

ADEQUACY DECISIONS UNDER THE GDPR AND ACCESS TO EU DATA: LIMITS FOR THIRD COUNTRIES IN THE AGE OF AI

Oksana PANICHKOVSKA

PhD student, Mykolas Romeris University

e-mail: okpanichkovska1@stud.mruni.eu

Abstract

Cross-border data transfers have become a central element of the global digital economy, particularly in the context of artificial intelligence, which relies on access to large and diverse datasets. Within the European Union, such transfers are regulated under the General Data Protection Regulation, which permits transfers to third countries primarily on the basis of adequacy decisions under Article 45. This paper examines the role of adequacy decisions as a mechanism for enabling access to EU personal data and analyses the challenges faced by third countries in meeting the required standard of protection. It focuses on the concept of “essential equivalence” and the legal and institutional conditions that must be fulfilled in order to obtain adequacy status. The paper adopts a doctrinal approach, based on the analysis of EU legal sources and relevant case law, and situates these findings within the broader context of global data flows. It argues that the adequacy framework sets a high and complex threshold, which is difficult to meet in practice, particularly for countries with developing regulatory systems. In the context of AI development, this may limit access to data and affect the ability of third countries to participate in data-driven innovation, thereby influencing the structure of global data flows.

Keywords: *Adequacy Decisions, Data Transfers, GDPR, Artificial Intelligence, Third Countries*

1. Introduction

Cross-border data transfers are now part of the ordinary functioning of the digital economy. Personal data moves through cloud services, social media platforms, online payments, outsourcing arrangements, multinational corporate groups, public procurement chains, and international research cooperation. In legal discussions, transfers are often treated as a compliance issue. In practice, however, they are also about power, market access, technological capacity, and the ability to participate in digital innovation. This is especially visible in relation to artificial intelligence (AI), where the availability of large and diverse datasets may influence whether systems are developed faster, trained on broader inputs, and integrated into real economic sectors.

The European Union (EU) regulates these transfers through a rights-based model. The General Data Protection Regulation (GDPR) does not prohibit international transfers as such, but it insists that personal data should not lose protection simply because it leaves the Union (Regulation (EU) 2016/679, 2016, arts. 44–50). This basic idea is easy to understand and hard to challenge in principle. If the EU recognises data protection as a fundamental right, it would be incoherent to allow data to be exported into legal systems where that protection becomes weak, purely formal, or practically unenforceable. At the same time, the legal tools through which this objective is pursued have practical consequences that go beyond individual compliance. Article 45 GDPR allows the European Commission to decide that a third country ensures an adequate level of protection. Such adequacy decisions are often described as the most complete transfer mechanism because they permit data flows without the need for case-by-case contractual safeguards. In policy and business terms, adequacy can reduce friction, increase predictability, and lower transaction costs. In constitutional terms, it operates as a legal judgment that a foreign system offers protection that is essentially equivalent to the level guaranteed within the EU.

This paper starts from a simple but important observation. Adequacy is usually presented as a facilitating mechanism. At the same time, in practice, only a limited number of jurisdictions benefit from it. This raises an important question: if adequacy is formally open to third countries, why is it limited in practice, and what does that mean in a digital economy where AI and other data-intensive technologies increasingly depend on access to data? This question matters not because AI creates a separate regime of transfer law, but because it makes the practical importance of lawful access to data much easier to see.

The research problem addressed in this paper is that, although adequacy decisions are intended to facilitate lawful international data transfers, the legal and institutional threshold they impose may operate as a restrictive filter that

shapes access to EU personal data and indirectly influences participation in data-driven innovation. The paper does not argue that the adequacy framework is unjustified or that the EU should lower standards for the sake of convenience. Its claim is narrower and more practical. The same features that make adequacy attractive from a rights perspective may also make it difficult to obtain, especially for countries whose regulatory systems are still developing or are organised according to different institutional logics.

The paper addresses three research questions. First, what legal and institutional criteria must a third country satisfy to obtain an adequacy decision under Article 45 GDPR? Second, why have adequacy decisions remained limited in number despite the growth of global digital trade and data-driven services? Third, how might the limited availability of adequacy decisions affect lawful access to EU personal data in the context of AI?

The central thesis is that adequacy decisions under Article 45 GDPR establish a high legal and institutional threshold that many third countries find difficult to meet in practice. This threshold is justified by the EU's commitment to protecting fundamental rights, particularly following the Court of Justice of the European Union (CJEU) judgments in *Schrems* and *Schrems II*. However, the practical result is that access to EU personal data is not the same for all third countries. In an environment where AI systems increasingly depend on international data infrastructures, the limited availability of adequacy may influence which jurisdictions are more advantageously placed to participate in data-driven innovation.

Methodologically, the paper is doctrinal. It relies on the interpretation of EU primary and secondary law, relevant CJEU case law, European Commission adequacy decisions, and academic literature on data protection law and digital governance. A limited comparative perspective is also included. Rather than comparing many countries superficially, the paper looks at a small number of examples that clarify the operation of adequacy in practice, especially Japan and the United Kingdom, while also discussing the broader difficulties faced by countries outside the current adequacy network.

The paper proceeds in six parts. Section 2 explains the legal structure of adequacy within Chapter V GDPR and the role of the standard of essential equivalence. Section 3 examines adequacy in practice through selected examples and identifies the main reasons why adequacy decisions remain limited. Section 4 discusses why adequacy has become increasingly important in the context of AI and data-intensive technologies. Section 5 offers a more critical assessment of the adequacy framework and considers its distributive and regulatory effects. Section 6 presents the main conclusions.

