislation. Regulation: was adopted that is directly applicable to all EU member states.

[18] Art. 44 of the GDPR.

[19] The movement of data that "crosses borders" is often referred to as cross-border data flows.

[20] Art. 45 of the GDPR.

[21] Art. 46 of the GDPR. SCCs and BCRs are the most frequently used appropriate safeguards in practice.

[22] Art. 47 of the GDPR.

These conditions for transfer are supposed to provide a high threshold of certainty for smooth, efficient, and safe movement of data.[23] SCCs are tailor-made standards by the European Commission (Commission) for companies based in third countries who can use a set of rules in their contracts to make sure that they and their business partners would follow the SCCs data protection standards in order to process any personal data that are from the EU.[24] The BCRs are for groups of companies that can set up BCRs among themselves to make sure that the data from the EU are protected. The application of BCRs has not taken off extensively in practice.[25] This could be because these rules are newer[26], they were not specifically mentioned in the Directive, however, the Data Protection Authorities (DPAs) recognized them. What could also be an obstacle in practice is that it takes time to build a strong legal foundation between companies and by the time the rules have been agreed upon, there might already be changes in the cooperation. Therefore, adopting SCCs provides more predictability in long term. However, SCCs and BCRs only apply to those companies that pursue to adopt these rules. The third mean to be compatible with the GDPR is for third countries[27] or international organizations to negotiate an adequacy decision.[28] The SCCs or BCRs create protection that an adequacy decision will automatically cover once it has come into force.[29]

The companies face less burden as there is an authority in the third country standing out for their interests, it is less costly for them as they do not need to negotiate or renegotiate contractual clauses with their business partners to comply with the GDPR. Contractual bases in data exchange are volatile as the sources and technological means are constantly changing.[30] Renegotiating contracts is costly, lengthy, and possibly with certain trade-offs. For example, company *Looq* specialized in data processing collects data from around 500 different companies that also have data on some EU citizens. *Looq* was already operating before the GDPR came into force and is not based in a country having an adequacy decision. Hence, *Looq* has to renegotiate all their 500 contracts on collection of data as the privacy protection clauses need to be updated in the contracts to be compatible with the GDPR. Company *Bel* was also operating before the GDPR came into force, however, *Bel* is based in a country that has an adequacy decision with the Commission and does not have to make any updates in their contracts. Also, it does not have to renegotiate terms for onward transfers[31] outside of the country if the companies outside follow the

[23] Voigt, P., von dem Bussche, A. The EU General Data Protection Regulation (GDPR): Practical Guide. Springer, 2017, p. 116.

[24] Art. 46 does not only apply to companies, but also public authorities. However, the text will just make a reference to business corporations.

[25] Voigt, P., von dem Bussche, A. The EU General Data Protection Regulation (GDPR): Practical Guide. Springer, 2017, p. 127.

[26] The GDPR came into force May 25, 2018.

[27] Or just a territory or one or more specified sectors within that third country.

[28] Art. 45 GDPR.

[29] Fuster, G. Un-mapping personal data transfers. European Data Protection Law Review (EDPL), 2(2), 2016, p.163. There is also a 'three-tier structure' in place for the 'legal bases for data transfers'. If there is an adequacy decision in place, then 'that should be relied on' and not SCCs or BCRs. Derogations come last as a legal basis if other forms exist. Kuner, C. *et al.* (eds.) The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020, pp. 764-765.

[30] Adele Barzeley's comment on Chapter 6 of the World Development Report 2021: Data policies, laws and regulations. She is a Governance Analyst at the World Bank and one of the co-authors of this Chapter. World Development Report 2021 Seminar Series, December 7, 2020.

[31] See recital 101, Arts. 44, 45(2)(a) and 47(2)(d) GDPR on the protection of onward transfers.

requirements of the GDPR. However, the Commission has not conducted any assessments about the safety of onward transfers in practice. An adequacy decision should correspond to the highest level of certainty to make sure that there would be no violation of privacy also with onward transfers.[32]

The Commission has the right to recognize third countries or international organizations that are considered having an adequate level of data protection with an adequacy decision and, therefore, being subject to the transfer of personal data according to Art. 45 of the GDPR.[33] The assessment to obtain an adequacy decision is based on an extensive list of elements to determine whether there is an essentially equivalent level of protection.[34] According to Art. 45(2), The Commission conducts a thorough analysis of the applicable domestic laws in the third country that the companies operating in that country are already subject to; and evaluates what has to be improved in the third country's legislation to secure a safe movement of data that would correspond to EU's privacy standards. This process should create the highest level of protection based on negotiations between two countries through the comparison of their legislations. An adequacy decision gives the highest threshold of advantages for data processing.[35] If a third country obtains an adequacy decision, then the companies within that country do not need specific authorization for data transfers and, therefore, not needing to adopt SCCs or BCRs. It gives companies an advantage in front of other companies that cannot benefit from an adequacy decision. The supervisory authority of the third country does not have to be involved in this process anymore neither.[36] This eliminates another element for the stakeholders in the third country to carefully follow. Thus, granting an adequacy decision should pass a rigorous and objective control of privacy measures in the country that negotiates an adequacy decision.

2. Cooperation between the EU and third countries on safe movement of personal data

2.1. Applications for adequacy

There are 13 countries that have successfully negotiated an adequacy decision with the EU: Andorra, Argentina, Canada[37], Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and United States of America (US).[38] The Commission has granted these countries, or specific sectors in those countries, like commercial organizations in Canada, access to EU personal data without further contractual constraints as discussed above.

---

[32] Art. 45(2) of the GDPR does refer to the importance of checking the regulation for onward transfers.

[33] Art. 45(1) GDPR. International organisations were added to Art.45 GDPR. The Directive only referred to third countries. So far, no international organisation has sought to start a negotiation of an adequacy decision. Therefore, as practice in the adequacy decisions framework mainly covers third countries and in few cases specific sectors in third countries, I will, henceforth, refer to third countries.

[34] Art. 45(2) of the GDPR.

[35] Compare Art. 45-50 GDPR.

[36] Voigt, P., von dem Bussche, A. The EU General Data Protection Regulation (GDPR): Practical Guide. Springer, 2017, p. 117. Kuner. C.: However, in *Schrems I*, "the CJEU said that DPAs have to bring an action if they find that data transfers are no longer receiving adequate protection[.]"

[37] The scope of the adequacy decision between the EU and Canada is narrower. It only grants the rights provided under the adequacy decision to commercial organizations in Canada.

