EASTERN EUROPEAN JOURNAL OF TRANSNATIONAL RELATIONS

The meaning of „adequate" under GDPR – lesson learnt from EU bodies

Dominika Kuźnicka-Błaszkowska
Department of Law, Administration and Economics, University of Wroclaw, Poland
dominika.kuznicka-blaszkowska@uwr.edu.pl
ORCID 0000-0001-8804-569X

Abstract. The concept of "adequate" data protection model in third country or organisation plays vital role in General Data Protection Regulation, but more importantly – in business and relations between European Union and other international actors. Understanding what "adequate" means is crucial for ensuring the security of personal data transferred outside EU. However, the European Union has not provided clear guidance on this matter, which may have negative consequences for businesses, individuals, and the EU as a whole. This paper examines the meaning of 'adequate' by analyzing the work of EU institutions through a deep-dive investigation, as well as comparative and conceptual legal research. The outcome of the research allow researchers and professionals to deeply understand adequacy requirements under General Data Protection Regulation and is viable source for further research in the area but also – in the practice of ensuring GDPR compliance by both private and public organisations.

Keywords: Data transfer, personal data protection, EU law, adequacy, GDPR.

JEL Classification: K33.

Citation: Kuźnicka-Błaszkowska, D. (2025). The meaning of „adequate" under GDPR – lesson learnt from EU bodies. *Eastern European Journal of Transnational Relations*, *9*(1), 55-67. https://doi.org/10.15290/eejtr.2025.09.01.05.

Publisher's Note:

1. INTRODUCTION

Under the General Data Protection Regulation (GDPR) the concept of "adequacy" of foreign data protection model plays a crucial role in personal data transfers. This is generally forbidden to transfer personal data from European Union (EU) to third countries unless either one of transfer mechanisms is used or exceptions apply. GDPR recognizes multiple transfer mechanisms, which provide different level of scrutiny and security of transfer. The primary one, which shall guarantee the most resilience is a decision of European Commission (EC) recognizing

adequate level of protection in third country or organisation. Other transfer mechanisms shall be used only in case EC has not granted adequacy decision yet[1].

The safe transfer of personal data from EU to third countries or organisations plays vital role in global business, especially in EU-US business relations (Murphy, 2021). Adequacy decision aims at reducing the workload affiliated with third country transfers, by, among other things simplifying the regulatory environment for international business (Dahl, 2019). In today's interconnected world, it is difficult to imagine a scenario where companies cannot transfer personal data between the EU and the US. This is not merely a question of accessing internet services, social media, or entertainment platforms—although these are important for individuals. More significantly, data transfer is essential for maintaining strong business and political relations between the EU and the US. One shall understand that the longer transfer of personal data from EU to US cannot provide full reliability, the more resilient US investors and business will be to conduct their activities in EU. Lack of fully reliable adequacy decision also creates a scratch on the bilateral political relations between EU and US. The US and EU's trade relationship is considered to be the "world's largest and most important bilateral commercial relationship" (Hamilton & Quinlan, 2020). The transatlantic economy accounts for 16 million jobs, trillions of dollars in total commercial sales, and one third of the total gross domestic product in terms of purchasing power (Hamilton & Quinlan, 2020).

As Schwartz (2019) and Calia (2022) note numerous countries have aligned their data protection standards with the EU' model, reflecting the GDPR's global influence. Such countries as Turkey, Bahrain, Switzerland fully recognize European Commission decisions on adequacy and recognize the same level of protection as EU does, therefore the stability of adequacy decisions is crucially important for global economy.

Apart from countries which clearly follows EU paths, there are other whose adequacy model differs significantly from GDPR. While the EU prioritizes comprehensive legal frameworks, the United States relies on a sectoral approach to data protection. China's Personal Information Protection Law (PIPL), on the other hand, imposes strict government oversight, which conflicts with EU principles of independent regulatory enforcement (Panek, 2024). Brazil's data protection model incorporates GDPR-like principles but lacks robust enforcement mechanisms.

The CJEU has already annulled two US adequacy decisions. Although the European Commission and the US have recently reached a new agreement, resulting in the granting of a third adequacy decision, it is highly likely that this decision will face further legal challenges before the CJEU[2]. Uncertainty towards adequacy decision and annulment of such by CJEU has cost business money, time, and efforts to implement other transfer mechanisms and allow lawful transfer of personal data to US. This shall not happen again, as at the end this is private business who needs to bear costs of decisions made by politicians. Additionally, the fact that the decision made by EC has been annulled twice and, in both verdicts, CJEU has been quite harsh towards Commission, makes the latter look frivolous and unreliable not only in the eyes of EU member states and public opinion, but also in the eyes of foreign actors.

