


Uncertain future of transatlantic data flows: Will the United States ever achieve the ‘adequate level’ of data protection?

ASLI ALKIŞ-TÜMTÜRK* 

Institute of Comparative Law, University of Szeged, 13 Dugonics square, 6720 Szeged, Hungary

ORIGINAL RESEARCH PAPER

Received: February 27, 2022 • Accepted: April 25, 2022

Published online: December 6, 2022

© 2022 The Author(s)



ABSTRACT

Personal data can be transferred to third countries without any additional measures by achieving the European Commission’s adequacy decisions if the third country’s data protection level is deemed essentially equal. Only a few countries have obtained this decision, and the United States is no longer one of them, since the European Court of Justice ruled in the *Schrems II* case that the Privacy Shield Decision could not provide ‘essentially equivalent’ protection for personal data to that provided by European Union legislation, and hence was invalid. This article will discuss what the term ‘essentially equivalent’ means and what it covers. Finally, it will examine and attempt to answer the question of whether the United States will ever reach the mentioned adequate level by comparing the examples of two adequate countries, the United Kingdom and Japan.

KEYWORDS

GDPR, Privacy Shield, adequacy decision, data transfer to third countries, UK-GDPR, APPI (Act on the protection of personal information)

* Corresponding author. E-mail: alkisasli@gmail.com

1. INTRODUCTION

Personal data protection and privacy are both fundamental rights in the European Union (EU).¹ The result of a long decision-making process of the EU, a broad-reaching data protection regulation, the GDPR has been adopted not only to strengthen data protection rights of EU residents and citizens, but also to regulate free flows of personal data.² As it is stated in the Recital 101 of the GDPR: ‘Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation.’³ However, data transfer to third countries is only allowed if the third country ensures an adequate level of protection and has been approved by the European Commission (the Commission), as defined in Article 45 of the GDPR.⁴

In contrast to the EU, in the United States (US), personal data and privacy are considered as a commercial commodity.⁵ Another significant difference between the EU and US privacy approaches is that the EU takes an omnibus approach, which means that an umbrella law attempts to protect all potential personal data abuses and violations by broadly defining data subjects, data controllers, data subjects’ rights, and data controllers’ obligations. This umbrella legislation also grants EU citizens and residents a privilege known as ‘extraterritoriality,’ which implies that EU data subjects can enjoy data protection wherever they travel or their data flows.⁶

Unlike the EU, the United States approaches privacy regulation on a sectoral basis. This method enables the United States to enact highly targeted legislation that addresses the privacy concerns of a specific industry sector. This provides a great level of flexibility in privacy legislation, as one industry defines its safeguards differently from those dealing with another sector. However, certain data or firms can simply go unregulated in this system if no sector covers them. Moreover, each state in the United States has a distinct standard for data protection.⁷

Despite the fact that the US is the EU’s largest trading partner,⁸ it has not reached a sufficient level of protection in current history, due to fundamental differences in data protection and privacy approaches between the two jurisdictions. The US received partial adequacy with the Privacy Shield’s ancestor Safe Harbour⁹ in 2000; however, it was invalidated in the *Schrems I* case by the European Court of Justice (CJEU) in 2015.¹⁰ Afterwards, the Privacy Shield entered into force in 2016,¹¹ however, it did not last so long as its predecessor and was invalidated in 2020 by the CJEU in the *Schrems II* case.¹²

¹Charter of Fundamental Rights of the European Union [2010] OJ C 83/389, Article 7-8.

²General Data Protection Regulation [2016] OJ L 119/1, art 1(1) and (2).

³GDPR, rec 101(1).

⁴GDPR, art 45(1).

⁵Schwartz and Peifer (2017) 132–37 cited in Schwartz (2019) 771, 773.

⁶Ivers (2021) 2586–88.

⁷Ivers (2021) 2589–91.

⁸European Commission (6 September 2021).

⁹US-EU Safe Harbour [2000] OJ L 215/7.

¹⁰Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650.

¹¹EU-U.S. Privacy Shield [2016] OJ L 207/1.

¹²Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* EU:C:2020:559.



Only a few countries have been deemed adequate thus far, due to the difficulty of meeting the EU's adequacy criteria. The criteria require that processing be based on clear, precise, and accessible rules, that it be necessary and proportional to the purpose for which the data is collected, that it be subject to independent oversight mechanisms, and that effective remedies be available to individuals in the event of a violation by public authorities.¹³ In this article, we will discuss Japan, the first country to receive an adequacy decision under the GDPR, as well as the United Kingdom (UK), which received an adequacy decision recently following Brexit.

Japan's adequacy decision was chosen, because Japan's data protection and privacy approach is similar to the US and thus its adequacy decision can serve as a model for the US to have two-way data protection. One way, which is the current situation, may remain for US citizens and residents, while the other way, which includes stricter rules and effective oversight and redress mechanisms, may be adopted only for EU citizens and residents, particularly in the case of access to personal information by public authorities.¹⁴

The UK could be also a good example, because the UK's intelligence services and mass surveillance remain a concern for the EU, as they were the biggest issue for the US. However, the UK still received the adequacy decision due to its effective oversight and redress mechanisms, and it has gained trust through ratification of the [Council of Europe's Convention 108+](#)¹⁵ and the European Convention on Human Rights,¹⁶ which will be discussed in detail in the following chapters. Therefore, the UK's adequacy decision can serve as a model for the US to access the [Convention 108+](#) in order to establish trust within the EU and as a first step toward an effective oversight mechanism and remedies for European data subjects.