[38] Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. European Commission. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Adequacy decisions have existed since 1995 under the GDPR predecessor, the Directive 95/46 on the processing of Personal Data. US and Switzerland were the two first countries to receive an adequacy decision. In total 15 decisions with third countries[39] were adopted under the Directive, 11 of them still in force. This shows that one country has been subject to more than one decision covering different areas of personal data protection. The adequacy decision given to Canada on the transfer of Passenger Name Record data of air passengers expired in 2009.[40] The US has received in total three adequacy decisions, which have all been invalidated by the Court of Justice of the European Union (CJEU) one after another depending on when the case was filed. The latest adequacy framework between the EU and US enforced in 2016, Privacy Shield, was invalidated in July 2020.[41] The two other US' decisions adopted under Art. 25 of the Directive in 2004 and in 2000 were respectively invalidated by CJEU in 2006[42] and in 2015[43]. As the GDPR became fully applicable on 15 May 2018, Japan is the only country that has received an adequacy decision under the GDPR.[44] In total, 15 different countries have had adequacy talks with the Commission. Hence, based on the above, 2 countries: Australia and the Principality of Monaco did not receive the implementing acts from the Commission. Both countries received an opinion from the relevant EU body on their data protection regulations according to Art. 30 of the Directive (the Working Party). In the case of Australia, the Working Party adopted two opinions on two separate adequacy decisions. In the first opinion from 2000, with a direct applicability to all stakeholders having access to EU personal data, the Working Party did not find adequacy. In the second opinion from 2004, the Working Party stated that Australia does provide adequate level of protection for the transmissions of passenger name record data.[45] Opinion on Monaco's data protection adequacy was adopted in 2012. The Working Party found that Monaco should also receive an adequacy decision.[46] However, the Commission did not adopt an implementing act after these two positive opinions given by the Working Party.

[39] With Canada two decisions and with the US three decisions. Rest of the countries have received one adequacy decision. See Table 1 below.

[40] This decision explicitly set a term of 3.5 years for its applicability. With regards to other adequacy decisions, this has not been the practice. 2006/253/EC: Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency (notified under document number C(2005) 3248). See 'Review and termination of commitments'.

[41] Case C-311/18 *Data Protection Commissioner* v *Facebook Ireland and Maximillian Schrems*. Judgement of 16 July 2020, ECLI:EU:C:2020:559.

[42] The Decision 2004/535 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection. Joined Cases C-317/04 and C-318/04 *Parliament v Council and Commission*. Judgement of 30 May 2006, ECLI:EU:C:2006:346.

[43] The decision from 2000 on the EU–US Safe Harbour. Case C-362/14, Maximilian *Schrems v. Data Protection Commissioner*. Judgement of 6 October 2015, ECLI:EU:C:2015:650.

[44] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information. Available at: 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.

[45] Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000. Article 29 Data Protection Working Party. 5095/00/EN, WP40 final; and Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines. Article 29 Data Protection Working Party. 10031/03/EN, WP85.

[46] Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco. Article 29 Data Protection Working Party. 01446/12/EN, WP198.

Besides the unadopted and adopted decisions, there are also on-going negotiations with South Korea and with India. Talks with India have not been officially announced. Table 1 below provides an overview of the different adequacy decisions and their status.

Table 1. Overview and status of the adequacy decisions

ADEQUACY DECISIONS							
Legal framework	Art. 25 of the Directive					Art. 45 of the GDPR	
Scope	Applicable to all stakeholders in the country		For commercial organizations	On Passenger Name Record Data from Airlines		Applicable to all stakeholders in the country	Unknown
Adoption of the implementing act	Adopted by the Commission:	**The Commission did not adopt an impl. act:**	Adopted by the Commission:	Adopted by the Commission:	**The Commission did not adopt an impl. act:**	Adopted by the Commission:	On-going talks
Recipient country/ countries	Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, US[47] (two decisions, both invalidated by the CJEU)	Australia, Principality of Monaco	Canada	Canada (expired), US (invalidated by the CJEU)	Australia	Japan	South Korea, India (has not been publicly announced)

[47] The Safe Harbor and EU-US Privacy Shield framework functioned through a self-regulatory framework which is different than other adequacy decisions. Greer, D. Tomorrow's Privacy. Safe Harbor – a framework that works. International Data Privacy Law. Vol. 1. No.3. 2011, p. 143. See also: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2462. Weber described the nature of the EU-US Privacy Shield more as a bilateral agreement, however, in practice it is treated as an adequacy decision. Weber, R.H. Free flow of data and digital trade from an EU perspective in Ed. Peng, S. *et al*. (Eds.) Governing Science and Technology under the International Economic Order. Regulatory Divergence and Convergence in the Age of Megaregionals. Edward Elgar Publishing, 2018, p. 56.

2.2. The assessment procedure for adequacy decisions

All the legal bases for international data transfers outside of EU's territory go through the assessment of the relevant GDPR provisions (Arts. 44-50), to ensure the personal data of EU citizens would receive the same protection abroad as they are supposed to receive within the EU. With regards to appropriate safeguards and derogations (Arts. 46-50), the controller or processors of personal data from the EU can consult the supervisory authority of an EU member state or the Commission on how to set up these measures to provide the necessary level of protection to be in compliance with the GDPR.

Adequacy decision proceedings are linked to the Commission based on Arts. 45(3) and 'in accordance with the examination procedure' in Art. 93(2) GDPR, previously Art. 25 of the Directive. Neither the article on adequacy decisions nor the Commission's website indicate what is the exact application procedure for third countries and international organizations, how the negotiations are held and how the Commission conducts the analysis on the practices and legislation before it gives an overview to the relevant EU body that adopts an opinion before the Commission moves forward with the implementing act for the adequacy decision. Art. 45 GDPR allows the Commission to hold adequacy decision negotiations either with third countries or international organizations. According to Kuner, the third countries 'typically' approach the Commission to seek for an adequacy decision.[48]

The EU provided the following answer to a question by India at the WTO as part of the 2004 Trade Policy Review of the EU:

> "As regards the procedure to be followed for an adequacy finding, the Commission, upon request of the third country and in close co-operation with the Working Party 29 (composed of the EU Member States' independent data protection commissioners and established under Article 29 of the data protection Directive) and the Member States, will assess the level of protection in the third country in question and, in case this level is adequate, will decide so."[49]

Here, the EU confirms that the third country needs to contact the Commission and the Commission work together with the Working Party. There is no information available whether the Commission itself addresses third countries to start talks under Art. 45 GDPR. However, it is plausible that the Commission could present the adequacy framework in other discussions, like a negotiation of a free trade agreement, especially based on the Communication that the Commission published in 2017. That gives a broad list on what the Commission assesses when deciding with which third countries to pursue talks on adequacy. It refers to 'the existence of a free trade agreement or ongoing negotiations[.]'.[50]

The Commission has the decision-making power on the adequacy of a data protection regime.[51] Before it adopts an implementing act or decides not to, there is an equivalency analysis conducted by a body that comprises of one representative from each EU member state. Under Art. 29 of the Directive, this body existed as the 'Working Party on the Protection of Individuals with regard to the Processing of Personal

[48] Kuner 2020, p. 785.
[49] Trade Policy Review: European Communities. Minutes of Meeting. Trade Policy Review Body, 25 and 27 October 2004, WTO. WT/TPR/M/136/Add.2, p. 29.
[50] Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World. Brussels, 10.1.2017, COM(2017) 7 final, p. 8.
[51] Arts. 45(3) and 93(2) GDPR. Recital 103 GDPR.

Data' (Working Party). According to Art. 30 of the Directive, the Working Party "[gives] the Commission an opinion on the level of protection in the Community and in third countries". Under the GDPR, the Working Party has been by the European Data Protection Board (EDPB).[52] The tasks of the EDPB with regards to adequacy decisions have not changed. According to Art. 70(s), the EDPB shall "provide the Commission with an opinion for the assessment of the adequacy of the level of protection in the third country or international organisation[.]"