1.1. Literature and contribution

The existing literature on international data transfers under EU law is extensive, but it addresses different aspects of the transfer regime rather than one single research question. A first group of scholarship examines the legal structure of EU transfer law and the development of the rules from earlier instruments to the GDPR. Kuner (2013) remains one of the key authors in this area. He explains that rules on cross-border data transfers developed because personal data could lose protection once they left the country where they were originally collected. Lynskey (2015) reaches a similar conclusion but places transfer rules within the broader framework of EU fundamental rights. She argues that restrictions on international transfers are intended to preserve the level of protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. More recent work by De Hert and Papakonstantinou (2016) explains how the GDPR strengthened this approach by giving greater importance to institutional safeguards and enforcement. Collectively, these authors show why Chapter V GDPR exists and how the transfer regime operates (De Hert & Papakonstantinou, 2016; Kuner, 2013; Lynskey, 2015). However, it says less about how the limited number of adequacy decisions affects third countries seeking access to EU personal data.

A second group of scholarship focuses on the case law of the Court of Justice of the European Union (CJEU), especially *Schrems* and *Schrems II*. Here, the discussion mainly concerns fundamental rights, government surveillance, and the meaning of the standard of “essential equivalence”. This literature shows that adequacy decisions are no longer only technical instruments allowing data transfers. Instead, they require a broader assessment of the legal system of a third country, including independent supervision, effective judicial remedies, and limits on state access to personal data (European Data Protection Board [EDPB], 2021). Much of this scholarship focuses on the EU-US relationship because this was the background of both *Schrems* cases (*Data Protection Commissioner v. Facebook Ireland Ltd & Schrems*, 2020; *Schrems v. Data Protection Commissioner*, 2015). While this focus is understandable, it also means that less attention has been given to countries outside the major transatlantic data transfer framework that may also seek adequacy status.

A third strand of literature examines the wider international influence of EU data protection law. Bradford (2020) explains this through the idea of the Brussels Effect, arguing that many countries adjust their domestic laws because access to the EU market creates incentives to follow European regulatory standards. In the field of data protection, this can be seen in the growing number of GDPR-inspired laws around the world. More recent authors develop this discussion further. Mc Cullagh (2025), for example, argues that adequacy assessments have become more demanding because the European Commission evaluates not only legislation but also how the rules work in practice. Marelli (2024) similarly observes that adequacy decisions require a broad assessment of

a third country's legal system, institutional safeguards, and practical enforcement rather than a simple comparison of legislative texts. Czerniawski (2024) also points out that adequacy decisions raise questions about transparency and legitimacy because they involve complex assessments of foreign legal systems. This literature shows that adequacy is more than a technical transfer mechanism. At the same time, there is still an important difference between adopting GDPR-inspired legislation and obtaining an adequacy decision. The second issue has received much less attention in the literature (Bradford, 2020; Czerniawski, 2024; Marelli, 2024; Mc Cullagh, 2025).

Finally, emerging literature on AI and data governance highlights that data access is not only a privacy question but also an innovation question. Wachter and Mittelstadt (2019) discuss how AI challenges traditional ideas in data protection law, especially regarding automated decision-making and the use of personal data to generate new information. Malgieri (2022) also argues that AI places increasing pressure on existing data protection rules because many AI systems depend on large amounts of data. Veale and Zuiderveen Borgesius (2021) make a similar point by showing that AI regulation cannot be separated completely from data protection law. This literature helps explain why access to data has become increasingly important. However, relatively little attention has been paid to how adequacy decisions influence the ability of third countries to obtain lawful access to EU personal data for AI development. Most studies discuss AI governance and international data transfers separately, rather than examining how these two areas interact.

Although these strands of literature make an important contribution, they generally examine adequacy either from the perspective of fundamental rights, the Schrems case law, or the EU's external regulatory influence. Comparatively less attention has been paid to how adequacy decisions shape lawful access to EU personal data by third countries in the context of AI development. This is particularly relevant because organisations developing AI increasingly depend on access to large and diverse datasets, while lawful international transfers remain subject to the conditions laid down in Chapter V of GDPR.

This paper contributes to that gap in a modest but concrete way. It does not propose a new theory of AI governance, nor does it attempt a full comparative assessment of prospective adequacy countries. Its contribution is narrower. It brings together doctrinal analysis of Article 45 of GDPR, case law on essential equivalence, and a governance-oriented discussion of how the limited number of adequacy decisions affects access to EU-origin personal data. In doing so, it seeks to show that adequacy should be understood not only as a compliance mechanism, but also as a legal structure with wider distributive effects.

The paper's contribution is also methodological. Rather than starting with broad claims about “digital inequality”, it starts with the internal legal structure of the adequacy framework and then examines its practical implications. The

argument developed here, therefore, remains careful. It does not claim that adequacy alone determines global technological hierarchies. It claims that adequacy is one legal factor that shapes access to data and deserves more attention in discussions on AI and international data governance.

1.2. Methodological remarks and limits of the paper

Because the topic sits between doctrinal EU law, comparative institutional analysis, and questions of digital governance, a short methodological clarification is necessary.

The paper primarily uses a doctrinal legal method. It analyses the text of the GDPR, the reasoning of the CJEU, the content of adequacy decisions, and academic commentary. This means that the argument is centred on the legal structure of the adequacy framework rather than on empirical measurement of its economic consequences. The paper does not, for example, provide quantitative evidence showing precisely how many AI projects have been delayed or redirected because of the absence of adequacy. Such evidence would be valuable, but it would require a different design and data set than is possible within the scope of a conference paper.