Accordingly, the history of the Privacy Shield and the invalidation process will be presented in this paper, and the essentially equivalent term mentioned in the *Schrems II* case will be interpreted. After clarifying what is essentially equivalent, we will examine and compare the concrete examples that are essentially equal to the GDPR's data protection and privacy approach. In conclusion, we will attempt to determine if one of the examples, or a combination of them may serve as a model for the US in obtaining an adequacy decision from the Commission.

Moreover, European Commission and the United States recently announced that they have reached a new agreement in principle on a joint statement on the Trans-Atlantic Data Privacy Framework on March 25, 2022. This new framework attempts to address the shortcomings of the Safe Harbour and Privacy Shield frameworks.¹⁷

In this article, we will examine whether the United States will achieve an appropriate level of data protection under this new framework, as well as what should be done to avoid *Schrems III*.

¹³Article 29 Working Party [2016] 16/EN WP 237 in Article 29 Data Protection Working Party [2018] 18/EN WP 254 rev01, Chapter 4, 9.

¹⁴Wang (2020) 691.

¹⁵Council of Europe (2018).

¹⁶ECHR (as amended by Protocols Nos. 11, 14 and 15).

¹⁷European Commission (25 March 2022). For more information: [European Commission \(25 March 2022a\)](#).



2. TRANSATLANTIC DATA FLOWS IN RECENT HISTORY: EU-US PRIVACY SHIELD

The US has not provided this adequate level of protection so far, but under the Privacy Shield agreement, they received a partial adequacy decision from the Commission on 12 July 2016. In other words, companies could only be deemed adequate, if they committed to self-certification in accordance with the Privacy Shield principles.¹⁸ The framework included seven principles: notice, data integrity and purpose limitation, choice, security, access, recourse, enforcement and liability, and accountability for onward transfer.¹⁹ Consequently, if US companies followed the principles of the Privacy Shield framework and registered their certification, they could achieve the adequate level and would be able to transfer European data subjects' data from the EU to the US without any further steps, as specified in Article 45.²⁰

As of June 2020, 5,211 companies were self-certified under the Privacy Shield, and according to a report from the US Department of Commerce in September 2019, 70% of the self-certified companies were small and medium-sized enterprises (SMEs). As a consequence, Privacy Shield-type frameworks are very beneficial for SMEs, because they do not require any additional procedures to be adequate and hence are less costly as compared to alternative complicated and expensive legal transfer options like as standard contractual provisions (SCCs).²¹ Nevertheless, in the absence of adequacy decisions, companies should search for other options, including as appropriate safeguards, as indicated in the GDPR.²² SCCs are the most widely used of these safeguards, but they need case-by-case assessment, which makes them challenging for SMEs

¹⁸EU-US Privacy Shield [2016] OJ L 207/1, para 14.

¹⁹EU-US Privacy Shield [2016] OJ L 207/1, para 19 et seq.

Notice: Organisations are obliged to provide information to data subjects on a number of key elements relating to the processing of their personal data (e.g., type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability).

Choice Principle: Where a new (changed) purpose is materially different but still compatible with the original purpose, this principle gives data subjects the right to object (opt out).

Data Integrity and Purpose Limitation: Personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended use, accurate, complete, and current.

Security Principle: Organisations creating, maintaining, using or disseminating personal data must take 'reasonable and appropriate' security measures, taking into account the risks involved in the processing and the nature of the data.

Access Principle: Data subjects have the right, without need for justification and only against a non-excessive fee, to obtain from an organisation confirmation of whether such organisation is processing personal data related to them and have the data communicated within reasonable time.

Recourse, Enforcement and Liability Principle: Participating organisations must provide robust mechanisms to ensure compliance with the other Principles and recourse for EU data subjects whose personal data have been processed in a non-compliant manner, including effective remedies.

Accountability for Onward Transfer Principle: Any onward transfer can only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group and (iii) only if that contract provides the same level of protection as the one guaranteed by the Principles, which includes the requirement that the application of the Principles may only be limited to the extent necessary to meet national security, law enforcement and other public interest purposes.

²⁰GDPR, art 45(1).

²¹Cory, Castro and Dick (2020) 5–6.

²²GDPR, art 46.



with limited resources and experience.²³ In this paper, we will not focus on the relevant safeguards and current remedies to the lack of adequacy decision issue, but rather on the topic of whether the US will achieve an adequate decision and how it will vary from its predecessors.

Although it is very useful to get an adequacy decision for the third countries, it is not easy to pass the assessment test for the adequate level of the protection under the GDPR. Due to this, the Commission has found just a few countries sufficient thus far: Andorra, Argentina, Canada (partial adequacy), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay. The US is no longer one of them.²⁴

2.1. Invalidation of the Privacy Shield: Schrems II

Maximillian Schrems, an Austrian lawyer, and privacy activist has been a Facebook user since 2008 and filed a complaint with the Irish supervisory authority about the transfer of his personal data from Facebook Ireland to Facebook Inc. in the US. He sought to prohibit the transfer of his personal data to the US, claiming that they do not provide an adequate level of protection against public authorities' access to EU data subjects' personal data transferred to that country. The Irish supervisory authority brought the case to the High Court in order to have questions referred to the Court of Justice (CJEU). Hence, the High Court questioned the CJEU whether the Privacy Shield was invalid.²⁵