The concept of 'adequacy' under EU law has been widely debated in academic literature. Blume (2015) examines the flexibility of adequacy decisions, highlighting their political nature, while Drechsler (2021) discusses the absence of Law Enforcement Directive (LED) adequacy decisions and its impact on fundamental rights. Duque de Carvalho (2019) provides a comparative analysis of adequacy findings in countries that have ratified Convention 108, arguing

[1] Under EU-US Data Privacy Framework other transfer mechanisms are also used if personal data is transferred to an entity in US which is not included in Data Privacy Framework list (European Data Protection Board 2023).

[2] In July 2023 European Commission published the third decision recognizing adequacy of personal data protection model in US (C (2023) 4745), however it has been questioned already twice. First was French MEP who in his complaint questioned the adequacy of the decision and applied for interim measures, the interim application has been dismissed by the General Court due to lack of demonstrated urgency (Latombe v Commission (case T-553/23 R)). Organisation None of Your Business lead by Max Schrems has already informed about the intention of revoking the decision again (NYOB 2023). Both of them are pending ruling from CJEU.

that GDPR's adequacy model is evolving towards a more rigid framework. Additionally, Hughes (2001) explores how the EU evaluates third-country privacy laws, emphasizing discrepancies in adequacy assessments. This paper builds on these discussions by evaluating whether recent adequacy decisions reflect a coherent legal standard.

This article does not seek to determine whether the United States provides an adequate level of data protection, as this question shall be subject of other legal analyses. However, a critical gap in existing analyses is the failure to first define what 'adequate' means under EU law. This study employs a doctrinal legal research methodology, systematically analyzing European Commission adequacy decisions, CJEU rulings, and relevant legislative texts. Comparative legal analysis is used to evaluate how different EU bodies understand adequacy requirements. Case law analysis focuses on the *Schrems I* and *Schrems II* decisions to illustrate judicial constraints on adequacy assessments. The research further incorporates academic literature to identify recurring legal themes and inconsistencies in the interpretation of 'adequacy'.

To substantiate this argument, the paper proceeds as follows: First, it examines the impact of adequacy decisions on international data transfers. Next, it analyzes European Commission adequacy decisions to identify common principles. Recognizing the European Data Protection Board's (EDPB) crucial role in the current EU data protection framework, the paper then explores its stance on adequacy. This is followed by a discussion of the CJEU's landmark rulings on personal data transfers to the United States. Finally, the paper addresses controversies surrounding the current approach and provides concluding remarks summarizing the findings

The challenge with defining adequacy may also be equally important for a greater cause. Even though this term is used quite frequently by EU lawmakers and policymakers, hardly ever it is sufficiently defined. Therefore, this paper may serve as a further as a guidance to understand the term "adequate" in EU laws and policies in wider concept and be considered as a basic for further research in any field of EU law.

2. ADEQUACY DECISION AND ITS IMPACT ON INTERNATIONAL DATA TRANSFER

Transfer mechanisms may provide different level of security of processing personal data originating from EU member states in third countries. One of the most important, and in most of the cases the safest mechanisms to transfer the data is adequacy decision granted by European Commission. In a nutshell adequacy requires that the content of data protection rules in third countries or international organisation to meet the standard of EU law, and that such rules be effective in practice. The adequacy decision is the main legislative instrument of the European Union to allow greater freedom of cross-border flow of data (Gonzalez Domenech, 2019).

There is currently 15 adequacy decisions in force[3]. Once granted, the data flow between EU and these countries is usually based on the decision and does not require further transfer mechanisms to be in place. Parties of such transfer are obliged to ensure that in the data processing agreement or other contractual relation between them it is agreed which transfer mechanism is used. It does not however release European data exporter from the responsibility to carefully choose the importer or data processor and ensure the adequate data protection in its organisation as well as in the moment of transfer. Nevertheless, transfers under adequacy decision do not require any further approval from data protection authorities or other authorities.

The procedure of issuing adequacy decision usually starts with a third country approaching the Commission and requesting discussion to be opened. Negotiation may take up to several years and are often tighten up with political affairs (i.e. Ireland blocking granting Israeli adequacy decision when the government of Israel was allegedly involved in forging Irish passports (Ihle, 2010; Wolf, 2014)). Commission typically makes its own investigation about the adequacy of data protection model, however, engages in reports and discussions academics, NGOs, think-

[3] As for October 13th 2023.

thanks, practitioners and third parties. Documents concerning deliberations are typically not public, thus the entire procedure misses the transparency.

Before issuing an adequacy decision, the European Commission must consult the European Data Protection Board (EDPB). The Commission submits all relevant documents, correspondence, and research findings, along with the draft decision, for EDPB review. Based on this information, the EDPB provides a non-binding opinion on the adequacy decision. In enacting adequacy decision, the Commission is assisted by a committee of Member States representatives that must approve decision in line with the examination procedure.

Adequacy decision shall contain at least the following points:

1) Clear recognition that the third country or international organisation ensures adequate protection by virtue of its domestic law or international commitments.
2) Territorial and sectoral application of the decision.
3) A mechanism for periodic review of the decision
4) Identify the supervisory authority or authorities with responsibility for ensuring and enforcing compliance with the data protection rules.