At the same time, the paper is not purely internal to doctrine. It includes a limited comparative and contextual perspective. The examples of Japan and the United Kingdom are used not to provide a full comparative study, but to illuminate different paths to adequacy: one based on adaptation and dialogue, the other on legal continuity. These examples are helpful because they show that adequacy can be achieved in more than one way, but also that the pathway is easier in some institutional settings than in others. The paper also refers, more generally, to the situation of third countries outside the existing adequacy network, especially those with developing or changing regulatory systems.

A further limit should also be acknowledged. The paper focuses on adequacy as such and therefore does not provide an equally detailed treatment of all other transfer tools. Standard contractual clauses are discussed because they are the main alternative and, therefore, necessary for evaluating the practical importance of adequacy. Derogations under Article 49 are mentioned only briefly, because they are exceptional by design and less suitable for regular, large-scale, or structurally important flows. The aim here is not to describe the entire transfer chapter of the GDPR exhaustively, but to analyse the specific legal and practical role played by adequacy decisions.

The paper also uses AI as a context rather than as an autonomous field of regulation. This is deliberate. If AI were treated as the main legal topic, the paper would risk becoming too broad, moving into questions of liability, discrimination, transparency, or the AI Act. Those issues are important, but they are not central here. AI is discussed because it helps reveal why the legal status of cross-border data access matters. It intensifies the practical significance of transfer law, but it does not replace the doctrinal core of the analysis.

Finally, the paper recognises that adequacy is not the only lens through which participation in the global digital economy can be assessed. Talent, infrastructure, political stability, industrial policy, procurement, and capital markets also matter. The argument is, therefore, not that adequacy explains everything. It is that adequacy has become one of the legal mechanisms through which inclusion and exclusion are structured in global data flows, and that this deserves more direct scholarly attention.

2. Adequacy decisions in the structure of EU data transfer law

2.1. Article 45 GDPR and the systemic character of adequacy

The regulation of international data transfers in EU law is built around continuity of protection. Article 44 GDPR states that any transfer of personal data that is undergoing processing or is intended for processing after transfer to a third country shall take place only if the conditions laid down in Chapter V are complied with. This means that transfer law is not a self-contained exception to the GDPR. It is one of the instruments through which the Regulation seeks to preserve the level of protection guaranteed inside the Union when data move outside it (Regulation (EU) 2016/679, 2016, art. 44).

The system of Chapter V is layered. The first layer is adequacy under Article 45. If the Commission has decided that a third country, a territory, or a specified sector ensures an adequate level of protection, transfers may take place without any specific authorisation and without the exporter having to put in place additional transfer tools. The second layer is transfer on the basis of “appropriate safeguards” under Article 46, including standard contractual clauses (SCCs), binding corporate rules, approved codes of conduct, and certification mechanisms. The third layer consists of derogations for specific situations under Article 49, such as explicit consent or necessity for the performance of a contract. This architecture already suggests that adequacy holds a privileged place. It is not merely one option among many. It is the mechanism through which the EU expresses institutional trust in a foreign legal order as a whole.

Article 45(2) makes clear that adequacy is assessed broadly. The Commission must take account of the rule of law, respect for human rights and fundamental freedoms, relevant legislation, including legislation concerning public security and criminal law, the existence and effective functioning of one or more independent supervisory authorities, and the international commitments entered into by the third country (Regulation (EU) 2016/679, 2016, art. 45(2)). The breadth of this list is important. It means that adequacy is not simply about whether a third country has enacted a privacy statute that resembles the GDPR. It involves a systemic assessment of the legal and institutional environment into which EU data will travel.

This systemic character of adequacy helps explain both its value and its difficulty. From the perspective of rights protection, a narrow assessment would be insufficient. Personal data can be affected not only by private-sector processing but also by public-authority access, weak oversight, and poor enforcement. Yet the more systemic the assessment becomes, the more demanding it is for the third country and the more politically sensitive it may become. Adequacy, therefore, operates at the boundary between legal technique and constitutional judgment.

Academic literature has long recognised that cross-border data transfer law is shaped by this tension. Kuner (2013) shows that transfer law emerged from the need to reconcile international data movement with domestic guarantees of privacy and data protection. The problem was never simply how to enable data flows. It was also how to preserve legal accountability across borders. The GDPR inherited this tradition but strengthened it significantly by framing the issue more explicitly in terms of fundamental rights and institutional guarantees. In that sense, adequacy under the GDPR is not a commercial facilitation mechanism with some privacy language attached. It is fundamentally a constitutional device, even if it also has major consequences for trade and innovation.

The concept of “adequate level of protection” has evolved through both legislation and case law. Earlier adequacy decisions were already politically and economically significant, but the legal test became much sharper after the CJEU’s intervention in *Schrems*. The current framework cannot be understood without that jurisprudence, because the Court has effectively constitutionalised the interpretation of adequacy. The next subsection, therefore, turns to the standard of “essential equivalence,” which now structures adequacy assessments.

A further point should be added at this stage. The privileged position of adequacy in EU law also gives it symbolic weight in international practice. For third countries, an adequacy decision is not only useful for facilitating transfers. It can also signal that their data protection system has achieved a level of maturity and credibility recognised by the EU. This partly explains why many recent privacy reforms around the world draw, directly or indirectly, on GDPR language and concepts. Bradford (2020) describes this broader phenomenon as the Brussels Effect: the capacity of EU rules to shape global regulatory behaviour because access to the EU market is economically valuable.