The CJEU examined the *Schrems* case and decided that the US intelligence services' surveillance was not limited to what was necessary and was not limited and proportional as required by EU law, that effective and actionable judicial redress was not available for EU data subjects under US legislation, and that the independent Ombudsperson mechanism was not working as it should have, because the Ombudsperson did not adopt any decision that were binding on the US intelligence services. Finally, for the reasons stated above, the CJEU ruled in the *Schrems II* judgement that the Privacy Shield did not provide an 'essentially equivalent' level of protection and so deemed it invalid.²⁶

2.2. Agreement on the new Trans-Atlantic Data Privacy Framework: Schrems III in the making?

An adequacy decision for both the EU and the US will always be needed because the US is one of the EU's largest trading partners. According to Eurostat data, 'In 2021, the United States was the largest partner for EU exports of goods (18.3%) and the second largest partner for EU imports of goods (11.0%)'.²⁷ The EU has previously recognized that its judgments on adequacy with the US were based on the grounds that they are 'important trading partners'.²⁸

²³Cory, Castro and Dick (2020) 6.

²⁴European Commission (13 January 2018).

²⁵Court of Justice of the European Union, 'Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems' (16 July 2020) Press Release No 91/20, 1–2.

²⁶Court of Justice of the European Union, 'Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems' (16 July 2020) Press Release No 91/20, 2–3.

²⁷Eurostat (2022).

²⁸European Commission (2017).



Accordingly, it was recently reported in March 2022 that the European Commission and the United States had achieved an agreement in principle on a joint statement on the Trans-Atlantic Data Privacy Framework. This new framework tries to improve the inadequacies of its predecessors, the Safe Harbour and Privacy Shield frameworks. Based on the new framework, data will flow freely and securely between the EU and the US; access to data by intelligence services in the US will be limited to what is proportionate and necessary for national security; the Data Protection Review Court will establish a new two-tier system for redress mechanisms for EU complaints; and self-certification of companies will continue with strict obligations; and lastly there will be specific monitoring and review mechanisms.²⁹

Based on the new framework attempt, it can be concluded that the third Trans-Atlantic adequacy decision will also reach a partial adequacy decision because not the entire US jurisdiction will be deemed adequate, but self-certifying companies will be deemed adequate based on their compliance with the required principles of the new framework through the US Department of Commerce. Furthermore, Max Schrems reacted to this new framework by stating that the US does not appear to improve anything in its surveillance law, but rather they are promising reassurances with ambiguous terminology such as ‘proportionate’ access. He mentioned that they have previously attempted to be proportional and failed twice in the *Schrems I* and *Schrems II* cases.³⁰

Besides, the surveillance law and intelligence services were one of the main reasons for the US failing to achieve an adequate level of data protection and the Data Protection Review Court is unlikely to have an impact on the US surveillance system. Moreover, self-certified companies will be unable to change this system while adhering to the principles of the new framework, just as they were unable to change while the Safe Harbour and Privacy Shield were valid. Lastly, the stated specific monitoring and review mechanisms remain unclear. Given all of the aforementioned, can we conclude that *Schrems III* is only a question of time?

To avoid falling into the same trap, the United States should obtain essentially equivalent levels of protection rather than expecting this level of protection from participating US companies. Because ensuring this level of protection appears to be achievable only for the government and not for some companies.

2.3. What is ‘essentially equivalent’ level of protection?

Since in the *Schrems II* judgement there is no guidance regarding the term ‘essentially equivalent’ level of protection, it should be sought to be determined by looking at previous EU guidelines.

The Working Party of EU Data Protection Authorities (the WP29) aimed to provide guidance to the Commission and third countries or international organizations on assessing the level of data protection in a third country in order to ensure essential equivalence with the GDPR through the transfers of personal data from the EU: applying Articles 25 and 26 of the EU

²⁹European Commission (25 March 2022). For more information: European Commission (25 March 2022a).

³⁰Schrems (2022).



Data Protection Directive (WP12)³¹ and its revised version Adequacy Referential (WP254 rev01).³²

The following essential and core content and enforcement principles should be present in the legal systems of third countries or international organizations to ensure the essentially equivalent level of protection according to WP12 and WP254 rev01. There should be fundamental data protection concepts in place. They should not be the same as the GDPR's principles, but they should be compatible with the GDPR's notions (e.g.: personal data, sensitive data, data subject, data controller, data processor, processing of personal data). The legal basis for data processing should be identified, such as consent of a data subject, performance of a contract, or a data controller's legitimate interest. The processing should be confined to what it was meant to be at the time the data was collected. The information should be current, accurate, and proportionate. In other words, processing should not go beyond what is required. The data controller should not keep the data for any longer than is absolutely necessary. Data controllers should ensure the security of collected and processed data using technical and organizational means that take current technological developments into account. Except for the circumstances stated in GDPR Article 23, data subjects shall be notified about all aspects and processes of data processing in a transparent and easily accessible manner. The data subject shall have the right to be informed about his or her data processing, to have it corrected if it is inaccurate, and to object to the processing of data relating to them. Exemptions from the right to object can also be found in Article 23. Onward transfers should be restricted to third countries that also have an adequate level of protection.³³

Additional rules should exist to apply to certain types of data, such as sensitive data, data acquired for direct marketing, automated decision making, and profiling. To process these specific types of data, certain requirements should be met, such as obtaining explicit consent from the data subject, and the data subject shall not be charged for exercising his/her right to object at any time regarding these specific data.³⁴

In terms of procedural principles, the third country should have an independent supervisory authority in place to ensure and monitor compliance with data protection and privacy rules. Third countries should maintain a high degree of compliance with their data controllers and data processors, ensuring that they are accountable for their obligations ('such measures may include for example data protection impact assessments, the keeping of records or log files of data processing activities for an appropriate period of time, the designation of a data protection officer or data protection by design and by default'³⁵), and that data subjects are aware of their rights. Independent data protection officials and agencies should play a critical role in providing an efficient legislative framework and implementing dissuasive sanctions. Lastly, data subjects should have access to effective administrative and judicial recourse in case their personal data is processed in a manner that does not comply with the rules. Compensation for damages should

³¹Working Party [1998] DG XV 1998 D/5025/98 WP12.