According to Article 45 GDPR adequacy decision can be issued for any country which is not EU Member State or a party of European Economic Area. Such decisions can apply to the entire country, its part of specific sector as well as international organisation (as defined in Article 4(26) GDPR). European Commission is out of the opinion that the sectoral decisions 'will need to be considered in light of elements such as, for instance, the nature and state of development the privacy regime (stand-alone, multiple or sectorial law etc.), the constitutional structure of the third country or whether certain sectors of the economy are particularly exposed to data flows from the EU' (COM 2017). For this reason, EC mentioned 'financial services and IT sector" as potential subjects of further adequacy decisions concerning specific sector. Considering other provisions of GDPR, especially basic rules for data transfer, one shall examine whether the concept of issuing adequacy decision only covering specific sector in each country appropriately safeguards individual's rights. At the end, the fact that sectoral adequacy decision has been issued does not change the factual level of data protection law in given country neither its enforcement. Theoretically, it may be possible that EC issues adequacy decision covering IT sector in a country in which public authorities have enormously broad access to personal data without justified reason and in a way not very compliant with basic principles of data processing recognized in EU. This is the case of US-EU Data Privacy Framework and other adequacy mechanisms issued towards this territory. Importantly, under the framework only business organisations participating in this programme may received data from EU controllers. As CJEU rightly pointed out (non-verbatim) in *Schrems I* and *Schrems II* - the fact that specific business organisations meet criterions of adequacy does not mean that the entire model of personal data protection is safe and that public authorities respect fundamental rules for data processing as established in EU.

In the changing world, even the law cannot be taken for granted, neither its enforcement. EU lawmakers understand that and decide to ensure that adequacy decisions will be firstly subject to periodic review and secondly: contain a mechanism which will allow its review if the circumstances change. If, according to Article 45, information reveals that a third country, a territory, or one or more specified sectors within a third country, or an international organisation no longer ensure adequate level of protection, the Commission must repeal, amend, or suspend its adequacy decision by means of implementing act under the examination procedure referred to in Article 93(2) GDPR, except for 'duly justified imperative ground of urgency'. In such case Commission must 'adopt immediately applicable implementing acts in accordance with the procedure referred in Article 93(3)'. Such repeal, amend or suspension of adequacy decision cannot have a retroactive effect. There is a strong rationale behind such approach. Applying retroactive effect would lead to unlawfulness of transfer from the very beginning and as such– liability of data exporter under GDPR. In such scenario this would be controller or processor who has to take responsibilities for someone's else action (e.g. EC assessment of adequacy of data protection model or politics choices of lawmakers

in third country) or even events which are beyond anyone's control (i.e. unstable situation in specific country due to war or riots which will end up in impossibility of data protection laws enforcement).

When Commission takes a decision on repealing, amending, or suspending its adequacy decision, it must enter consultation with interested country to remedy the situation. This is to ensure that 1) personal data which has been already transferred are safe; 2) business continuity is not threatened; 3) appropriate relations between EU and third country or international organisation are still pursued. It must be mentioned that in case that adequacy decision is being repealed, amended, or suspended, other transfer mechanisms which either have been used or are about to be used are not affected. For these reasons it is recommended to ensure that any contractual agreements between the parties include provisions about the transfer of data in case of suspension of adequacy decision or failure of any other transfer mechanism[4].

Apart from reacting immediately to changes which may lead to degradation of data protection level, European Commission is also obliged to run periodic review on already released decisions. This obligation placed in Article 45 GDPR shall be read as a follow up of *Schrems I* ruling, in which CJEU noted that Commission must check 'periodically whether the finding relating to the adequacy of the level of protection ensured by third country in question is still factually and legally justified' (CJEU C-362/14). The implementing decision shall indicate the time for periodic reviews, but no longer than each four years. For example, EU-US Privacy Shield forced a joint annual review. If the changes in the law of the country or international organization require, a periodic review may be conducted ahead of a schedule.

The procedure of periodic review shall be conducted in consultation with third country or international organisation and Commission shall consider the views and findings of European Parliament and of the Council as well as of other relevant bodies and sources. In general, procedure included in the article 93 of GDPR shall be followed. Adequacy decisions issued pre-GDPR also included periodic review clauses, however formulated more vaguely. It is not clear whether the 4-years maximum period for review also applies to previously issued decisions and if it shall be calculated from the date decision has been released or the day GDPR came into force. In any way, all pre-GDPR adequacy decisions shall be reviewed in due time, considering changes in the approach of EU towards data protection law.

Whereas the process of accepting and reviewing adequacy decisions is clearly described in GDPR and supporting documents, this is difficult to assess what "adequacy" means under EU law. As European Commission had already issued a couple of adequacy decisions, whereas CJEU invalidated two of them, the practice of these two bodies may bring interesting conclusions on what "adequate" really means.