The EDPB's work is divided into sub-groups that address different aspects of the GDPR. One of the sub-groups deals specifically with cross-border data flows regulated under Arts. 44-50. When the Commission wants to move forward on the adequacy decision to complete the assessment on the third country's data protection legislation and its equivalence to the GDPR, the Commission consults the EDPB to set up a special task force under the Commission, which is created separately when an opinion on the adequacy of a third country's data protection laws is under evaluation (or to conduct a review of an adequacy decision). The GDPR does not state that the Commission is obliged to ask for an opinion from the EDPB. Recital 105 of the GDPR states that "the Commission *should* consult the Board when assessing the level of protection /…/" (emphasis added).[53] It has not been documented that the Commission has acted otherwise.

For the EDPB to provide an 'opinion for the assessment of the adequacy of the level of protection'[54], the Commission addresses the EDPB to appoint three national experts for the task force that will examine all the available information gathered by the Commission and conduct a legal analysis on the adequacy. The EDPB is legally obliged to provide and forward an opinion to the Commission.[55] Based on that the Commission can adopt the implementing act of the adequacy decision. The opinion given by the WP/EDPB and the implementing act are the only two publicly available documents from the procedure of a third country's application for an adequacy decision. The implementing act is the legal act enforcing the adequacy decision given to a third country and provides the information on the necessary legal requirements established under Art. 45 GDPR. The only available source to assess how the adequacy decision's analysis is conducted is, however, the opinion provided by the WP/EDPB. Art. 70(3) GDPR sets a clear requirement for the EDPB to make 'its opinions, guidelines, recommendations, and best practices to the Commission' publicly available. The Commission provided the WP and now the EDPB with the relevant information for the WP/EDPB to write an opinion. The opinions show that the Commission asks for additional research on the data protection law evaluations. They do not make this information accessible to the public even though the studies are academic[56] and should be neutral. Therefore, the only way to understand what those studies evaluated is when the Working Party/EDPB is directly referring to them.

Even though the WP/EDPB is supposed to conduct a comprehensive analysis on the equivalency of the data protection in the third country and examines the relevant documents and studies to adopt an

[52] Art. 68 GDPR.

[53] This cited sentence from recital 105 is also linked to recitals 103 and 104 GDPR.

[54] Art. 70.1(s) GDPR.

[55] According to Art. 70.1(s) and 70(3) GDPR. Under the Directive, see Art. 30.

[56] Kuner 2020, p. 785. See for example: Opinion 11/2011 on the level of protection of personal data in New Zealand. Article 29 Data Protection Working Party. 00665/11/EN, WP182, 4 April 2011.

opinion, the Commission is not bound by it.[57] Therefore, the Commission can still adopt an implementing act even if the WP/EDPB has not found adequacy or its opinion gives recommendations to make changes in the third country's legislation to be compatible with the level of data protection of the GDPR. It has happened twice that the Commission did not follow a positive opinion: (1) Australia's protection of passenger data and (2) Monaco's overall personal data protection legislation. In 2004, the Working Party adopted an opinion on 'the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines', finding that Australia provides adequate protection to this set of data that would be subject to the adequacy decision.[58] An adequacy decision was not given to Australia. The Commission and Australia signed an agreement on the same matter in 2012.[59] The agreement from 2012 is not an adequacy decision and to conclude the discussions it took more than eight years. The second example of a difference between the WP's opinion and the Commission's decision-making power is from 2012 when the Working Party found the data protection regulation in the Principality of Monaco equivalent to EU's data protection regulation.[60] The Commission did not take any further actions on the opinion on Monaco and no adequacy decision was adopted. Why the Commission did not follow the recommendation adopted by the WP is unknown.

Under the Directive, there is also one case where the Working Party did not find a country's data protection regulation adequate and gave recommendations how to reach that level of protection. In 2001, the Working Party gave an opinion on Australia's legislation. It listed the elements that Australia should consider changing and updating to reach the equivalent level of personal data protection as in the Directive. However, there was no public reporting on what occurred or was discussed between Australia and the Commission after the Working Party released this opinion. The Commission has not released an implementing act. With regards to the first adequacy decision taken under the GDPR, the EDPB found in 2018 that certain changes had to be made in the data protection regulation in Japan to grant adequacy.[61] However, the Commission did not follow this recommendation by the EDPB and moved forward with the proceedings to affirm adequacy.

There is no official statement that the Commission would have to release that would explain why the Commission did not follow the opinion of the WP/EDPB or why the third country does not have to make the changes that the WP/EDPB found necessary to meet the level of personal data protection of the GDPR. Scholars working in this field have pointed to the political nature of the procedure for adequacy decisions. Kuner notes the extensive length of the discussions and argues negotiations "become entangled in political factors" like in the case where Ireland delayed the adequacy decision of Israel due to political

[57] There has never been a ruling on the relationship between the EDPB and the Commission in the cases the Commission decides to take a different approach than suggest by the WP/EDPB.

[58] Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines, p. 13.

[59] Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service. CELEX number: 22012A0714(01). OJ L 186, 14.7.2012.

[60] Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco. Article 29 Data Protection Working Party. 01446/12/EN, WP198, p. 19.

[61] Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan. Opinion of the Board (Art. 70.1.s) adopted on 5 December 2018. Kuner 2020, p. 785 fn.91.. See also Greenleaf, G. Japan: EU Adequacy Discounted. 155 Privacy Laws & Business International Report 8-10; UNSW Law Research Paper No. 19-5, 2018.

reasons.[62] Stoddart, Chan and Joly describe tensions with Quebec, Canada in the adequacy decision negotiations and its length.[63] Greenleaf argues that New Zealand received an adequacy decision due to the "size and nature of its economy".[64] The Commission itself has referred to the political nature of its framework on adequacy findings in its Communication "Exchanging and Protecting Personal Data in a Globalised World".[65] This, however, does not serve the purpose to provide the highest protection for personal data and as argued in Section 1, an adequacy decision gives the highest threshold of advantages for data processing. Therefore, negotiations must be open to all interested countries and conducted on a non-discriminatory basis. Differentiating between countries that can start negotiations and those that cannot is discriminatory as it gives a preferential treatment to those the Commission finds suitable according to the list of assessment criteria published in the 2017 Communication.[66]

The procedures on the Commission side are not transparent, as highlighted by the CJEU and Kuner.[67] The current lack of transparency requires empirical research to further analyze the procedural side of adequacy decisions as an example for regulatory cooperation. Procedural elements, however, are only one part of the assessment. Adequacy will not be found without an equivalent level of personal data protection in the third country or international organization. The Directive and the GDPR set specific requirements for the protection of personal data. The Commission and the WP/EDPB conduct the assessment based on the applicable criteria.