³²Article 29 Data Protection Working Party [2018] 18/EN WP 254 rev01.

³³WP 254 rev01, Content principles, 5–7.

³⁴WP 254 rev01, Examples of additional content principles to be applied to specific types of processing, 7.

³⁵WP 254 rev01, Accountability, 8.



be offered for them, as should sanctions for data controllers who do not comply with the requirements when necessary.³⁶

WP29 also provides a guideline consisting of four essential guarantees for third-country surveillance by public authorities in order to be deemed adequate:

- 1) Processing should be based on clear, precise and accessible rules (legal basis); 2) Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated; 3) The processing has to be subject to independent oversight; 4) Effective remedies need to be available to the individuals.³⁷

Furthermore, all the above elements should be considered in combination with Articles 7 and 8 of the EU Charter of Fundamental Rights, which address the respect for private and family life as well as the protection of personal data.³⁸

Taking into account the CJEU's decision in *Schrems II*, it appears that the US did not take these WP29 guidelines into consideration, because public authorities' surveillance was not proportional, there were no effective legal remedies for EU data subjects, and there was no independent oversight mechanism, such as an independent Ombudsperson. These recommendations should be taken into account for the upcoming Trans-Atlantic data privacy framework.

Last, but not least, as stated in Recital 105 of the GDPR, ratification of Convention 108, the first legally binding international agreement specifically addressing the protection of personal data, would be an important factor in the Commission's adequacy assessment.³⁹ However, the US has not accessed this Convention, and it would be a significant step forward if it has accessed to the treaty in the near future.

3. TWO EXAMPLES FOR ADEQUATE COUNTRIES: JAPAN AND THE UNITED KINGDOM

In this chapter, it will be attempted to address the issue of whether the United States has a possibility of being an adequate country in the future by comparing Japan's and the United Kingdom's adequacy decisions.

3.1. EU-Japan adequacy decision

Due to fundamental differences between the APPI⁴⁰ and the GDPR, Japan's Act on the Protection of Personal Information (APPI) failed the adequacy test solely based on its text,

³⁶WP 254 rev01, Procedural and Enforcement Mechanisms, 8.

³⁷Working Party [2016] 16/EN WP237 in Article 29 Data Protection Working Party [2018] 18/EN WP 254 rev01, 9.

³⁸CFR, art 7–8 in WP254, Chapter 1: Some broad information in relation to the concept of adequacy, 3.

³⁹GDPR, rec 105.

⁴⁰Personal Information Protection Commission, Amended Act on the Protection of Personal Information (Tentative Translation) (June 2020) 1–49.



necessitating the adoption of Supplementary Rules issued by Japan's Personal Information Protection Commission (PPC) that apply only to personal data transfers from the EU to Japan.⁴¹ Nevertheless, Japan was the first country to get an adequacy decision on 23 January 2019 under the GDPR, and we picked this case specifically to grasp how a country might become 'GDPR-adequate'.⁴²

The approach to data protection and privacy is the most significant difference between both legislations. The EU considers privacy and data protection to be fundamental rights, and privacy is not a commodity. On the other hand, unlike the EU, Japanese legislation emphasizes the importance of personal information as an economic commodity, resulting in a weaker protection for personal data when compared to EU data protection. The EU, for example, protects potentially identifiable information such as IP addresses and cookie IDs, whereas Japan solely protects identifiable individual information.⁴³

We may deduce from this fundamental difference in privacy concepts that the data protection legislations of Japan and the EU differ culturally in many cases. However, essentially equivalent does not imply that the laws should be identical, but rather that the third country's laws should cover all the core principles of EU data protection outlined above. Enhancing the definition of sensitive data with Supplementary Rules and including sexual orientation and trade union membership as sensitive personal information merely to meet EU adequacy standards may be an example of Japan attempting to comply with GDPR data protection and privacy concepts.⁴⁴

Professor Greenleaf opposes Japan's enforcement mechanisms, claiming that they are ineffective, and questions how, since the maximum fines is less than \$10,000, it can be essentially equivalent to the EU's GDPR.⁴⁵ Unlike the EU's hard power – legal and punitive sanctions –, the Japanese PPC employs soft power by issuing guidelines when there is a data breach. In that regard, there is a significant cultural difference since Japanese companies place a higher value on public trust and reputation than financial sanctions, but this is not the case in European and other Western nations. Therefore, a foreign company's data breach in Japan might be problematic. For example, just issuing a warning to Facebook in reaction to the Cambridge Analytica Scandal sparked questions about Japan's ability to protect its citizens' data privacy.⁴⁶

Since this data breach affected 100,000 Japanese Facebook users, but because there were no legally binding penalties under APPI, Facebook did not apologize enough or try to compensate by delivering any number of presents to Japanese consumers, as local Japanese companies would do in such circumstance.⁴⁷ After realizing that multinational companies do not respond to soft power in the same manner as domestic companies do, Japan decided to strengthen PPC

⁴¹Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision, Annex I. cited in [Greenleaf \(2018\)](#) 8.