3. ADEQUACY OF THE DATA PROTECTION MODEL IN EC ADEQUACY DECISIONS

Whereas European Commission has a lot of independency when conducting research on data protection laws in a country applying for adequacy decision and deciding whether such shall be issued, there are certain criteria to be met. Article 45(2) of GDPR states that the following factors shall be analysed while assessing the adequacy of data protection model in the third country or organisation:

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

[4] Controller shall also ensure that other obligations imposed on him under GDPR (i.e., ensuring that data subjects are properly informed about transfer mechanisms used and transfer risk assessment has been conducted).

country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

B) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, 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; and

C) the international commitments the third country or international organisation concerned has entered, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in relation to the protection of personal data" (GDPR).

Majority of the terms used in the commented article is quite vague and unclear. However, as similar criteria have been used under directive 95/46, guidelines developed by Article 29 Working Party as well as CJEU ruling in Schrems case are not out of use when interpreting adequacy criteria.

Nevertheless, adequacy decisions granted by EC so far provide some guidance on the approach of EC towards the meaning of "adequacy" under data protection model in EU. EC emphasizes that the level of data protection should be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations and considering a number of elements relevant for the transfer and listed in GDPR. The standards shall be binding and enforceable towards private and public actors, in general and sector-specific ways (i.e., Argentina, Japan), constitutional (or other fundamental) rights guarantees (i.e., Andorra) and its further development under specific laws, redress possibilities granted to individuals, sanctions for breaches and non-compliance. This is not relevant, whether constitution of third country provides for general (as in Andorra) of very specific guarantees (as in Argentina) for personal data protection if they are enforceable, binding and are further developed by statutory laws. If the given country does not have a constitution, this is important for the right to privacy to be included in other acts governing fundamental human rights and principles of the country (i.e., Israel[5], New Zealand[6]). Among the factors which are considered by EC is setting data protection laws in the given countries on the same basis as EU data protection model and ratification of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 as well as the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 (i.e. Andorra). Processing of personal data shall be only allowed if based on basic data processing principles, like those agreed within European Union (i.e., Andorra, Canada).

Existence of the supervisory authority invested with powers of investigation and intervention, and which acts completely independently is also an argument for recognizing adequate level of data protection (i.e., Andorra, US, Israel). In so far practice, EC focused on recognizing the entire countries as providing adequate level of personal

[5] The State of Israel's legal system has no written constitution, but constitutional status has been conferred on certain 'Basic Laws' by the Supreme Court of the State of Israel. Those 'Basic Laws' are complemented by a large body of case law, as the Israeli legal system adheres largely to common law principles. The right to privacy is included in the 'Basic Law: Human Dignity and Liberty' under section 7.

[6] New Zealand does not have a written constitution in the conventional sense of an entrenched constitutive document. Nevertheless, by convention there are several statutes that are of constitutional importance and are regarded as 'higher law'. This is in the sense that they form part of the constitutional background or landscape by informing government practice and the enactment of other legislation. Moreover, cross-political consensus would be expected in the event of amendment or repeal of this legislation. Several of these statutes — the Bill of Rights Act of 28 August 1990 (Public Act No 109 of 1990), the Human Rights Act of 10 August 1993 (Public Act No 82 of 1993), and the Privacy Act of 17 May 1993 (Public Act No 28 of 1993) — are relevant to data protection.

data protection with just a few exceptions (related to federal states such as US and Canada[7]). It seems that the adequacy decision is more likely to be granted to self-governing territories of member states (i.e., Faeroe Islands) or its dependencies (i.e., Guernsey, Isle of Man, Jersey). These self-governing territories and dependencies follow the EU legal order and adopt laws (if this is in their powers) reflecting EU data protection model.

Interestingly, as noted by Panek (Panek, 2024), adequacy decisions often miss the assessment of the level of human rights protection which is required by art 45 GDPR. Also, in most of the cases, the considerations on the "rule of law" and commitment to international standards in the area of human rights and personal data protection are not sufficiently elaborated. This is a gap which shall be filled by European Commission when conducting periodical review or issuing adequacy decisions towards next countries.

EC rightly points out that considering the different approaches to data protection in third countries, the adequacy assessment should be carried out, and any decision should be made and enforced in a way that does not arbitrarily or unjustifiably discriminate against or between third countries where like conditions prevail, nor constitute a disguised barrier to trade, regard being had to the Community's present international commitments (COM 2017).

While assessing the adequacy of a given country, EC shall take into consideration opinion of European Data Protection Board (EDPB). To ensure that the decision is in line with EDPB approach, EC should respect guidance and recommendations acquired by this body.