2.3. Assessment criteria for adequacy

The criteria that the EDPB and the Commission must consider, to evaluate the adequacy of the given third country or international organization, are laid down in Art. 45(2) GDPR. Under the Directive the criteria were regulated in Art. 25. In summary, there are three main elements that have to be analyzed in the assessment: the 'data protection regime'; existence and effective functioning of an independent supervisory authority; and the third country's international commitments and activities.[68] These elements are both captured in Art. 25 of the Directive and the subparagraphs of Art. 45(2) GDPR.[69] However, Art. 45(2) GDPR does set a longer list of criteria under each subparagraph providing more transparency on the relevant requirements for personal data protection. This is because the subparagraphs of Art. 45(2) now capture the criteria that the CJEU addressed in *Schrems I* (EU-US Safe Harbour) judgement.[70]

---

[62] Kuner 2020, p. 785. See also footnote 84 on p. 785.
[63] Stoddart, Chan and Joly 2016. Kuner 2020, p. 785.
[64] Greenleaf, G. Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection. Privacy Laws & Business International Report, Issue 111, 2011, p. 2.
[65] Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World. Brussels, 10.1.2017, COM(2017) 7 final, p. 8.
[66] *Ibid*., p. 8.
[67] Case C-362/14, Maximilian *Schrems v. Data Protection Commissioner*. Judgement of 6 October 2015, ECLI:EU:C:2015:650, paras. 67-106. Kuner 2020, p. 785.
[68] Rücker, D., Kugler, T. New European General Data Protection Regulation. A Practitioner's Guide. C.H. Beck, Hart, Nomos, 2017, p. 196.
[69] Together with Art. 45(2) GDPR, the Commission and the EDPB also need to take into consideration the complete regulation of the GDPR and its content principles, like security and confidentiality principles, restrictions on onward transfers etc. The WP also published a paper on that in 2017. Kuner 2020, p. 788.
[70] Case C-362/14, Maximilian *Schrems v. Data Protection Commissioner*. Judgement of 6 October 2015, ECLI:EU:C:2015:650.

This subsection draws attention to the differences in the evaluation of adequacy approaches followed in various cases. The assessment criteria for adequacy decisions demonstrate that the evaluation criteria are not defined in an exhaustive manner and the legal text provides room for circumstantial criteria. The evaluation analysis practice does not provide a continuity in the methodology used which hampers transparent comparison of systems along the main elements of an adequacy determination. This highlights the importance of understanding the application of the requirements of EU personal data protection in cross-border data flows between the EU and third countries. It is the key to enhance the coherence between EU's law and the regulations in the third country on privacy protection to keep an open digital economy for both sides.

Art. 45 GDPR and the opinions on the adequate level of personal data protection in third countries that have applied for adequacy show that there is wide leverage to decide whether a third country's regulation provides or does not provide an adequate level of protection. The first sentence of Art. 45(2) states that '[w]hen assessing the adequacy of the level of protection, the Commission shall, *in particular*, take account of the following elements:/…/' (emphasis added). This shows that the Commission could find that other criteria are also relevant to determine the adequacy. Kuner contends that "the grounds for evaluation of adequacy under the GDPR are largely political rather than objective requirements"[71] and Greenleaf has questioned the objectivity of the studies and how it has been interpreted by the WP/EDPB.[72] The assessment criteria of adequacy can be best understood by the analysis of the opinions. This sub-section gives examples based on three adequacy opinions: Australia, New Zealand and Japan.[73]

When comparing the analysis conducted before the GDPR: Australia's and New Zealand's data protection law, the opinions examined under the Directive do not follow the same content and structure.[74] The transparency and depth of the analysis differs. As one decision is from 2001 (Australia) and the other one from 2011 (New Zealand), it is understandable that the practice has evolved in those ten years. However, the working document used as a basis for the examination of adequacy of New Zealand data protection legislation "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive"[75] is from 1998. The WP refers to this working paper in the 2011 opinion. There is no reference to this document in the opinion on Australia's data protection legislation. However, one could assume that it should have been taken into consideration also in 2001.

[71] Mishra, N. Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? World Trade Review, 2019, p. 12. Kuner, C. The Internet and the Global Reach of EU Law. LSE Law, Society and Economy Working Papers 4/2017. London School of Economics and Political Science, 2017, p. 28. Kuner, C. The Internet and the Global Reach of EU Law in Cremona, M. and Scott, J. (eds.) EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law. Oxford University Press, 2019.

[72] Greenleaf, G. and Bygrave, L. Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection. Privacy Laws & Business International Report, Issue 111, 2011. Greenleaf, G. Japan: EU Adequacy Discounted. 155 Privacy Laws & Business International Report 8-10; UNSW Law Research Paper No. 19-5, 2018.

[73] As presented above, both New Zealand and Australia negotiated an adequacy decision under the Directive. Japan is the only country that has received an adequacy decision under the GDPR.

[74] Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000. Article 29 Data Protection Working Party. 5095/00/EN, WP40 final. Opinion 11/2011 on the level of protection of personal data in New Zealand. Article 29 Data Protection Working Party. 00665/11/EN, WP182, 4 April 2011.

[75] Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. Working Document. DG XV D/5025/98, WP12, 24 July 1998.

Another difference between these two opinions is that in 2011, the Commission provided the WP with an academic analysis for their evaluation.[76] Before the details of the New Zealand's data protection, the research and the examination process of the legal instruments has been laid out in the New Zealand's opinion.[77] Also the analysis takes into account the domestic case law in New Zealand. In the opinion on Australia's data protection there is no indication how the research on the analysis of the Australian privacy clauses were conducted nor is there any reference to case law in Australia that could be relevant and clarify certain elements of the privacy law in place. These differences in the analysis methodology create a significant gap between the two documents which make it difficult to understand all the relevant elements of the two systems.

In the results of the assessment, the WP refers to the fact that New Zealand's data protection and privacy law was implemented before the EU Directive and that New Zealand also implements the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. This reference is not made in the assessment of Australia's privacy law as an argument. Australia's privacy legislation dates to 1988 where Australia first defined the Information Privacy Principles (IPPs), which were also based on the OECD Guidelines.[78]

The WP also considered the size and nature of the market in New Zealand as a relevant factor: "it is relevant that New Zealand is a small country of approximately 4.3 million people and as the expert report makes clear fair information handling is seen as good business. Organisations cannot afford to alienate such a small market, and news of poor practice spreads quickly. This has a significant effect on business practice."[79] This argument is only used for New Zealand and the WP has taken a rather arbitrary argument to find adequacy. In a globalized and complex digital economy, cross-border movement of data need not be correlated with population size.

Both opinions do examine the regulation for onward transfers to protect EU personal data when data leave the territory of the country that has obtained an adequacy decision.[80] This is one of the content principles that must be evaluated for adequacy.[81] In the case of Australia, the WP suggests Australia adopt appropriate safeguards, as the protection of the relevant provision does not extend to non-Australians.[82] The Working Party did not find that Australia's data protection law is adequate to EU's protection.[83]

---

[76] "The European Commission provided a report it had requested on the adequacy of the protection of personal data in New Zealand, which was written by Professor Roth, Faculty of Law, University of Otago, Dunedin, New Zealand. This report was written under the supervision of the Centre de Recherches Informatique et Droit (CRID) of the University of Namur." WP Opinion 11/2011, p. 2.

[77] The structure of the opinion could be based on Prof. Roth's research report.

[78] The 1980 OECD Guidelines can be accessed here: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. These Guidelines have been updated in 2013 and OECD is currently (2020) working on enhancing these rules further. See: http://www.oecd.org/sti/ieconomy/privacy.htm.

