UNIVERSITY OF TARTU

SCHOOL OF LAW

Department of Public Law

Namık Berk Vurkır

VIABILITY OF EXISTING METHODS FOR INTERNATIONAL DATA TRANSFERS BETWEEN THE EU AND US

Master's Thesis

Supervisor

Anna-Maria Osula, PhD

Tallinn

2024

ACKNOWLEDGMENTS

This thesis is dedicated to the late Colonel Mete Vurkır, whose experiences inspired me to embark on a career in law, it was his last wish to see me graduate.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
GDPR	General Data Protection Regulation
US	United States of America

INTRODUCTION

Privacy is a fundamental concept that is interconnected with other areas of law, and although it may seem to develop independently, it has unique characteristics that can directly impact them at any moment. When the so-called third industrial revolution happened, and technological advancements resulted in the creation of digital solutions that require digitalized personal information to function[1], this characteristic of privacy became more apparent and led scholars to argue its vitality to business operations.[2] Today, the importance of personal data can be seen from the corporation's desire to leverage data collected from users with sophisticated collection practices. However, as much as the general concept, this new relationship between international trade, business, and privacy has also directed scholars' attention to the transborder data flows (or, as we know it today, international data transfers).

The earliest arguments defined the concept by establishing specific requirements like; transferring the data between two different jurisdictions, storing it in a database physically located in a territory other than the exporting country, and processing the data outside the exporting state.[3] Also, in addition to these, the scholars pointed out at the challenges of these transfers, like the lack of supervision of the transfers and regulation of data processing activities located in a country beyond the supervision of another.[4] Even though they were limited by the technological advancements of their time, the definitions and arguments made by scholars in the past still hold relevance today. Naturally, as time has passed, the narrative regarding the legal and technical problems has evolved, but they still served as the foundation for new discussions and debates that were fuelled by further advancements in technology.

One of these discussions involves the government's surveillance practices. Even before the digitisation of personal information, the relationship between privacy and surveillance was already subject to debates on how they should be treated by law. While surveillance is generally justified as an important tool to combat crime and terrorism, there have always been arguments regarding the violation of privacy of personal life and the need to balance.[5] Though, governments are now leveraging and using the abundance of personal data for their

[1] See Kunii, Tosiyasu L., "The 3rd industrial revolution through integrated intelligent processing systems" IEEE International Conference on Intelligent Processing Systems Vol.1, Cat. No. 97TH8335 (1997)
[2] Eger, John M. "Emerging restrictions on transnational data flows: privacy protection or non-tariff trade barriers." Law & Pol'y Int'l Bus. 10 (1978): p 57-64
[3] Novotny, Eric J. "Transborder Data Flow Regulation: Technical Issues of Legal Concern, 3 Computer LJ 105 (1981)." UIC John Marshall Journal of Information Technology & Privacy Law 3.1 (1981): p 106 para 3
[4] ibid, at p 107 para 2
[5] See Posner, Richard A. "Privacy, surveillance, and law." U. Chi. L. Rev. 75 (2008)

national security programs, adding more on top of the age-old problem. Scholars have raised concerns about the government's free access to personal data and the possible consequences of these surveillance programs, such as mapping out individuals' behaviours, attributes, resources, associates, and beliefs[6], which, without proper authorisation, is a clear violation of privacy.

This new facet of the topic especially gained attention after the Snowden Revelations, where Edward Snowden leaked the details of the United States (hereinafter "US") surveillance program to the public, exposing the relationship between the government and US corporations and describing how the US government uses personal data[7], making the connection with international data transfers. Some countries have responded to this news with localisation of data, reasoning it as a way to secure specific types of personal data by keeping them within their physical borders. However, the utilisation of data localisation has led to increased arguments regarding its impact on individual rights, claiming that it is serving as a catalyst for domestic and foreign surveillance programs instead of preventing it and also providing governments with the possibility to be used for political repression.[8] In addition to national security programs and associated legal complexities, the advancements in technology have led to resurfacing of an old topic: data security.