4. EUROPEAN DATA PROTECTION BOARD ON ADEQUACY

The EDPB has not provided comprehensive guidelines on the meaning of 'adequacy' and factors which shall be considered when determining the model. However, EDPB has acquired (European Data Protection Board 1/2018) Adequacy Referential adopted by Article 29 Working Party in 2017 (WP 254 rev.01). This document shall serve as a basic for further discussion in this area, unless EDPB decides to release new guidelines in this area. Importantly, this is the only document in European Union which comprehensively discussed this issue (Panek, 2024). Therefore, EC decisions in great extent rely on the findings contained therein (Panek, 2024).

Article 29 Working Party in its guidelines emphasized the Schrems I ruling and the fact that data protection model in the given country shall not "mirror point by point the European legislation, but to establish the essential – core requirements of that legislation" (WP 254 rev. 01). European Commission shall not only consider the law which is binding in the country or organisation, its content, rights provided towards individuals and obligations imposed on actors processing personal data but more importantly, enforcement and applicability of law. EC shall be particularly interested in "effectiveness of agreed rules, the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence, and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organization has entered into (with the special attention given to EU Charter on Fundamental Rights, GDPR and Convention 108+)" (WP 254 rev. 01). According to Article 29 Working Party this is crucially important to consider the legal framework for the access of public authorities to personal data. In general, Article 29 Working Party emphasized that the assessment shall include two major components: the merits of data protection laws (i.e. rights granted to individuals and general rules) and the enforcement mechanisms (together with independent supervisory authority) (Wolf, 2014).

. The list of adequacy criterions includes::

1) Content principles:

[7] This approach is quite reasonable considering the great autonomy of states in given countries and a possibility of them to develop their own data protection laws which may allow different standards (which in general shall not be lower than this guaranteed by constitution of these countries).

- Existence of basic data protection concepts/principles
- Grounds for lawful and fair processing for legitimate purposes
- The purpose limitation principle
- The data quality and proportionality principle
- Data Retention principle
- The security and confidentiality principle
- The transparency principle
- The right of access, rectification, erasure, and objection
- Restrictions on onward transfers

2) Additional principles covering specific types of processing:
   - Tighten rules on processing special categories of personal data
   - Specific rules for direct marketing
   - Enhanced rules for automated decision making and profiling;
3) Procedural and enforcement mechanisms
   - Competent independent supervisory authority
   - Implementing mechanisms guaranteeing a good level of compliance with data protection laws
   - Accountability principle
   - Support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms.

All these principles shall be followed and implemented with the respect towards legal system in each country.

Article 29 Working Party expressed special attention to essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights and suggested certain principles which shall be followed. Even though these basic rules seem to be like general ones, the real question is how strong mechanisms are in place to prevent infringements committed by public authorities. In its guidelines Article 29 Working Party refers a lot to CJEU judgement in *Schrems I* case. This requires further consideration which are made in the next parts of this paper. Article 29 Working Party has also released several opinions on the adequacy of data protection model in specific countries. They describe the shortcomings of given legislation and point out to such issues as comprehensiveness of regulations, publicly available data, use of data for direct marketing or onward transfer (Hughes, 2001).

Importantly, the guidance provided by Article 29 Working Party which was later acquired by EDPB do not focus on human rights nor rule of law. Moreover, sadly these guidelines do not highlight enough that the assessment of privacy frameworks shall be conducted considering the constitutional model of given country, which may differ from European countries. This also seems that the guidance is based on very liberal, extensive and purposive interpretations of adequacy criteria and they go beyond the literal meaning of what was stated in directive 95/46/WE and then repeated in GDPR.

European Data Protection Board also released Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, and even though Recommendations relate to different legal act, EDPB considerations towards adequacy are also applicable under GDPR. In its guidance the EDPB clarifies that it considers essential equivalence also applicable for the context of the LED. For the EDPB this concretely means that for a third country or an international organisation to achieve adequacy under the LED they have to 'establish the essential - core requirements' of EU data protection law interpreted in light of the Charter, but do not need to 'mirror point by point the EU legislation' (Recommendations 01/2021). This can be achieved according to the EDPB 'through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies' (Drechsler, 2021).

5. CJEU ON THE ADEQUACY OF DATA PROTECTION MODEL

Apart from adequacy decisions released by European Commission, also CJEU tried to interpret the term "adequate" under European law in two separate rulings[8].

In the *Schrems I* case, CJEU has rightly pointed out that the directive 95/46 did not provide a definition of "adequate" term (and unfortunately the same has been repeated in the GDPR-author). However, the court stated that to achieve an adequate standard of data protection "a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order" (*Schrems I*). Moreover, this third country does not have to use "the same means as those employed within the European Union in order to ensure that the requirements stemming from directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union" (*Schrems I*). CJEU rightly stated in Schrems I, that "content of any regulation thriving to provide adequate data protection shall be assessed considering domestic and international commitments and the practice designed to ensure compliance with those rules, since it must, take account of all the circumstances surrounding a transfer of personal data to a third country. The obligation stated in art 25(6) directive 95/46 implemented the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion (Bot 2015), is intended to ensure that the high level of that protection continues where personal data is transferred to a third country" (*Schrems I*).