[79] WP Opinion 11/2011, p. 3.

[80] See recital 101, Arts. 44 and 45(2)(a) GDPR on the protection of onward transfers.

[81] Kuner 2020, p. 788. Working Party, 2017.

[82] Opinion 3/2001, p. 6.

[83] Hughes, Aneurin. A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (CTH). University of New South Wales Law Journal (UNSW Law Journal), Volume 24(1), 2001, pp. 270-276.

In the case of New Zealand, the WP found as follows: "As New Zealand law is based on the OECD guidelines, there is no specific provision on protections and safeguards when personal data is transferred to a third country."[84]/…/ "The Working Party has some concerns as regards the effectiveness of the provisions in practice as it is not clear how the Commissioner will become aware of transfers out of New Zealand other than through data protection authorities. Nevertheless the changes in the law and the Commissioner's guidance have alerted businesses to the need to provide 'adequacy' in relation to any onward transfers on penalty of a transfer prohibition notice. In reality, given the geographical isolation of New Zealand from Europe, its size and the nature of its economy, it is unlikely that New Zealand agencies will have any business interest in sending significant volumes of EU-sourced data to third countries."[85] Greenleaf argues that it seems the WP was 'eager to find adequacy'[86] in the case of New Zealand even though the possibility remained that EU's personal data would not be protected when leaving the territory of New Zealand and the WP found other issues in the regulation. The WP found that New Zealand does, however, provide an adequate level of protection.

Onward transfers also seem to be a concern in the EDPB opinion on Japan, as the EDPB asked the Commission to monitor that Japan will change its practice in order to protect personal data from EU if it moves to a country that is not subject to an adequacy decision.[87] The Commission moved forward with the adoption of the implementing act to grant adequacy to Japan despite the fact that the opinion by the EDPB raised several issues that should still be addressed in order to find adequacy.[88]

The other main element to receive adequacy is the analysis of third country's 'international commitments and activities'. Recital 105 GDPR links Convention 108 to one of the criteria to decide adequacy.

Recital 105 reads as follows:

> Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

The WP stated that adequacy requires compliance "with a 'core' of principles relating both to the content of data protection rules and their enforcement, based on the GDPR, the Charter of Fundamental Rights of the European Union (CFR) and other relevant international instruments, such as Council of Europe Convention 108".[89] In the 1998 working document directly referred to in the opinion given to New

[84] WP Opinion 11/2011, p. 9.
[85] *Ibid*., p. 10.
[86] Greenleaf, G. Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection. Privacy Laws & Business International Report, Issue 111, 2011, pp. 2-3.
[87] Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan. Opinion of the Board (Art. 70.I.s), 5 December 2018, p. 6, paras. 15-17; p. 18-19.
[88] *Ibid*., para. 30.
[89] Kuner, 2020, p. 775. WP29, 2017, p. 3.

Zealand, the WP dedicated a separate Chapter on the role of Convention 108.[90] Carvalho suggests that there is a strong linkage between having ratified Convention 108 and receiving an adequacy decision.[91]

Australia, New Zealand and Japan all belong to the category observer countries/data protection authorities.[92] They have not signed Convention 108. The opinions should have explicitly explained based on recital 105 GDPR why this has not been taken into consideration with regards to Australia, New Zealand. The EDPB does refer to the fact that Japan is only an 'observer of the Consultative Committee of Convention 108+' and that the Commission should take that into account.[93] This is a step forward in the assessment of adequacy compared to the opinion adopted under the Directive.

The Commission could state that it is only a small part of the overall analysis of the adequacy. However, there is no transparency on the Commission's decision-making process after the opinion has been adopted. As noted, the Commission does not always follow the recommendation of the WP/EDPB (it did not in the case of Japan). It is therefore argued that the lack of coherence and consistency in applying the assessment criteria throughout the opinions and the evaluation framework of the adequacy decisions as it exists now, there is a need to be as transparent as the other safeguard mechanisms under the GDPR.

The foregoing does not imply the WP did not make the right decision. For this it is necessary to conduct a complete analysis of the legislation in Australia and New Zealand. The examples discussed here do highlight that there is not enough information available for either an EU citizen that wants to know how their data is protected or for a third country to prepare itself for negotiations. There is no clear line to follow in the opinions and in the Commission's decisions to understand the full rationale behind the evaluation of the presented criteria or the methodology framework used. Furthermore, as the previous adequacy decisions have also been challenged with regards to the level of protection they create in practice,[94] the Commission needs to further address the review mechanism established under Art. 45(3) GDPR and the necessity to apply this also to the adequacy decisions negotiated before the GDPR came into force.

2.4. The review mechanism for adequacy decisions

As discussed above, the substance of the adequacy decisions framework under the GDPR and the Directive are considered similar.[95] However, the GDPR is more detailed, with a broader scope including a review

[90] Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. Working Document. DG XV D/5025/98, WP12, 24 July 1998, p. 8-9.
[91] Duque de Carvalho, S.L. Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108. 5 EDPL, 2019.
[92] Parties. Convention 108 in the world. Council of Europe. Available at: https://www.coe.int/en/web/data-protection/convention108/parties.
[93] Opinion 28/2018, p. 12.
[94] All three decisions on the EU-US privacy frameworks. Greenleaf, G. Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection. Privacy Laws & Business International Report, Issue 111, 2011, p. 2.
[95] Weber, R.H. Free flow of data and digital trade from an EU perspective in Ed. Peng, S. *et al*. (Eds.) Governing Science and Technology under the International Economic Order. Regulatory Divergence and Convergence in the Age of Megaregionals. Edward Elgar Publishing, 2018, p. 56. Kuner, C. The Internet and the Global Reach of EU Law. LSE Law, Society and Economy Working Papers 4/2017. London School of Economics and Political Science, 2017, p. 17.

mechanism for adequacy decisions that did not exist under Art. 25 of the Directive.[96] According to Art. 45(3) GDPR, the implementing act must provide for a mechanism for a periodic review, at least every four years.[97] The adequacy decision prior to the GDPR do not indicate when and how often the Commission conducts a review about the data protection regulations.

There is no information given to the Working Party that the Commission conducted any reviews between 1995 to 2018 nor during the implementation period of the GDPR to reassess whether the third countries continue to ensure an adequacy level of personal data protection. There are no documents available on this, except the decision adopted after *Schrems I*[98] judgement where the Commission amended the existing adequacy decisions. For example, from 2016 the new text of Article 3 for New Zealand's adequacy decision is the following:

"The Commission shall, on an ongoing basis, monitor developments in the New Zealand legal order that could affect the functioning of this Decision, including developments concerning access to personal data by public authorities, with a view to assessing whether New Zealand continues to ensure an adequate level of protection of personal data."[99]

The Commission did not inform the WP and has not informed the EDPB about any reviews with regards to the 11 currently in force adequacy decisions adopted under the Directive. Even though Art. 70.1(s) does not state that the EDPB shall conduct a review, the Commission has involved the EDPB in the first review of the adequacy decision given to Japan. The implementing act specifies that the first review has to be conducted two years after entry into force.[100] How the review is supposed to be conducted, is unknown to the public. The Commission has said that they do not only need to evaluate the laws that provide the protection of personal data, but how the laws are implemented in practice. Due to the comprehensive changes in the EU data protection regulation these adequacy decisions should have been reviewed together with the adoption of the GDPR. This contributes to the perception of deficiency or subjectivity in the enforcement of Art. 45 GDPR.