2.2. The meaning of “essential equivalence”

The standard of “essential equivalence” is central to understanding why adequacy decisions are both attractive and difficult. It is not expressly defined in detail in the GDPR, but it has been developed in the case law of the CJEU. In Case C-362/14 *Schrems*, the Court invalidated the Safe Harbor Decision and emphasised that the level of protection in a third country must be “essentially equivalent” to that guaranteed within the EU legal order (*Schrems v. Data Protection Commissioner*, 2015). The point was not that foreign legal systems

had to be identical to EU law, but that they had to ensure protection of substance and effectiveness comparable to that offered under EU law, read in the light of the Charter of Fundamental Rights of the European Union. This standard was deepened in Case C-311/18 Schrems II, where the Court invalidated the EU-US Privacy Shield (Data Protection Commissioner v. Facebook Ireland Ltd & Schrems, 2020). The Court focused particularly on two matters: first, the scope of public-authority access to personal data for national security purposes, and, second, the availability of effective judicial remedies for data subjects. The Court accepted that third-country systems will differ from EU law, but it insisted that the protection afforded must be sufficiently effective in practice. In other words, formal legal guarantees are not enough if surveillance powers are too broad, oversight is weak, or redress is unavailable or ineffective.

This is where the standard becomes especially significant. “Essential equivalence” is more demanding than formal similarity, but also less rigid than legal “identity”. That makes it useful as an evaluative concept. At the same time, it creates uncertainty because it does not provide precise metrics. How far can a third-country system diverge from EU approaches before equivalence is lost? Which aspects of institutional design are indispensable, and which admit variation? The case law provides guiding principles, but it does not eliminate the need for judgment.

From one perspective, this openness is beneficial. It allows the Commission to recognise different legal traditions so long as the practical level of protection remains comparable. The adequacy decision concerning Japan shows this clearly, because it was based not on complete legal alignment but on a combination of existing domestic law and supplementary rules designed to address specific EU concerns (European Commission, 2019). From another perspective, however, this openness of the concept can make the way to achieve adequacy less predictable, especially for countries that do not already have close legal and institutional links with the EU.

This uncertainty also affects the relationship between law and politics. Adequacy decisions are formally legal acts, but they are prepared through detailed exchanges between the Commission and the relevant third country. Because “essential equivalence” requires systemic evaluation, the process necessarily involves judgment about institutional effectiveness and public-law conditions. In practice, then, adequacy is never only a technical assessment. It is a legal evaluation with important political consequences.

A further point should be noted here. The standard of essential equivalence is meant to preserve a high level of protection, which is understandable in light of the EU’s approach to personal data. At the same time, it may be easier to satisfy this standard for countries whose legal systems and administrative structures are already closer to those of the EU. This does not necessarily mean that the standard is openly biased. However, it does suggest that

institutional similarity may matter in practice, even if the legal test is formulated in universal terms. As a result, countries whose legal systems are easier to assess within the EU rights framework may be in a stronger position when seeking adequacy recognition.

3. Adequacy in practice: criteria, examples, and limits

The practical application of adequacy decisions shows more clearly why they remain limited in number. In formal terms, Article 45 GDPR is open-ended and does not restrict adequacy to particular regions or categories of states. In practice, however, the number of jurisdictions recognised as adequate remains relatively small.

One of the main reasons why adequacy remains limited is that the Commission must assess a foreign legal system not only on the basis of legislative text, but also in terms of how institutions function in practice. The GDPR requires independent supervisory authorities with actual powers, effective remedies for individuals, and legal safeguards against disproportionate access by public authorities. Some countries may satisfy part of these conditions without satisfying all of them. Others may have adopted new privacy legislation but still lack administrative capacity or consistent enforcement. In such cases, there may be a considerable distance between formal legal reform and adequacy recognition.

A further reason is that adequacy is not assessed in isolation. Since *Schrems* and *Schrems II*, the Commission must proceed on the assumption that any adequacy decision may later be reviewed by the CJEU. This encourages a more cautious approach, especially where surveillance rules, intelligence access, or redress mechanisms raise doubts. Matters that might previously have been addressed through political assurances or general trust are now more likely to be examined more strictly in the light of fundamental rights.

The following examples illustrate both the possibilities and the limits of the adequacy model. Japan shows that legal adaptation and regulatory dialogue can make adequacy possible even where legal systems are not identical. The United Kingdom shows that adequacy is easier to maintain where strong legal continuity already exists. At the same time, both examples also demonstrate that adequacy depends on a wider framework of trust, institutional capacity, and ongoing review. They should, therefore, not be treated as evidence that adequacy is equally accessible to all third countries willing to reform.

3.1. The example of Japan: supplementary arrangements

The adequacy decision concerning Japan is often presented as a successful example of regulatory cooperation. This is important because Japan did not receive adequacy simply on the basis of its existing domestic framework. Instead, the process involved detailed exchanges between Japanese authorities and the EU, followed by the adoption of supplementary rules by Japan's Personal

Information Protection Commission in order to address differences between Japanese law and EU requirements (European Commission, 2019). These supplementary rules were important in substantive terms. They dealt with issues that the EU considered necessary for preserving continuity of protection, including the treatment of sensitive data, onward transfers, and certain aspects of individual rights and complaint procedures. The adequacy finding, therefore, did not rest on domestic legislation alone, but on a broader assessment that also included interpretive and administrative commitments (European Commission, 2019, 2023). This suggests that adequacy does not necessarily require a complete reproduction of the GDPR. It may also be reached through more targeted legal and institutional adjustments.

At the same time, the Japanese example should be approached with some caution. The process required administrative expertise, sustained engagement with EU institutions, and the ability to respond to specific regulatory concerns. Japan was in a position to do this because it already had a functioning data protection regime, established administrative structures, and the political willingness to invest in the process. Other countries may not be equally well placed to undertake this kind of alignment. For this reason, the Japanese case is both encouraging and cautionary. It shows that adequacy can be achieved through cooperation, but also that the process is demanding and resource-intensive. The Japanese example also shows that adequacy may form part of a broader strategy of digital economic integration. In this case, adequacy was not only about legal compliance, but also about creating stable conditions for data flows between major economic partners. This does not reduce the importance of rights protection, but it does show that adequacy stands at the intersection of rights protection and economic governance.