Advocate General further states that "a third country ensures an adequate level of protection only where, following a global assessment of the law and practice in the third country in question, it can establish that that third country offers a level of protection that is essentially equivalent to that afforded by the directive" (AG in C-362/14*)* (more broadly: EU data protection model – author). According to Advocate General, "while assessing the adequacy of data protection in a third country or organisation, European Commission shall consider two factors: the content of the applicable rules and the means of ensuring compliance with those rules" (AG in C-362/14). With self-certification mechanisms such as Safe Harbour, Privacy Shield or Privacy Framework, this is crucial to ensure that there are sufficient control mechanisms.

From the *Schrems I* case it is clear that the assessment of adequacy of data protection model shall be conducted with respect towards legal order and constitution of the third country. EU does not have competence to impose changes in the regulatory model or constitution of the third country (unless this third country is in the procedure of accessing to the Union and such changes are required for this country to be able to sign the Charter and the Treaties). The Court seek to establish the concept of "essential equivalence" which was furtherly included in Recital 104 GDPR. The "essential equivalence" relates to the model of personal data protection in third country, which even though may differ from EU order, but in principles shall be adhered to GDPR and other data protection laws in European Union. Unlike EC in its decisions and EDPB in its guidelines, CJEU indirectly takes attempts to assess the question of the rule of law in given country, but in discussed rulings – only in relation to surveillance mechanisms. This is due to the nature of the proceedings conducted by this court and the way they are bind by the questions raised by the initiating court.

From the perspective of application, the adequacy decision, it is crucial to mention that the Member States and their bodies, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be

[8] It shall be noted that in joined cases C-317/04 and C-318/04 CJEU restrained from trying to define what "adequate" means even though it annulled decision of Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (CJEU C-317/04 and C-318/04).

lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (C-475/01).

CJEU ruling in *Schrems I* as well as opinion of Advocate General emphasize the need to ensure the constant monitoring of third country laws and timely re-assessment of the decision taken by Commission considering changing circumstances and legal landscape. This approach has been reflected in GDPR by article 45 and an obligation to monitor developments in the given country and a need to include mechanism for periodic reviews in the decision itself.

After invalidating Safe Harbour, European Commission made another attempt to recognize US as providing adequate level of protection under Privacy Shield mechanism. This another self-certified programme was supposed to answer doubts raised in Schrems I ruling and simplify data transfers between EU member states and US. In 2020 CJEU found Privacy Shield mechanism invalid under Schrems II (C-311/18). The court ruled that the Privacy Shield failed to provide an adequate level of protection for EU citizens' personal data citing concerns over extensive U.S. surveillance practices and the absence of effective redress mechanisms for EU citizens. CJEU stated that "although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term 'adequate level of protection' must, as confirmed by recital 104 of that regulation, be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph would be undermined" (C-311/18).

Under *Schrems II* it has been made clear that one of the factors implicating the adequacy of data protection model is existence and applicability of redress mechanisms. However, this is not sufficient to provide the redress mechanism by law, the supervisory authority who is obliged to respond to claims shall be independent and ensure that the law is being implemented in comprehensive, effective, and unilateral way.

6. CONTROVERSIES

Deconstruction of the term "adequacy" requires to firstly look at the reasons why such strong transfer mechanisms have been implemented in GDPR. One of them is ensuring security of personal data of EU citizens even if they are processed outside Europe, especially with third countries authorities accessing this data (Naef, 2021). This is not about the security of personal data per se or respect for individuals' rights. This is also a matter of national/EU security; hence this is highly unlikely that EC will grant adequacy decision to a country with which EU does not keep international relations or these relations are particularly tense (i.e., China, Russia). However, in recent years EU bodies have been focused on questioning of personal data protection model of its allies (such as US, Brazil, Canada) rather than countries such as Russia or China in which personal data originating from EU is also processed.

Outside EU, the concept of "adequacy" and stringent data transfer mechanisms have been criticized for prioritizing economic protectionism over fundamental rights. In the US these measures are often perceived as efforts to disadvantage American companies (Obama, 2015). In fact, such statements are contradictory to the general principles of EU Digital Agenda, but may have valid impact on the practice of transfer of certain services and free trade (Velli, 2019). On the other hand, this is clear from EC adequacy decisions and Article 29 Working Party guidelines that criterions relating to human rights and rule of law are not sufficiently elaborated and are treated as a side thread. The focus of these institutions is on the merits and substantial aspects of personal data protection model, not even necessarily, its enforcement. This is CJEU who steps in and tries to additionally elaborate on the rule of law, focusing on the mechanisms guaranteeing respect towards data subjects' rights, including existence of independent supervisory authority.