⁴²EU-Japan Adequacy Decision [2019] OJ L 76/1.

⁴³Wang (2020) 661, 668.

⁴⁴Wang (2020) 672.

⁴⁵Greenleaf (2018) 8.

⁴⁶Wang (2020) 679, 682.

⁴⁷Wang (2020) 682–83.



enforcement powers by imposing stricter penalties on international businesses through the 2020 Cabinet Decision on the Amendment Bill of the APPI.⁴⁸

Onward transfers to third countries are allowed under Article 24 of the APPI if Japanese data subjects consent in advance.⁴⁹ This right is also granted to EU data subjects under Supplementary Rule (4).⁵⁰ However, as stated in [Article 49](#) para. 1(a), giving consent for data transfer is an exception rather than a rule under the GDPR.⁵¹ Thus, it was criticized in the doctrine that if consent is a rule for data transfer, this would not be essentially equivalent to the GDPR's data transfers to third countries provisions.⁵² Because the EDPB (European Data Protection Board) specifically states that consent should remain a derogation for specific situations.⁵³

Important data protection measures, such as the right to be forgotten and data protection by design and default, do not exist in the Japanese APPI and do not have to. Because, as previously stated being essentially equivalent does not imply that a country should replicate the GDPR. Notwithstanding, the Japanese government provided significant assurances to EU data subjects that they would have effective redress mechanisms in the event of public authorities' non-proportional and limitless access to their personal data,⁵⁴ and that there would be an independent data protection authority (PPC) that would supervise the complaint-handling mechanism for EU data subjects' complaints against the data breach and/or mass surveillance by the Japanese public authorities.⁵⁵

Taking into account the aforementioned explanations and doctrine, we can state that the Japanese data protection legislation applies stricter rules to the personal data of EU data subjects than to its own citizens. There are different ways to adopting data protection in that manner, and they can serve as a model for other countries, particularly for the United States, which has been unable to find an adequate solution for years. Taking this example, the US likewise could implement two-way data protection procedures, one for internal issues and one for personal data of EU data subjects.⁵⁶

3.2. The EU-UK adequacy decision

Since the United Kingdom (UK) has become a third country after the Brexit, the Commission issued an adequacy decision for the UK on June 28, 2021. Thereby, personal data can easily transfer from the EU to the UK. Although the UK has a version of the same regulation (UK GDPR), it takes a different approach than the EU GDPR. Taking these differences and potential future disagreements into account, the EU for the first time restricted its adequacy

⁴⁸Personal Information Protection Commission Japan (10 March 2020).

⁴⁹APPI, art 24(1).

⁵⁰Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision, Annex I, 9.

⁵¹GDPR, art 49.

⁵²Greenleaf (2018) 8.

⁵³EDPB (25 May 2018) 4.

⁵⁴EU-Japan Adequacy Decision [2019] OJ L 76/1 para. 113.

⁵⁵EU-Japan Adequacy Decision [2019] OJ L 76/1 para. 103.

⁵⁶Wang (2020) 690–91.



determination to four years with a safeguard known as a ‘sunset clause.’ If the UK maintains the existing legal condition, the decision can be renewed after this period.⁵⁷

Nonetheless, the United Kingdom has earned trust because it is still

[s]ubject to the jurisdiction of the European Court of Human Rights and it must adhere to the European Convention of Human Rights as well as to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which is the only binding international treaty in the area of data protection.⁵⁸

One distinction between the UK and EU data protection approaches is that under the UK Data Protection Act 2018, data subjects do not have the right to be informed, the right to access, the right to erasure, the right to restrict processing, right to confirm the processing, right to access to data and safeguards for third country transfers or the right to object if public authorities process personal data for immigration purposes.⁵⁹ Accordingly, the UK immigration did not satisfy the Article 23(2) since there were no legislative measures contains specific provisions.⁶⁰

Thus, the Adequacy Decision of the European Commission does not apply to personal data transferred for UK immigration control purposes.⁶¹ Transfers for UK immigration control purposes may be carried out if the appropriate conditions are satisfied, in accordance with the transfer methods set down in Articles 46 (Appropriate Safeguards) to 49 (Derogations) of the GDPR.⁶²

Accordingly, the UK Court of Appeal ruled in May 2021 that this exception violates EU GDPR Article 23 and is thus unlawful.⁶³ In response to this, the Immigration Exemption was amended on January 31, 2022, and it is stated that it is no longer a blanket provision but must be analysed on a case-by-case basis. The exemption is no longer valid for controllers other than the Home Office. The amendment also includes safeguards to prevent unlawful data access and transfer, as well as a time limit on any use of data.⁶⁴ Along with its specific provisions, the new amendment appears to comply with Article 23(2) GDPR.

The Five Eyes alliance, an intelligence sharing agreement involving five English-speaking democracies: the UK, the US, Canada, New Zealand, and Australia, may cause some data-protection issues. Because the EU did not grant an adequacy decision for all the members in the alliance. Especially, the US and the EU have not agreed on a framework for the free movement of personal data from the EU to the US. Hence, the personal information transfer from the UK to the US might be problematic.⁶⁵

⁵⁷European Commission (28 June 2021).

⁵⁸European Commission (28 June 2021).

⁵⁹UK Data Protection Act 2018 (c.12) [23 May 2018], 1–335, Schedule 2, Part 1(4) (2).