3.2. The example of the United Kingdom: continuity under ongoing review

The United Kingdom provides a different kind of example. After Brexit, the UK became a third country for the purposes of EU transfer law, yet its legal framework began from a point of near-complete alignment with EU standards because the GDPR had already been part of its domestic law (European Commission, 2021). In that sense, the UK adequacy decision was less about adaptation from outside and more about preserving continuity after a constitutional separation.

The adequacy finding for the UK, therefore, demonstrates that adequacy may be comparatively easier to secure where legal continuity already exists. At the same time, the UK case also shows that adequacy is not unconditional. The Commission's approach included monitoring and review mechanisms, reflecting the possibility that future legal divergence, particularly in areas linked to surveillance or rights protection, could alter the overall assessment (European

Commission, 2025). This confirms that adequacy is dynamic, not static. It is better understood as an ongoing legal relationship than as a one-time recognition.

The UK case is useful because it shows that adequacy is easier to maintain where there is already a high degree of legal and institutional continuity (European Commission, 2025). This means that countries with different legal traditions or weaker administrative systems are likely to face a more difficult path. For this reason, the question is not only whether a country wants adequacy, but also from what starting point it is trying to achieve it.

3.3. Obstacles faced by other third countries

For many third countries outside the existing adequacy network, the path to adequacy is more difficult, and the obstacles they face can be grouped into four categories: legislative, institutional, constitutional, and practical.

Legislative obstacles arise where a country lacks a comprehensive data protection framework or where rights, obligations, or definitions differ substantially from EU expectations. This does not mean that exact textual similarity is required. It does mean that the legal framework must be coherent and provide meaningful limits on processing, rights for data subjects, duties for controllers, and possibilities for enforcement.

Institutional obstacles are equally important. Article 45 requires consideration of independent supervisory authorities with effective powers. Independence is not only a formal matter. It concerns resources, expertise, investigative capacity, and the ability to act without improper political influence. Countries may enact modern privacy laws relatively quickly, but building an authority capable of enforcing them credibly often takes much longer.

Constitutional obstacles are especially visible in the area of state access to data. Schrems II made clear that broad surveillance powers or weak avenues of redress can undermine a transfer framework even where private-sector data protection looks relatively advanced. This means that adequacy cannot be achieved through private-sector regulation alone. Broader public-law and constitutional questions become central.

Finally, there are practical obstacles. Rights on paper do not guarantee rights in practice. Complaint mechanisms may exist but be little used. Judicial review may be formally available but too costly, too slow, or too inaccessible to non-citizens. Enforcement may be selective or inconsistent. The adequacy framework is concerned with effectiveness, and effectiveness is often the most difficult part to demonstrate.

These obstacles help explain why adequacy remains limited, especially for jurisdictions undergoing regulatory transition. They also explain why adequacy should not be treated simply as a binary badge. It is the endpoint of a deeper process of legal and institutional development.

3.4. Adequacy compared with standard contractual clauses

Where adequacy is absent, transfers may still take place through SCCs and other safeguards under Article 46 GDPR. In practice, SCCs are widely used and often indispensable for international business operations. Yet they do not provide the same legal position as adequacy.

The difference is conceptual as well as practical. Adequacy expresses institutional trust in the recipient system as a whole. SCCs do not. They are contractual tools that create obligations between exporter and importer, but after Schrems II they also require assessment of whether the law of the recipient country allows those obligations to be complied with in a manner that ensures essentially equivalent protection. Exporters may therefore need to conduct transfer impact assessments and adopt supplementary technical or organisational measures where necessary (EDPB, 2021).

This matters because, in the absence of adequacy, responsibility shifts more heavily onto private actors. Large multinational firms may be able to manage these burdens. Smaller firms, research collaborations, or actors in countries with fewer compliance resources may struggle more. In this sense, the absence of adequacy does not prohibit data flows outright, but it makes them more conditional, fragmented, and costly. That distinction is central to the argument of this paper. Access to EU data is not only about whether transfers are legally possible in theory. It is also about under what conditions they are feasible in practice.

4. Adequacy decisions and AI

AI is not the legal source of the adequacy framework, but it is one of the contexts in which the practical importance of international data transfers becomes much more visible. Many AI systems depend on large datasets, repeated updating, geographically distributed infrastructure, and cooperation between organisations located in different countries. Even where developers increasingly rely on anonymisation, synthetic data, or privacy-enhancing technologies, personal data still plays an important role in many AI applications, including healthcare, speech recognition, fraud detection, and consumer services (Wachter & Mittelstadt, 2019; Malgieri, 2022). At the same time, the role of data should not be overstated. Not every AI system requires unrestricted access to EU personal data, and many models can be trained using open, synthetic, or non-personal datasets. Nevertheless, in sectors where the quality, diversity, and scale of data remain important, international transfer rules become one of the legal conditions shaping AI development.

For that reason, the question of adequacy should not be confined to traditional privacy scholarship. It should also be considered within the broader discussion of how legal regimes shape digital opportunity. This section examines

three aspects of that relationship: first, the way AI sharpens the significance of transfer law; second, the mismatch between a relatively static legal model and dynamic data-processing environments; and third, the implications for third countries seeking to participate in AI-related innovation.

4.1. Why AI brings the adequacy question into focus

In conventional discussions on international data transfers, the legal question often appears in a relatively narrow form: can company X transfer employee, customer, or supplier data to country Y? AI changes this perspective because data are rarely used for a single, isolated purpose. Instead, they may form part of broader processing environments, where information is collected, combined with other datasets, reused for model development, and refined over time. Although the principles of purpose limitation and data minimisation remain fully applicable under the GDPR, AI highlights the practical importance of lawful international data transfers in a way that traditional business processing often did not (Malgieri, 2022; Wachter & Mittelstadt, 2019).