The current framework of adequacy decisions implementation creates a layer of discrimination between the adequacy decisions that have been negotiated before and after 15 May 2018. The standards are stricter for the countries that do not have an adequacy decision and would like to negotiate one. The standards to determine the level of personal data protection cannot differ. The balance between the costs

Kuner, C. The Internet and the Global Reach of EU Law in Cremona, M. and Scott, J. (eds.) EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law. Oxford University Press, 2019.

[96] Art. 45(3) GDPR. Voigt, P., von dem Bussche, A. The EU General Data Protection Regulation (GDPR): Practical Guide. Springer, 2017, p. 116.

[97] The implementing acts that are in force can be found under the file of each country that has obtained an adequacy decision. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[98] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner.*

[99] Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2016) 8353). ELI: http://data.europa.eu/eli/dec_impl/2016/2295/oj.

[100] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information. ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj.

and benefits have drastically changed as the impact of the GDPR is bigger than the Directive. Negotiations take for years and companies outside of the protection of an adequacy decision had to in any case set up internal regulations and contracts during that period to comply with the GDPR. Therefore, it is crucial to set the same standards for all EU's adequacy decisions. Otherwise, based on EU's WTO obligations, the framework of adequacy decisions could be challenged by any other WTO members under the GATS.

3. WTO commitments and data adequacy decisions

The GDPR determines how personal data that belongs to EU citizens should be treated within the EU and outside of its borders. When personal data of an EU citizen moves outside of the EU's territory, it constitutes a cross-border data flow. Domestic regulations on cross-border data flows are directly linked to international trade rules set in the GATS for cross-border movement of services that regulates how information that is being exchanged electronically or via post is moving from one country to another.[101] The GATS is an agreement that applies to all countries that are members of the WTO. If data goes through any kind of processing it is linked to a service as there is exchange of information that serves a purpose and the GATS provisions can have an impact on it.[102] The EU is a member of the WTO and has taken international commitments under the GATS that the GDPR has to be in line with.[103] Therefore, the regulations that the EU imposes at the domestic level have to comply with the GATS.

The GDPR aims at protecting privacy of individuals and the security of this information. However, the way it is currently applied in practice raises several questions about EU's compatibility with Articles XVI: Market Access, XVII: National Treatment and Article II: Most-Favoured-Nation Treatment (MFN) of the General Agreement on Trade in Services (GATS).[104] Therefore, the EU would defend the GDPR under Article XIV of the GATS or Article XIV:(bis) of the GATS.

A WTO member could file a case against the EU if the companies based in that country have faced losses because of the necessity to renegotiate their contracts compared to companies in a country that has an adequacy decision. Another ground could be linked to a request for consultations where a country does not receive an adequacy decision even though another country that has similar privacy regulations in place has received an adequacy decision or the conditions for negotiating an adequacy decision are different. These are several reasons why EU data transfer requirements could be disputed under Art. II of the GATS. Article XIV of the GATS becomes a relevant defence if there is a violation with a certain provision under the GATS. The adequacy brings stability in the relationship of selected group of countries, but it

---

[101] Burri, M. Designing Future-Oriented Multilateral Rules for Digital Trade, in Sauvé, P. and Roy, M. (eds.). Research Handbook on Trade in Services. Cheltenham: Elgar, 2016, pp. 331, 349.

[102] Weber, R.H. Free flow of data and digital trade from an EU perspective in Ed. Peng, S. *et al*. (Eds.) Governing Science and Technology under the International Economic Order. Regulatory Divergence and Convergence in the Age of Megaregionals. Edward Elgar Publishing, 2018, p. 56. It can be as simple as a hotel company, owning hotels in the EU and outside of the EU, wanting to know who are their clients, which age group, which nationalities prefer one of their hotels or another; or the hotel wants to process their data to improve customer service; or it could be a data processing company offering a service to another company to improve their marketing for a specific group of customers.

[103] European Union. Schedule of Specific Commitments. 07/05/2019, GATS/SC/157. Available at: https://www.wto.org/english/tratop_e/serv_e/serv_commitments_e.htm.

[104] Mishra, N. Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? World Trade Review, 2019. Meltzer, J.P., Mattoo, A. International Data Flows and Privacy: The Conflict and Its Resolution. Journal of International Economic Law, Volume 21, Issue 4, pp. 769–789, 2018.

creates potential competitive distortions that may be contested under the WTO rules on non-discrimination and/or specific market access commitments made by a country in the GATS. Therefore, the EU could potentially defend Art. II GATS violations under the GATS exceptions provisions – Articles XIV (General Exceptions) and XIV bis (Security Exceptions).

If an adequacy decision constitutes a part of a free trade agreement, as was the case for Japan, where negotiations on adequacy and a free trade agreement were held simultaneously, there would not be violation of Art. II of the GATS. Thus, the matter arises in contexts where adequacy is not embedded in an EU free trade agreement. Arguments could be made on the issues raised under Section 2. The Commission has referred to the political nature of its framework on adequacy findings and to its commercial relations to the third country through free trade agreement in its Communication "Exchanging and Protecting Personal Data in a Globalised World".

> "Under its framework on adequacy findings, the Commission considers that the following criteria should be taken into account when assessing with which third countries a dialogue on adequacy should be pursued:
> (i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
> (ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
> (iii) 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
> (iv) 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." (footnotes of the text have been excluded).[105]

It could also be argued that the framework on its own violates Art. V: Economic Integration of the GATS as it provides preferential access to the EU for data flows, and an adequacy decision on its own does not have a substantial sectoral coverage as required by Art. V:1(a) of the GATS.

The transparency issue in the proceedings and ununified evaluation methodology of adequacy and the selection process of the Commission to decide which country gets to negotiate an adequacy decision, could violate Art. VI:1 of the GATS: 'In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner.'

A third country might also invoke GATS Art. VII (recognition). Art. VII:1 of the GATS states that "a Member may recognize the education or experience obtained, requirements met, or licenses or certifications granted in a particular country. Such recognition, which may be achieved through harmonization or otherwise, may be based upon an agreement or arrangement with the country concerned or may be accorded autonomously." Art. VII paras 2 and 3 go on to say that:

> 2. A Member that is a party to an agreement or arrangement of the type referred to in paragraph 1, whether existing or future, shall afford adequate opportunity for other interested Members to negotiate their accession to such an agreement or arrangement or to negotiate comparable ones with it. Where a Member accords recognition autonomously, it

[105] Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World. Brussels, 10.1.2017, COM(2017) 7 final, p. 8.

.

shall afford adequate opportunity for any other Member to demonstrate that education, experience, licenses, or certifications obtained or requirements met in that other Member's territory should be recognized.

3. A Member shall not accord recognition in a manner which would constitute a means of discrimination between countries in the application of its standards or criteria for the authorization, licensing or certification of services suppliers, or a disguised restriction on trade in services.