⁶⁰GDPR, art 23(2).

⁶¹European Commission (28 June 2021).

⁶²GDPR, art 46–49.

⁶³ICO (n.d.).

⁶⁴Home Office (2022) 1–16.

⁶⁵Home Office (2022) 10.



Furthermore, following Brexit, the UK is now free to make its own adequacy decisions. According to Joe Jones, Deputy Director of International Data Transfers at the UK Department for Digital, Culture, Media, and Sport, they prioritize data adequacy arrangements with the US, Australia, the Republic of Korea, Singapore, the Dubai International Financial Centre, and Colombia, as well as in the long term with Brazil, Kenya, and Indonesia.⁶⁶ Except for the Republic of Korea, none of the mentioned countries are adequate according to the Commission and if these arrangements are implemented, the UK's adequacy judgment may be undermined.

Moreover, following the Snowden revelations, it became clear that the United States and the UK engaged in mass surveillance, raising worries that individuals' freedom may be restricted by the government. Accordingly, it caused concern for the people in the UK whose jobs are most at risk (e.g., journalists) for the government to monitor them. They filed a complaint *Big Brother Watch and Others v. the United Kingdom* case with the European Court of Human Rights, claiming that the UK government violated the European Convention on Human Rights. As a result of the *Big Brother Watch and Others v. the United Kingdom* case, jurisprudence has evolved stating that states' powers to monitor and inspect are broad in order to ensure public safety but can be limited when the conditions in Article 8 of the Convention are met.⁶⁷ These conditions are 'the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.'⁶⁸ So, the European Court of Human Rights ruled that Article 8 was violated since the United Kingdom's surveillance practice went above and beyond the legal requirements.⁶⁹

Nonetheless, because the UK has safeguards in place, such as the collection of personal data by an independent authority with prior authorization, and in the case of public authorities' non-proportional and limitless access to personal data, individuals may bring an action before the ECHR (European Court of Human Rights) or the Investigatory Powers Tribunal, the Commission deemed the UK adequate.⁷⁰ However, there are still some concerns in the doctrine about the mass surveillance of the UK being an issue for EU people and residents in the future.⁷¹

Aside from the concerns raised above, the UK's Department for Digital, Culture, Media, and Sport ('DCMS') issued a consultation on September 10, 2021, and the Consultation's recommendations indicate a significant departure from the EU's essentially equivalent approach and a shift toward the 'risk-based' approach. Hence, the UK will focus on 'actual' risks and threats rather than 'academic or immaterial' ones.⁷² That would be a very risky step in terms of its adequacy as well as a significant divergence from the EU's current policy.⁷³

The consultation also proposes a proportionate increase in derogation flexibility, so that derogations can be used repeatedly, in contrast to the EU approach, which considers that

⁶⁶Fennessy (2021).

⁶⁷*Big Brother Watch and Others v UK* App no 58170/13 62322/14 24960/15 (ECtHR, 25 May 2021).

⁶⁸Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15), art 8(2).

⁶⁹*Big Brother Watch and Others v UK* App no 58170/13 62322/14 24960/15 (ECtHR, 25 May 2021).

⁷⁰European Commission (28 June 2021).

⁷¹Choromidou (2021) 397.

⁷²UK's Department for Digital, Culture, Media, and Sport, 'Data: A New Direction' (10 September 2021), 1, 87.

⁷³Choromidou (2021) 398.



derogations should not be used repetitively in order to avoid making them a rule rather than an exception. However, the UK's new policy may represent a significant departure from the EU's, presenting a danger to its adequacy.⁷⁴

Despite these concerns, the UK currently functions as a rule-taker, attempting to align its legislation with the EU's GDPR, remaining essentially equivalent and, more importantly, providing adequate protection with independent oversight mechanism so-called the Information Commissioner⁷⁵ and, in the event of a violation and access to personal data by public authorities, providing effective redress mechanisms for EU data subjects.

The US is currently far from being adequate because it lacks effective independent oversight mechanisms and redress mechanisms in the event of a violation, particularly by public authorities with access to personal information of EU data subjects. Furthermore, the United States has not accessed the Council of Europe's [Convention 108+](#).

Accessing to the [Convention 108+](#) would be a significant first step for the US in regaining the trust of the European Union. Furthermore, there should be effective independent oversight and redress procedures in the event of a breach, particularly by public authorities. These measures do not have to involve US citizens and residents in the same manner that the UK GDPR covers UK citizens and residents. However, the Japan adequacy model can be adopted, and the stricter and adequate mechanisms could apply solely to EU citizens and residents if it would be more beneficial to the US.

4. CONCLUSION

First and foremost, we addressed the necessity for EU adequacy decisions for personal data transfers from the EU to third countries in this article. And it was found that if the Commission decides if a third country is essentially equivalent, it deems that country adequate and issues an adequacy decision, allowing personal data to flow freely from the EU to that country without the need for any additional steps. It is not easy to pass the Commission's adequacy assessment test, despite the fact that it is a practical solution for both parties.

In order to pass this examination process, a third country must follow the fundamental and core enforcement principles outlined in the WP29 guidelines: fundamental data protection concepts should exist, legal basis for data processing should be identified, the collected data should not be used for other purposes which was not intended by the data subject (purpose limitation), the data controller should keep the data as long as it is necessary (time limitation), data controllers should use technical and organizational measures to ensure the security of collected data (security principle), data subjects should be informed about data processing in a clear and transparent manner using simple language (transparency), the data subject should

⁷⁴[Choromidou \(2021\)](#) 401. For EU's approach see: GDPR, Recital 113.