The importance of transfer law becomes particularly visible in the development of large language models (LLMs). Modern foundation models are trained on extremely large collections of textual information originating from different jurisdictions. Developers increasingly use filtering techniques, synthetic data, and privacy-enhancing technologies to reduce the presence of personal data. Nevertheless, personal information may still appear in training datasets or during later stages of model refinement, evaluation, or fine-tuning (EDPB, 2024; Kuru, 2024). The European Data Protection Board (2024) has also recognised that the development and deployment of AI models raise important questions concerning the lawful use of personal data. As a result, the legal conditions governing international transfers remain relevant throughout different stages of AI development rather than only at the moment when data are initially collected. Healthcare AI provides another useful illustration. AI systems supporting medical imaging, disease prediction, personalised medicine, or clinical decision support frequently rely on cooperation between hospitals, universities, and research institutions located in different countries. Individual national datasets are often too small to ensure sufficiently representative training data, particularly for rare diseases or specialised medical applications. International data sharing can therefore improve the quality and reliability of AI systems, while also helping to reduce bias caused by geographically limited datasets (Anderson & Sutherland, 2024). Where research partners are established outside the EU, however, the absence of an adequacy decision may increase legal complexity because organisations must rely on alternative transfer mechanisms and assess whether additional safeguards are required following Schrems II (EDPB, 2021; Hallinan, 2024). A similar issue arises in relation to facial recognition and biometric AI. Such technologies generally require large and diverse image datasets in order to improve performance across different demographic groups. Since biometric data

used for identification constitute a special category of personal data under Article 9 GDPR, international transfers are subject to particularly strict safeguards. In practice, organisations established in third countries without adequacy status may therefore face additional legal and organisational requirements before such datasets can be transferred lawfully. These challenges have become more visible as European regulators have paid increasing attention to the risks associated with biometric surveillance and AI systems processing sensitive personal data (European Union Agency for Fundamental Rights, 2019; Regulation (EU) 2024/1689, 2024).

These examples should not be interpreted as suggesting that all AI development depends on unrestricted access to EU personal data. Many AI systems are trained using open datasets, synthetic data, anonymous information, or data generated entirely within one jurisdiction. Nevertheless, where AI systems require high-quality personal data collected across different populations or sectors, the legal framework governing international data transfers becomes part of the broader conditions under which innovation takes place. In this sense, adequacy decisions are relevant not only from the perspective of privacy protection but also because they may influence the legal environment in which cross-border AI research and development are organised.

4.2. The mismatch between a static legal model and dynamic data environments

A more structural issue also appears. The transfer framework of Chapter V GDPR was developed around a territorial logic. That logic remains understandable: the exporter is in the EU, the recipient is in a third country, and the legal issue is whether the receiving environment protects data sufficiently. Yet modern digital infrastructures are less linear. Data processing may be distributed, iterative, and remote. Access, storage, analysis, and model deployment may occur across multiple legal environments that do not fit comfortably within a simple exporter-recipient picture.

This does not mean that the GDPR is obsolete or incapable of addressing AI. It does mean that adequacy decisions now operate in a setting more complex than the one for which the original transfer model was designed. The law remains territorially framed, while the technological environment is often networked and continuous. The consequence is that adequacy acquires strategic significance. It is not merely a compliance shortcut. It can influence how technical and organisational infrastructures are built.

Malgieri (2022) argues more generally that data protection law faces difficulties when applied to automated and data-intensive processing environments. That observation is useful here. The challenge is not that the law has no principles. The challenge is that some of its mechanisms were designed

around assumptions that become harder to sustain in distributed technological systems. Adequacy, as a macro-level transfer mechanism, inherits this tension.

4.3. Implications for third countries seeking to participate in AI development

For third countries, the limited availability of adequacy decisions can have the following practical consequences.

First, it can increase the cost of lawful access to EU-origin personal data. These costs are not only legal fees. They may include repeated transfer assessments, supplementary safeguards, internal compliance programmes, and technical limitations on data use. For some companies this is manageable. For others, especially smaller firms, public research institutions, or actors in emerging innovation systems, it may be an important barrier.

Second, the absence of adequacy can reduce predictability. AI projects often require planning over a long period, cooperation between different entities, and stable data governance arrangements. Where transfer legality depends on complex and heavily qualified mechanisms rather than on an adequacy finding, the legal environment becomes more fragile.

Third, the limited network of adequacy-recognised jurisdictions may indirectly shape where collaboration, outsourcing, and infrastructure are concentrated. Of course, innovation depends on many factors, including talent, capital, public investment, local demand, and broader industrial policy. But where lawful access to EU data matters, adequacy may still influence the legal attractiveness of a jurisdiction. In that sense, adequacy is not only a privacy mechanism. It also forms part of the legal geography of innovation.

4.4. Adequacy and the extraterritorial application of the GDPR

The relationship between adequacy decisions and the extraterritorial scope of the GDPR deserves brief consideration. Under Article 3(2), the GDPR may apply directly to controllers or processors established outside the European Union where they offer goods or services to individuals in the Union or monitor their behaviour. Consequently, some organisations located in third countries are required to comply with substantive GDPR obligations even though their country has not received an adequacy decision.

This illustrates that adequacy and extraterritoriality pursue different objectives. Article 3 determines when the GDPR applies to particular organisations, whereas Chapter V regulates the conditions under which personal data may be transferred outside the European Union. Compliance with the GDPR by an individual company, therefore, does not eliminate the need for an appropriate transfer mechanism where personal data are exported to a third country (EDPB, 2023).