Although the focus of Art. VII is on professional qualifications and licensing of service suppliers, these principles presumably apply to adequacy decisions as well. After the July 2020 CJEU judgement, there is no adequacy decision in force between the EU and US. However, as the Safe Harbour and the Privacy Shield framework were based on self-certification system. There is no evidence whether, for example EU and Australia discussed this also as an alternative framework for an adequacy decision. However, this option has to be available for all third countries to be in compliance with Art. VII of the GATS.

Finally, there is a potential issue as regards compliance with GATS Art. III (Transparency). The EU must present and inform WTO members about this cooperation model under Art. III of the GATS. The EU has not formally notified adequacy decisions to the WTO and there has been limited discussion of such decisions in the WTO. Adequacy was discussed in the context of EU Trade Policy Reviews from 2002 and 2004.[106] Why there has been such limited attention given to adequacy determinations by the EU is question for further research.

3.1 Open plurilateral agreements as a potential way forward

Hoekman and Sabel (2019; 2021) note that domain- or issue-specific plurilateral cooperation offers an alternative to the negotiation of trade agreements as a mechanism for countries address cross-border policy spillovers.[107] Open plurilateral agreements (OPAs) provide a potential vehicle to support international regulatory cooperation on data protection and data adequacy in the WTO, in the process addressing many of the potential concerns that unilateral data adequacy decisions may raise under the GATS.

Hoekman and Sabel argue OPAs differ from standard preferential trade agreements (PTAs) in at least four ways.[108] First, OPAs are open to participation of any country able to satisfy the membership conditions, in contrast to PTAs that generally are closed to access by new countries. Second, insofar as OPAs address trade costs created by regulatory heterogeneity they do not lend themselves to quid pro quo exchange of concessions. Third, because they are domain specific, OPAs involve narrower and more limited commitments. A member must only undertake to meet the requirements that have been agreed for the issue or class of goods and services concerned. Insofar as an OPA requires only equivalent performance—

[106] Trade Policy Review: European Union. Minutes of Meeting. Trade Policy Review Body, 24 and 26 July 2002, WTO. WT/TPR/M/102/Add.1, p. 61. Trade Policy Review: European Communities. Minutes of Meeting. Trade Policy Review Body, 25 and 27 October 2004, WTO. WT/TPR/M/136/Add.2, p. 29.

[107] Hoekman, B. and Sabel, C. 2019. Open Plurilateral Agreements, International Regulatory Cooperation and the WTO. At https://onlinelibrary.wiley.com/doi/abs/10.1111/1758-5899.12694.

[108] Hoekman, B. and Sabel, C. 2021. Plurilateral Cooperation as an Alternative to Trade Agreements: Innovating One Domain at a Time. At: http://respect.eui.eu/wp content/uploads/sites/6/2020/12/Hoekman_Sabel_JSIs_OPAs_Dec_2020.pdf.

not identical procedures or institutions—they permit members to produce the required outcome through their own regulatory regimes and institutions. Fourth, and related, implementation of OPAs calls for continuing reciprocal review of existing regulatory policies and their implementation, and joint evaluation of potential adaption to changes in circumstances. The potential for learning through regular interactions between regulators and/or a broader epistemic community involved in a policy area may also arise in the implementation of trade agreements but is less of a central feature given the narrow focus on disciplining discrimination. These elements are found in the New Zealand, Chile and Singapore Digital Economy Partnership Agreement (DEPA), which is conceived to be open to any country interested in joining, and where participation is facilitated through a modular design, allowing signatories to opt in or out of modules.

As argued previously, the current EU adequacy framework can be part of a free trade agreement, which is covered under Art. V of the GATS. However, as a separate framework adequacy determinations may violate the GATS. Clearly the EU can, and presumably will, invoke GATS Art. XIV in defense of this separate framework for the protection of privacy, arguing it is necessary for the free cross-border flow of data. Giving consideration to embedding adequacy in a plurilateral framework would increase transparency and ensure compliance with GATS Art. III:3 as well as compatibility with Art. XIV GATS chapeau requirements. A plurilateral framework along the lines of what is suggested in Hoekman and Sabel (2021) would also help the EU to operationalize the principles embodied in Art. VII on regulatory recognition by providing a mechanism for deliberation among like-minded countries that share public policy objectives in the area of data privacy.

In order to consider the EU's framework of adequacy decisions as the basis of a potential OPA, the adequacy decisions adopted before the Directive need to go through a review process and the mechanism for periodic review has to be added to the implementing acts of the decisions adopted before the GDPR. Art. 45(3) GDPR requires this for the adequacy decisions adopted after the enforcement of the GDPR. Undertaking such assessments as part of a plurilateral initiative would help to improve transparency in the criteria and evaluation of domestic regulatory systems that are relevant for assessments of equivalence and thus adequacy determinations.

Cooperation among a like-minded group of WTO members could build on the experience to data in negotiation of digital economy agreements that span equivalence of data privacy regimes and provide a framework for plurilaterizing extant unilateral decisions and bilateral or regional cooperation in this area, including the New Zealand-Singapore-Chile DEPA. What such a plurilateral might look like in terms of substantive provisions is beyond the scope of this paper. Thinking through if and how an OPA could benefit the EU and its trading partners and complement the ongoing negotiations among groups of WTO members on e-commerce and domestic regulation of services could help the EU support the open rules-based multilateral trading system.

4. Conclusion

The European Union (EU) regulates cross-border movement of personal data through several instruments, including the General Data Protection Regulation (GDPR). Companies processing or with access to personal data originating in the EU must comply with EU regulation or confront fines. For third countries, the most comprehensive way to ensure cross-border data flows are unencumbered is to obtain an adequacy decision by the EU. The three case studies considered in this paper – Australia, New Zealand and Japan – reveal there is a lack of transparency about the procedures for the application of adequacy

decisions. Australia was denied adequacy, while New Zealand was granted adequacy status under Directive 95/46, the predecessor to the GDPR. Japan to date is the only example of a positive adequacy decision taken under the GDPR.

The shift from a privacy Directive to a comprehensive personal data protection Regulation, also raises the questions how the Commission has made sure that the decisions adopted under the Directive correspond to the same standards that the GDPR sets for privacy protection. The analysis of the EU's determinations of adequacy and the assessment procedures reveals not only an absence of transparency but a lack of clarity in the processes and criteria applied.

As noted in the submission of the RESPECT consortium in response to the EU consultation on a renewed trade policy for a stronger Europe, transfers of data are crucial for today's economy. The EU could start engaging more actively in promoting free and safe transfer of data across borders by broadening the Free Flow of Data Initiative to other countries and extend 'adequacy' status to countries which implement strong data protection rules. To promote legal certainty, a revision of the process to grant adequacy could be considered so that the process is more transparent and does not create concerns about arbitrariness and de facto discrimination. Regulation of cross-border data flows is a key policy area calling for greater legal clarity at the multilateral level including in the context of GATS commitments. When multilateral cooperation is not viable, plurilateral discussions offer a possible path towards gradual multilateralization of cooperation.[109]

The current EU framework for data adequacy decisions can be made part of a free trade agreement, which would insulate it from challenges under the WTO. However, as a separate framework, as it has been since 1995, the implementation of the EU approach can be challenged under the GATS. To defend its approach the EU must argue for the necessity for this separate framework for the protection of privacy of cross-border data flows under Art. XIV of the GATS. Adopting a plurilateral approach would help to complement the current strictly unilateral approach by enhancing transparency of both decisions and their implementation, and help to create a network of like-minded countries that have equivalent standards of data privacy and protection, in the process reducing trade costs for firms based in participating countries.