⁷⁵[EU-UK Adequacy Decision \[2021\]](#) OJ L 360/1 para 86: 'In the United Kingdom, the oversight and enforcement of compliance with the UK GDPR and the DPA 2018 is carried out by the Information Commissioner. The Information Commissioner is a 'Corporation Sole': a separate legal entity constituted in a single person. The Information Commissioner is supported in her work by an office. On 31 March 2020 the [Information Commissioner's Office](#) had 768 permanent staff. The sponsor-department of the Information Commissioner is the Department for Digital, Culture, Media and Sport.'



have the right to be informed, right to rectification, and right to object. There should also be procedural principles, such as independent oversight mechanisms and appropriate redress mechanisms in the event of a breach or violation of personal information, particularly by third-country public authorities. Even if it is necessary, public authorities should have limited and proportional access to personal data.

The US appears to have ignored these WP29 guidelines since public authorities' surveillance was not proportional, there were no effective legal remedies for EU data subjects, and there was no independent oversight mechanism, such as an independent Ombudsperson. These recommendations should be considered for the new Trans-Atlantic Data Privacy Framework to ensure that the Commission would deem the US adequate and that the CJEU would not declare it invalid.

Japan's adequacy decision was chosen because Japan's data protection and privacy perspective is comparable to that of the United States, in that personal data is regarded as an economic commodity, in contrast to the EU's fundamental right approach. Consequently, its adequacy decision can serve as a model for the US to have two-way data protection; one way, which is the current situation, may be maintained for US citizens and residents, while the other way, which includes stricter rules with the Japan's Supplementary Rules, including effective oversight and redress mechanisms, may be adopted only for EU citizens and residents. In addition, public authorities' access to the personal data of the EU data subjects should be restricted and proportional.

Furthermore, the UK might be a useful model for the US since they both had mass surveillance issues in recent history, as the UK's Big Brother Watch case and the US's *Schrems II* case demonstrated in the previous chapters. However, the UK received the adequacy decision and one of the most important reasons for this is that it signed and ratified the Council of Europe's [Convention 108+](#) and the European Convention of Human Rights, demonstrating commitment to these fundamental frameworks. So that the US may follow the footsteps of the UK and accessed the [Convention 108+](#) as a first step toward an effective oversight mechanism and remedies for EU data subjects in order to re-establish the trust of the Commission. Nevertheless, adopting the [Convention 108+](#) into domestic data protection legislation in the US may take longer than establishing separate Supplementary Rules.

As previously stated, because the US and the EU are each other's most important trade partners, and data is one of today's most important economic values, they cannot cease data sharing with each other, and both sides would like to be able to do so safely and freely. Indeed, lately, the European Commission and the United States have reached an agreement in principle for a Trans-Atlantic Data Privacy Framework for the third time. They would like to address and enhance the shortcomings of Safe Harbour and Privacy Shield under this framework.

Yet, the US has not relinquished the intelligence agencies' monitoring mechanisms but has committed to limit data access to when it is necessary and proportionate. In addition, they established a new two-tier redress system, which includes a Data Protection Review Court, to review and resolve Europeans' concerns about data access by U.S. intelligence agencies. However, the question of whether this court will have the authority to limit the acts of intelligence services remain unclear.

The main concern is that, under the new arrangement, data will once again be able to flow freely between the EU and, not the US, but the participating US companies. In other words, self-certifying companies, not the US, should have an adequate level of protection. In this scenario, it



is unclear how the companies should ensure that the US intelligence services have the necessary and proportionate level of access to personal data of EU citizens and residents. This strategy did not function in the previous examples, which were deemed invalid by the CJEU in the *Schrems I* and *Schrems II* judgments. ‘Playing the same game a third time,’ as Max Schrems stated it, does not appear to be a logical solution.⁷⁶

Taking all of the above findings into consideration, the best and quickest way for the US to achieve an adequate level of data protection may be a two-way data protection approach with stricter Supplementary Rules covering only EU data subjects; requiring intelligence services to stop accessing data received from the EU unless there is a reasonable concern for national security; ensuring an independent oversight mechanism; and providing effective redress mechanisms especially in the event of intelligence services’ non-proportional and limitless access. Having significant duties for self-certifying companies, as outlined in the key principles of the new framework, would not preclude a *Schrems III* case. As a result, appropriate protection could only be achieved via government initiatives, not through the mere efforts of individual companies.

Finally, if the WP29 guidelines and the Council of Europe’s [Convention 108+](#) were followed, the above-mentioned suggestions would be well-prepared. The two-way solution, which includes stricter rules for EU data subjects, may pave the way for the US to enact comprehensive data protection legislation on a federal level in the future, allowing them to have stricter rules not only for EU data subjects, but also for their citizens and residents, as well as all data flowing into the US from all over the world.

LITERATURE

- Choromidou, A., ‘EU data protection under the TCA: the UK adequacy decision and the twin GDPRs’ (2021) 11 *Int. Data Priv. Law* 388–401.
- Cory, N., Castro, D. and Dick, E., ‘“Schrems II”: What Invalidating the EU-US Privacy Shield Means for Transatlantic Trade and Innovation’, *Information Technology and Innovation Foundation* (3 December 2020) <<https://www2.itif.org/2020-privacy-shield.pdf>> accessed 7 September 2022.
- European Commission, ‘Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection’ (13 January 2018) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 21 December 2021.
- European Commission, ‘Data protection: Commission adopts adequacy decisions for the UK’ (28 June 2021) <https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183> accessed 12 January 2022.
- European Commission, ‘European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework’ (25 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087> accessed 3 May 2022.
- European Commission, ‘Trans-Atlantic Data Privacy Framework’ (25 March 2022a), <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 3 May 2022.