From a practical perspective, this distinction may not always be obvious. A technology company established outside the EU may comply with the GDPR

because it targets European users while simultaneously relying on SCCs or another transfer mechanism because its home jurisdiction has not obtained adequacy status. Adequacy, therefore, operates at the level of the legal system as a whole, whereas Article 3 concerns the territorial reach of EU data protection law to individual organisations. Questions of jurisdiction and questions of cross-border data movement should not be treated as identical, even though they often arise in the same factual situations (EDPB, 2023).

This distinction also illustrates the broader external influence of the GDPR. Through Article 3, EU data protection rules may apply beyond the territory of the Union. Through adequacy decisions, the EU also evaluates the legal systems of third countries before recognising that they provide an essentially equivalent level of protection. Although these mechanisms are different, together they contribute to the wider international influence of EU data protection law.

5. Critical assessment: protection, asymmetry, and regulatory legitimacy

A serious assessment of adequacy should avoid two overly simple positions. The first is to treat adequacy as a purely technical and neutral mechanism of rights protection. The second is to dismiss it as a form of disguised protectionism or legal imperialism. Neither view is fully convincing. The adequacy framework has a genuine constitutional and rights-protective logic, but it also produces broader structural effects that require closer analysis.

5.1. The protective logic of adequacy

From the perspective of fundamental rights, the protective logic of adequacy is strong. The transfer regime exists because personal data may be exposed to significant risks when it enters legal systems in which state access is disproportionate, oversight is weak, or remedies are ineffective (Lynskey, 2015; Kuner, 2013). The case law of the CJEU has consistently treated these risks as serious, and there is no persuasive reason to disregard them simply because global business or AI development might become easier under more permissive standards (*Data Protection Commissioner v. Facebook Ireland Ltd & Schrems*, 2020; *Schrems v. Data Protection Commissioner*, 2015). Any critical account that ignores this point would be incomplete.

5.2. Structural asymmetries and uneven accessibility

At the same time, adequacy clearly produces asymmetries. Countries that already have stable rule-of-law institutions, sufficiently funded supervisory authorities, and privacy-oriented regulatory cultures are more likely to meet EU expectations (Mc Cullagh, 2025; Regulation (EU) 2016/679, 2016, art. 45(2)). By contrast, countries undergoing regulatory transition may adopt modern data

protection legislation and still remain outside the adequacy framework for a long period. In practice, similar asymmetries also appear at the level of private actors. Large multinational companies are usually better placed than smaller organisations to cope with the absence of adequacy through standard contractual clauses and supplementary measures (EDPB, 2021). These effects do not make the framework illegitimate, but they do show that it is not neutral in its practical consequences.

This is where a more nuanced critique becomes possible. The problem is not simply that adequacy is “too strict.” Rather, the problem is that the route towards adequacy may be lengthy, uncertain, and unevenly accessible. Essential equivalence is a defensible standard, but from the perspective of third countries it may be difficult to know how much legislative approximation, institutional strengthening, or reform of surveillance law will actually be sufficient in practice. Recent scholarship argues that greater transparency in the adequacy assessment process would improve legal certainty for third countries without lowering the substantive level of protection required by the GDPR (Mc Cullagh, 2025; Czerniawski, 2024).

The literature on EU external regulation helps to explain this point further. Bradford (2020) describes the Brussels Effect as a process through which EU rules influence global behaviour because alignment with the EU is economically beneficial. In the field of data protection, this can be seen in the spread of GDPR-inspired legislation. At the same time, the adequacy framework also shows the limits of legislative imitation. Reproducing definitions or individual rights is not enough if deeper institutional conditions are absent. This suggests that EU influence in this field may be strongest where a country already has the administrative and constitutional capacity to absorb it. Recent scholarship has also begun to examine adequacy in the wider context of AI governance. As AI systems increasingly depend on cross-border access to data, transfer rules influence not only privacy compliance but also innovation ecosystems and international regulatory cooperation. Rather than viewing adequacy solely as a technical transfer mechanism, recent literature increasingly treats it as part of the broader governance framework shaping trustworthy AI and international digital trade (Bradford, 2023; Veale & Zuiderveen Borgesius, 2021).

5.3. Legitimacy, transparency, and the path towards adequacy

A related question concerns legitimacy. Is it legitimate for the EU to assess foreign legal systems according to a standard anchored in its own constitutional order? In one sense, yes. The EU has a legitimate interest in ensuring that the level of protection guaranteed to persons in its legal order is not undermined by external transfers. In another sense, however, the practice remains politically sensitive because adequacy judgments affect countries with different traditions and priorities. The legitimacy of the framework, therefore, depends not only on the substantive standard, but also on the fairness, consistency, and

transparency of the assessment process (Czerniawski, 2024; Mc Cullagh, 2025). In practical terms, this suggests that the future of adequacy should not be discussed only in terms of “more” or “less” strictness. A better question is whether the process of working toward adequacy can be made more predictable without diluting the core rights standard. More detailed public reasoning in adequacy decisions, clearer pathways for regulatory dialogue, and more transparent identification of the reforms needed in prospective adequacy countries could make the system more predictable while preserving its protective aim. Recent scholarship argues that greater transparency in the adequacy assessment process would improve legal certainty for third countries without lowering the substantive level of protection required by the GDPR (Mc Cullagh, 2025; Czerniawski, 2024).