[109] See: http://respect.eui.eu/wp-content/uploads/sites/6/2020/12/EU-trade-policy-consultation_RESPECT.pdf.

References

Aaronson, S.A., Leblond, P. Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. Journal of International Economic Law (JIEL), 2018.

Burri, M. Designing Future-Oriented Multilateral Rules for Digital Trade, in Sauvé, P. and Roy, M. (eds.). Research Handbook on Trade in Services. Cheltenham: Elgar, 2016.

Duque de Carvalho, S.L. Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108. 5 European Data Protection Law Review (EDPL), 2019.

Fuster, G. Un-mapping personal data transfers. European Data Protection Law Review (EDPL), 2(2), 2016, 160-168.

Greenleaf, G. and Bygrave, L. Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection. Privacy Laws & Business International Report, Issue 111, 2011.

Greenleaf, G. Japan and Korea: Different Paths to EU Adequacy. 156 Privacy Laws & Business International Report, 2018, 9-11.

Greenleaf, G. Japan: EU Adequacy Discounted. 155 Privacy Laws & Business International Report 8-10; UNSW Law Research Paper No. 19-5, 2018.

Greer, D. Tomorrow's Privacy. Safe Harbor – a framework that works. International Data Privacy Law. Vol. 1. No.3. 2011.

Hoekman, B. and C. Sabel. Open Plurilateral Agreements, International Regulatory Cooperation and the WTO. Global Policy, 10(3): 297-312, 2019.

Hoekman, B. and C. Sabel. Plurilateral Cooperation as an Alternative to Trade Agreements: Innovating One Domain at a Time. Global Policy, forthcoming 2021.

Hughes, A. A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (CTH). University of New South Wales Law Journal (UNSW Law Journal), Volume 24(1), 2001, pp. 270-276.

Kuner, C. *et al*. (eds.) The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020.

Kuner, C. The Internet and the Global Reach of EU Law in Cremona, M. and Scott, J. (eds.) EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law. Oxford University Press, 2019.

Kuner, C. The Internet and the Global Reach of EU Law. LSE Law, Society and Economy Working Papers 4/2017. London School of Economics and Political Science, 2017.

Linn, E. A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement. Vanderbilt Journal of Transnational Law, 50(5), 1311-1358, 2017.

Meltzer, J.P., Mattoo, A. International Data Flows and Privacy: The Conflict and Its Resolution. Journal of International Economic Law, Volume 21, Issue 4, pp. 769–789, 2018.

Miadzvetskaya, Y. What are the pros and cons of the Adequacy decision on Japan? KU Leuven. Centre for IT & IP Law. Available at: https://www.law.kuleuven.be/citip/blog/what-are-the-pros-and-cons-of-the-adequacy-decision-on-japan/.

Mishra, N. Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? World Trade Review, 2019.

Puccio, L., Monteleone, S. From Safe Harbour to Privacy Shield. Advances and shortcomings of the new EU-US data transfer rules. European Parliamentary Research Service (EPRS), PE 595.892, January 2017.

Rücker, D., Kugler, T. New European General Data Protection Regulation. A Practitioner's Guide. C.H. Beck, Hart, Nomos, 2017.

Schwartz, P. M. The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. 126(7) Harv. L. Rev. 1966, 2013.

Shaffer, G. Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards. Yale Journal of International Law, 25(1), 1-88, 2000.

Voigt, P., von dem Bussche, A. The EU General Data Protection Regulation (GDPR): Practical Guide. Springer, 2017.

Weber, R.H. Free flow of data and digital trade from an EU perspective in Ed. Peng, S. *et al*. (Eds.) Governing Science and Technology under the International Economic Order. Regulatory Divergence and Convergence in the Age of Megaregionals. Edward Elgar Publishing, 2018.

The General Agreement on Trade in Services. LT/UR/A-1B/S/1, 15 April 1994.

Trade Policy Review: European Union. Minutes of Meeting. Trade Policy Review Body, 24 and 26 July 2002, WTO. WT/TPR/M/102/Add.1.

Trade Policy Review: European Communities. Minutes of Meeting. Trade Policy Review Body, 25 and 27 October 2004, WTO. WT/TPR/M/136/Add.2.

European Union. Schedule of Specific Commitments. 07/05/2019, GATS/SC/157. Available at: https://www.wto.org/english/tratop_e/serv_e/serv_commitments_e.htm.

Australia and Singapore (signed December 2020). See: https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement.

Chile, New Zealand and Singapore DEPA (signed June 2020). Available at: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement/.

Japan-US Agreement on Digital Trade (signed October 2019). Available at: https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

The 1980 OECD Guidelines. Available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Parties. Convention 108 in the world. Council of Europe. Available at: https://www.coe.int/en/web/data-protection/convention108/parties.

Adequacy decisions. European Commission. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union. COM/2019/250 final, 29.5.2019.

Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World. Brussels, 10.1.2017, COM(2017) 7 final.

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 Data Protection Regulation). ELI: http://data.europa.eu/eli/reg/2016/679/oj.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. ELI: http://data.europa.eu/eli/reg/2018/1807/oj.

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. ELI: http://data.europa.eu/eli/dir/1995/46/oj.

Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. Working Document. DG XV D/5025/98, WP12, 24 July 1998.

Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000. Article 29 Data Protection Working Party. 5095/00/EN, WP40 final;

Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines. Article 29 Data Protection Working Party. 10031/03/EN, WP85.

Opinion 11/2011 on the level of protection of personal data in New Zealand. Article 29 Data Protection Working Party. 00665/11/EN, WP182, 4 April 2011.

Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco. Article 29 Data Protection Working Party. 01446/12/EN, WP198.

Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan. Opinion of the Board (Art. 70.1.s) adopted on 5 December 2018.

2006/253/EC: Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency (notified under document number C(2005) 3248).

Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information. Available at: 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.

Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2016) 8353). ELI: http://data.europa.eu/eli/dec_impl/2016/2295/oj.

The Decision 2004/535 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection.

Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service. CELEX number: 22012A0714(01). OJ L 186, 14.7.2012.

C-362/14 *Maximillian Schrems* v. *Data Protection Commissioner, Joined Party Digital Rights Ireland Ltd.*, ECLI:EU:C:2015:650.

C-131/12 *Google Spain SL, Google Inc.* v. *Agencia Española de Protección de Datos (es), Mario Costeja González*, ECLI:EU:C:2014:317.

T-670/16 *Digital Rights Ireland v Commission*, ECLI:EU:T:2017:838.

Case C-311/18 *Data Protection Commissioner* v *Facebook Ireland and Maximillian Schrems*. Judgement of 16 July 2020, ECLI:EU:C:2020:559.

Joined Cases C-317/04 and C-318/04 *Parliament v Council and Commission*. Judgement of 30 May 2006, ECLI:EU:C:2006:346.