⁷⁶Schrems (2022).



- European Commission, 'United States' (6 September 2021) <<https://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/>> accessed 25 January 2022.
- Fennessy, C., 'The UK's new plans for data transfers: An interview with Joe Jones', *iapp* (7 September 2021) <<https://iapp.org/news/a/the-uks-new-plans-for-data-transfers-an-interview-with-joe-jones/>> accessed 17 January 2021.
- Greenleaf, G., 'Japan: EU Adequacy Discounted' (2018) 155 Privacy Laws & Business International Report 8–10.
- Home Office, 'Immigration Exemption Policy Document: Use of the immigration exemption under Article 23 of the UK GDPR and Schedule 2 of the DPA 2018, v. 1 (January 2022) (entered into force 31 January 2022)' <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1052791/IEPD_v.1.pdf> accessed 25 February 2022.
- Ivers, E. A., 'Using State-Based Adequacy Now, National Adequacy over Time to Anticipate and Defeat Schrems III' (2021) 62 BC L Rev. 2573–2617.
- Schrems, M., "Privacy Shield 2.0"? - First Reaction by Max Schrems' *NOYB* (25 March 2022) <<https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems>> accessed 3 May 2022.
- Schwartz, P. M. and Peifer, K. N., 'Transatlantic Data Privacy Law' (2017) 106 Geo. LJ. 115–179.
- Schwartz, P. M., 'Global Data Privacy: The EU Way' (2019) 94 NYU L Rev. 771–818.
- Wang, F. Y., 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the Eu-Japan GDPR Adequacy Agreement' (2020) 33 Harv. JL & Tech. 661–691.

LEGAL TEXTS

- Article 29 Data Protection Working Party, Adequacy Referential, 18/EN 6 February 2018 WP 254 rev01.
- Charter of Fundamental Rights of the European Union, OJ 2010C 83/389.
- Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 26.07.2000, p. 7–47.
- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207/1, 12.07.2016, 1–112.
- 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, OJ L 76, 19.3.2019, p. 1–58.
- Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom under the Act on the Protection of Personal Information, OJ L 360, 11.10.2021, p. 1–68.
- Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, Article 8(2).
- Council of Europe, 'Convention 108 + [2018] ETS 108' (2018). <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf> accessed 7 September 2022.



- ECHR (as amended by Protocols Nos. 11, 14 and 15) <https://www.echr.coe.int/documents/convention_eng.pdf> accessed 7 September 2022.
- EDPB, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679' (25 May 2018) <[edpb_guidelines_2_2018_derogations_en.pdf](https://edpb.europa.eu/edpb/files/2018/05/guidelines_2_2018_derogations_en.pdf)(cnil.fr)> accessed 9 January 2022.
- European Commission, 'Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World, COM/2017/07 final, 10.01.2017.'
- Eurostat, 'USA-EU international trade in goods statistics' (2022) <[https://ec.europa.eu/eurostat/statistics-explained/index.php?title=USA-EU_-_international_trade_in_goods_statistics#:~:text=The%20position%20of%20the%20United,and%20Russia%20\(4.1%20%25\)>](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=USA-EU_-_international_trade_in_goods_statistics#:~:text=The%20position%20of%20the%20United,and%20Russia%20(4.1%20%25)>)> accessed 3 May 2022.
- ICO (Information Commissioner's Office), 'Immigration Exemption, "Can we still rely on the immigration exemption?"' (n.d.) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/immigration-exemption/>> accessed 13 January 2022.
- Personal Information Protection Commission Japan, 'The Amendment Bill of the Act on the Protection of Personal Information, etc. (Overview)' (10 March 2020) <https://www.ppc.go.jp/files/pdf/amendment_bill202003.pdf> accessed 9 January 2022.
- Personal Information Protection Commission, 'Amended Act on the Protection of Personal Information (Tentative Translation)' (June 2020) <https://www.ppc.go.jp/files/pdf/APPI_english.pdf> accessed 9 January 2022.
- 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), OJ 2016 L 119/1, Article 1(1)(2).
- Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision, Annex I. <https://ec.europa.eu/info/sites/default/files/annex_i_supplementary_rules_en.pdf> accessed 7 September 2022.
- UK Data Protection Act 2018 (c.12) [23 May 2018], 1–335, Schedule 2, Part 1(4)(2). <<https://www.legislation.gov.uk/ukpga/2018/12/enacted/data.pdf>> accessed 13 January 2022.
- UK's Department for Digital, Culture, Media, and Sport, 'Data: A New Direction' (10 September 2021), 1, 87. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document_Accessible_.pdf> accessed 22 January 2022.
- Working Party's Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN 2016 WP237.
- Working Party's Working Document on the Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive, DG XV 1998 D/5025/98 WP12.

LEGAL CASES

- Big Brother Watch and Others v UK* App no 58170/13 62322/14 24960/15 (ECtHR, 25 May 2021).
- Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* EU:C:2020:559.



Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650.

Court of Justice of the European Union, 'Judgment in Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*' (16 July 2020) Press Release No 91/20, 1–2.

Open Access. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited, a link to the CC License is provided, and changes – if any – are indicated. (SID_1)