This issue is especially relevant for countries outside the existing adequacy network that are currently strengthening their privacy frameworks. For such countries, adequacy may function as a long-term strategic objective. Yet if the framework is experienced as opaque or politically contingent, the incentive structure becomes weaker. In that sense, making the route to adequacy clearer is not only a matter of administrative fairness. It may also support stronger data protection globally. AI gives this debate additional urgency because it makes visible the practical consequences of uneven access to data. When access to EU-origin personal data depends on whether a jurisdiction benefits from adequacy or must rely on more uncertain alternatives, the transfer regime becomes part of the broader political economy of innovation. The paper’s point is not that adequacy alone determines technological outcomes. It is that transfer law, often treated as a specialised compliance question, has wider consequences than is sometimes acknowledged.

Conclusion

This paper examined adequacy decisions under Article 45 GDPR as a central mechanism of EU transfer law and asked how their limited availability affects access to EU personal data for third countries, especially in the context of AI. The analysis showed that adequacy occupies a privileged place within Chapter V GDPR because it allows data to move without the case-by-case burdens associated with alternative transfer tools. At the same time, adequacy is demanding because it requires a broad assessment of legislation, institutions, remedies, and public-authority access in the third country.

The concept of essential equivalence, as developed in Schrems and Schrems II, explains both the value and the difficulty of adequacy. It preserves flexibility by not requiring identical legal systems, but it also makes adequacy a systemic and exacting form of evaluation. Existing examples such as Japan and the United Kingdom show that adequacy is achievable, but usually where

institutional capacity, legal continuity, or sustained regulatory dialogue are already present. For many other countries, the path is more difficult.

The paper further argued that in the age of AI, this matters more visibly than before. AI does not replace transfer law, but it makes more apparent that lawful access to data can shape conditions of participation in innovation. The absence of adequacy does not make transfers impossible, but it can make them more uncertain, costly, and fragmented. In that sense, adequacy decisions are both protective and structuring. They protect fundamental rights, but they also help structure the legal geography of global data flows.

The following conclusion follows. The adequacy framework should not be weakened simply for the sake of convenience. Its rights-protective logic remains justified. However, if adequacy is to function as a credible and legitimate gateway rather than as a narrowly accessible status, greater attention should be given to the transparency and predictability of the path toward adequacy. This would not remove all asymmetries, but it could make the framework easier to understand and, perhaps, more effective in supporting both rights protection and fairer participation in the global digital economy.

References

- Anderson, B., & Sutherland, E. (2024). Collective action for responsible AI in health. OECD Artificial Intelligence Papers, No. 10. OECD Publishing. <https://doi.org/10.1787/f2050177-en>
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press. <https://doi.org/10.1093/oso/9780190088583.001.0001>
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press. <https://doi.org/10.1093/oso/9780197649268.001.0001>
- Czerniawski, M. (2024). Shrouded in secrecy – does the comitology procedure for GDPR adequacy decisions fit its purpose? *Masaryk University Journal of Law and Technology*, 18(2), 215–244. <https://doi.org/10.5817/MUJLT2024-2-3>
- Data Protection Commissioner v. Facebook Ireland Ltd & Schrems, Case C-311/18, EU:C:2020:559 (2020).
- De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?

- Computer Law & Security Review, 32(2), 179–194.
<https://doi.org/10.1016/j.clsr.2016.02.006>
- European Commission. (2019). 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. Official Journal of the European Union, L 76, 1–58.
https://eur-lex.europa.eu/eli/dec_impl/2019/419/oj
- European Commission. (2021). 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. Official Journal of the European Union, L 360, 1–68. https://eur-lex.europa.eu/eli/dec_impl/2021/1772/oj
- European Commission. (2023). Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan (COM(2023) 275 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023DC0275>
- European Commission. (2025). Commission Implementing Decision (EU) 2025/2574 of 19 December 2025 amending Implementing Decision (EU) 2021/1772 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom. Official Journal of the European Union, 2025/2574. https://eur-lex.europa.eu/eli/dec_impl/2025/2574/oj
- European Data Protection Board. (2021). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
- European Data Protection Board. (2023). Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (Version 2.0). https://www.edpb.europa.eu/documents/guideline/guidelines-052021-on-the-interplay-between-the-application-of-article-3-and-the_en
- European Data Protection Board. (2024). Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models. https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-282024-on-certain-data-protection-aspects-related-to_en?
- European Union Agency for Fundamental Rights. (2019). Facial recognition technology: Fundamental rights considerations in the context of law enforcement. <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>

- Hallinan, D. (2024). The concept of international health research adequacy decisions. *International Data Privacy Law*, 14(4), 377–390. <https://doi.org/10.1093/idpl/ipae019>
- Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199674619.001.0001>
- Kuru, T. (2024). Lawfulness of the mass processing of publicly accessible online data to train large language models. *International Data Privacy Law*, 14(4), 326–351. <https://doi.org/10.1093/idpl/ipae013>
- Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.
- Malgieri, G. (2022). Automated decision-making and data protection in Europe. In G. González Fuster, R. Van Brakel, & P. De Hert (Eds.), *Research handbook on privacy and data protection law* (pp. 433–448). Edward Elgar Publishing. <https://doi.org/10.4337/9781786438515.00028>
- Marelli, M. (2024). Transferring personal data to international organizations under the GDPR: An analysis of the transfer mechanisms. *International Data Privacy Law*, 14(1), 19–36. <https://doi.org/10.1093/idpl/ipad022>
- Mc Cullagh, K. (2025). EU adequacy assessments: Evolving criteria, political tensions, and the push for a global data standard. *Common Market Law Review*, 62(3), 879–912. <https://doi.org/10.54648/cola2025045>
- 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 (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). (2024). *Official Journal of the European Union*, 2024/1689. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Schrems v. Data Protection Commissioner, Case C-362/14, EU:C:2015:650 2015
- Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/cr-2021-220402>
- Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019(2), 494–620. <https://doi.org/10.7916/cblr.v2019i2.3424>