The case of US adequacy decision also has shown that CJEU and other EU bodies tend to require higher standards from third countries than EU Members States. US data protection model has been vastly criticized due to

lack of independent supervisory authority and broad surveillance. These problems are also clearly visible in EU Member States. Independency of data protection authorities is questioned in Poland and Hungary (due to tight connections of DPAs with governments) and Ireland (which has been accused of business having broad influence on conducted investigations). The use of surveillance tools in Poland and France have been broadly criticized in European Union. Neither of these issued gained as much attention as lack of supervisory authority and surveillance methods in US.

Some authors also point out that EU bodies require higher standards that those established on international level (Wolf, 2014). Even if this is factually correct, this is difficult not to notice that international standards in this regards have been established before new threats in the area of personal data protection occurred. EU legislation is one of the newest and does take into account the challenges imposed by new technologies (clouds, surveillance, AI, big data, behavioural profiling and others). Also, there is no doubt that EU traditionally is driven by human-centric approach and does place fundamental rights and freedoms at the centre of its regulations, even at the cost of business and economic growth. By the powers granted to EU by Member States, this organisation is competent to establish whatever standard in the area of personal data protection it wants, but this comes at some costs – i.e. weakening of trade and political relations between the EU and other countries. It is obvious that this is a question of balancing the benefits and risks and making a conscious decision whether the Union wants to continue to appear as a stronghold of rights and freedoms, which is associated with losing the race for economic leadership.

This is European Commission which shall, especially in its decisions focus more on defining the term of "adequacy", as this is the only body who has a power to decide on which country or territory is adequate (Mednis, 2023). So far, EC hardly ever touches the "core" of the data protection model in each country and the assessment often looks like ticking the boxes, rather than deep-dive analysis. What is also missing in the existing decisions is analysis of the standards in human rights protection. I'm not saying that EC shall conduct full assessment on this part, but surely can rely on reports and analysis of independent organisations such as United Nations, Amnesty International and others.

European Commission should not rush to issue adequacy decisions under external pressure. Data controllers have alternative transfer mechanisms available, ensuring continuity even in the absence of an adequacy decision. The assessment of a country's data protection framework must be meticulous, evidence-based, and transparent. Ultimately, the reliability and legal certainty of an adequacy decision are far more valuable than the speed of its issuance.

5. SUMMARY

The "adequacy" requires third countries to generally follow EU data processing principles and ensuring its enforcement by independent supervisory authority. The adequacy aims to ensure that basic fundamental rights (such as right to privacy) are protected. The country which is being recognized as adequate shall 1) have binding law in place (either at the level of constitution or statutory law guarantying right to privacy and data protection not only to its citizens but also other individuals who are permanently or temporarily under its jurisdiction; 2) prove the general respect towards human rights; 3) ensure that independent supervisory authorities is equipped with powers and resources to oversee processing of personal data in the country. Country which is being considered as "adequate" does not need to have same data subject rights and same procedural mechanisms in place, but definitely needs to grant a right to re-dress to individual. Basic data processing principles shall be adhered to (such as data minimisation, proportionality, transparency, and accountability) regardless of whether processing is conducted by public of private entity.

This paper has demonstrated that the European Union's approach to adequacy decisions under GDPR lacks a consistent legal standard, leading to legal uncertainty for businesses and policymakers. By comparing adequacy findings across various bodies, it is evident that the EU applies stricter scrutiny to some countries (e.g., the US)

while granting adequacy to others with similar or weaker privacy frameworks. This inconsistency raises concerns about whether adequacy assessments are legally grounded or politically motivated.

When assessing adequacy European Commission shall put more attention on the general respect towards human rights in given country. Personal data protection is meaningless if not supported by the right to fair trial, freedom of expression and freedom of information. Additionally, the process of adopting adequacy decision shall in the broaden extent involve NGOs and activists to incorporate their findings in the decision process. The given process shall be fully transparent, including ensuring public access to Commission deliberations. European Commission shall also develop a standardized adequacy assessment framework with clear, measurable criteria.

ACKNOWLEDGEMENTS

1) The author used ChatGPT to clarify and simplify wording in the Introduction and Summary sections, by prompting the tool to suggest language corrections of the draft of the paper (OpenAI. (2025). ChatGPT (Jan 15 version) [Large language model].
2) This research was funded in whole by National Science Centre PRELUDIUM 20, NO. 0209/0037/22, registration no: 2021/41/N/HS5/03225, contract no: UMO-2021/41/N/HS5/03225. For the purpose of Open Access, the author has applied a CC-BY public copyright licence to any Author Accepted Manuscript (AAM) version arising from this submission.

REFERENCES

Advocate General Bot. (2015, September 23). *Opinion in Case C-362/14, Maximillian Schrems v. Data Protection Commissioner*. Court of Justice of the European Union.

Article 29 Working Party. (2017, November 28). *Adequacy referential*. https://ec.europa.eu/newsroom/article29/items/612080

Calia, D. (2022). Schrems II: The EU's influence on U.S. data protection and privacy laws. *Washington University Global Studies Law Review, 21*(2), 247–272.

Charter of Fundamental Rights of the European Union, O.J. C 326 (2012, October 26).

Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)* (as amended by Convention 108+).

Court of Justice of the European Union. (2004, October 5). *Commission v. Greece, C-475/01*. E.C.R. I-0000.

Court of Justice of the European Union. (2006, May 30). *Joined Cases C-317/04 and C-318/04*. E.C.R. I-0000.

Court of Justice of the European Union. (2015, October 6). *Schrems v. Data Protection Commissioner, C-362/14*. E.C.R. I-0000.

Dahl, K. (2019). *Data adequacy and China - The possibility of an adequacy decision adopted on China in accordance with the GDPR Article 45*. University of Bergen. https://bora.uib.no/bora-xmlui/handle/1956/21714.

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.

Drechsler, L. (2021a). EDPB issues guidance on personal data transfers based on adequacy decisions in the context of the Law Enforcement Directive. *European Data Protection Law Review, 7*(2), 221–227.

Drechsler, L. (2021b). Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context. *International Data Privacy Law, 11*(3), 182-195.

Duque de Carvalho, S. L. (2019). Key GDPR elements in adequacy findings of countries that have ratified Convention 108. *European Data Protection Law Review, 5*(1).

European Commission. (2002/2/EC). Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, O.J. L 6.

European Commission. (2003/490/EC). Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC on the adequate protection of personal data in Argentina, O.J. L 168.

European Commission. (2003/821/EC). Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey, O.J. L 308.

European Commission. (2004/411/EC). Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man, O.J. L 181.

European Commission. (2008/393/EC). Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC on the adequate protection of personal data in Jersey, O.J. L 159.

European Commission. (2010/146/EU). Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC on the adequate protection provided by the Faeroese Act on processing of personal data, O.J. L 71.

European Commission. (2010/625/EU). Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC on the adequate protection of personal data in Andorra, O.J. L 281.

European Commission. (2011/61/EU). Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC on the adequate protection of personal data by the State of Israel about automated processing of personal data, O.J. L 27.

European Commission. (2013/65/EU). Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC on the adequate protection of personal data by New Zealand, O.J. L 28.

European Commission. (2017). *Communication from the Commission to the European Parliament and the Council: Exchanging and protecting personal data in a globalised world* (COM(2017) 7 final).

European Commission. (2019/419). Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, O.J. L 76/1.

European Data Protection Board. (2018). *Endorsement 1/2018*. https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf

European Data Protection Board. (2021). *Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive*. https://edpb.europa.eu

European Data Protection Board. (2023, July 10). *Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision*. https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-transfers-under-gdpr-united-0_en

General Court of the European Union. (2023). *Philippe Latombe v. European Commission, T-553/23 R* (pending).

Gonzalez Domenech, J. (2019). Las decisiones de adecuación en el derecho Europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros. *Cuadernos de Derecho Transnacional, 11*(1), 350–371.

Hamilton, D., & Quinlan, J. (2020). *The transatlantic economy 2020: Annual survey of jobs, trade and investment between the United States and Europe*.

Hughes, A. (2001). 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, 25*(1), 270-276.

Ihle, J. (2010, July 8). Ireland blocks EU data sharing with Israel. *Jewish Telegraphic Agency*. https://www.jta.org/2010/07/08/global/ireland-blocks-eu-data-sharing-with-israel.

Mednis, A. (2023). Kryteria uznawania odpowiedniego stopnia ochrony danych osobowych w państwie trzecim. In M. Sakowska-Baryła (Ed.), *Transfer danych osobowych na podstawie RODO* (pp. 115–133). Warszawa: Wydawca.

Murphy, H. M. (2021). Assessing the implications of Schrems II for EU–US data flow. *International & Comparative Law Quarterly*. Advance online publication. https://doi.org/10.1017/S0020589321000348.

Naef, T. (2021). *Data protection without data protectionism: The right to protection of personal data and data transfers in EU law and international trade law*. Springer.

noyb. (2023). *New trans-Atlantic data privacy framework largely a copy of "Privacy Shield". noyb will challenge the decision*. https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

Panek, W. (2024). People's Republic of China and the adequacy – Why Chinese data protection law is not adequate within the meaning of the GDPR. *Masaryk University Journal of Law and Technology, 2*, 143-167.

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), O.J. L 119/1.

Schwartz, P. M. (2019). Global data privacy: The EU way. *New York University Law Review, 94*(3), 771–817.

Swisher, K. (2015, February 13). *Kara Swisher interviews President Barack Obama on cyber security, privacy and his relationship with Silicon Valley*. Re/code.

Velli, F. (2019). The issue of data protection in EU trade commitments: Cross-border data transfers in GATS and bilateral free trade agreements. *European Papers, 4*(3), 881–894.

Wolf, J. (2014). Delusions of adequacy - Examining the case for finding the United States adequate for cross-border EU-U.S. data transfers. *Washington University Journal of Law & Policy, 43*, 227-257.