The significant increase in outsourcing since the 2010s and the widespread adoption of remote working since 2020, combined with the idea of data localisation, raised awareness regarding data security during international data transfers. Now, due to business and economic strategies, personal data is being handed over to third parties more often than a decade ago[9], and even though a company may be established in a specific country, it can have employees on another continent[10], which means they require constant data transfers between different countries, indicating that the sudden increase in the number of data transfers and individuals involved in these transfers is the main source of concern.

---

[6] Cate, Fred H. "Government data mining: The need for a legal framework." Harv. CR-CLL Rev. 43 (2008): p 436 para 4

[7] See von Solms, Suné, and Renier Van Heerden. "The consequences of Edward Snowden NSA related information disclosures." ICCWS 2015—The Proceedings of the 10th International Conference on Cyber Warfare and Security: ICCWS2015. (2015)

[8] Fraser, Erica. "Data Localisation and the Balkanisation of the Internet." SCRIPTed 13 (2016): p 363-367

[9] Iqbal, Zafar, and Aasim Munir Dad. "Outsourcing: A review of trends, winners & losers and future directions." International Journal of Business and Social Science 4.8 (2013); p 96 para 2

[10] Nurse, Jason RC, et al. "Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy." HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part III 23. Springer International Publishing, (2021); p 585-588

Primarily, fears about breaches were stemming from the increased involvement of third-party service providers and the potential misuse of personal data.[11] While this strengthened the connection between international data transfers and the importance of data security, it has also shown that the issues pertaining to international data transfers are no longer only sourced by the national authorities or limited to the incompatibilities with regulatory frameworks; the source of the issues is now extended to third parties who are willingly receiving personal data, and other stakeholders like Internet Service Providers (hereinafter "ISPs"), who are initiating and realising these transfers.

The European Union (hereinafter "EU") has been battling against these issues for the past 30 years. Throughout this journey, the lawmakers of the EU have created two different legal frameworks, namely; the Data Protection Directive and its successor, the General Data Protection Regulation (hereinafter "GDPR"). They have also cooperated with their biggest trade partner, the US, and created three specialised legal instruments for the realisation of safe data transfers between each other. However, despite the long history of privacy laws in the EU, predecessors of existing frameworks have displayed vulnerabilities against the issues debated by scholars.

For example, DPD has failed to ensure the protection of personal data after their transfer since its boundaries were the jurisdiction that it clashes with[12], and the first two of the specialised data transfer instruments, Safe Harbor and EU-US Privacy Shield, have failed to protect personal data against the surveillance practices of the US and resulted with their invalidation.[13] DPD have been replaced with GDPR, and a third instrument named Data Protection Framework (hereinafter "DPF") was created. Although GDPR imposes stricter rules than DPD, it does not cover data security aspects of international data transfers beyond mandating "appropriate technical and organisational measures"[14] leaving the question of what is 'appropriate' measures.

[11] Weber, Rolf H. "Transborder data transfers: concepts, regulatory approaches and new legislative initiatives." International Data Privacy Law 3.2 (2013): p 118 col 2 para 2

[12] Maximillian Schrems v Data Protection Commissioner, Case C-362/14 (CJEU, 6 October 2015); para 44-45 [hereinafter "Schrems I"].

[13] See Tzanou, Maria. "Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights." Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, Hart Publishing, Forthcoming (2020)

[14] Council Regulation, [EC] No 2016/679 General Data Protection Regulation, Regulation OJ L 119/1 (25 May 2018); Article 32 [hereinafter "GDPR"]

Furthermore, despite the fact that it is claimed that DPF provides protection of personal data after its transfer[15], the US executive order on surveillance, which has been addressing surveillance concerns that have been raised in the EU, only limits the scope of the surveillance activities to a certain extent.[16] On top of these, the US has a complicated legal system called "the Patchwork of Laws"[17], which only provides protection for certain types of data that are in possession of specific kinds of entities, meaning the legal protections in the US are limited. And, at the time of writing, only 13 of the 50 states are providing protections for personal data[18], which raises questions over the legal landscape in the US and also how the EU legal framework is interacting with this landscape.

The history between both countries shows that there is a significant effort to ensure the protection of personal data. In particular, the EU, which recognises privacy as a human right[19] and has developed its current data privacy laws as an extension of it, is particularly struggling to keep its virtual borders open and provide adequate data protection for its subjects. Despite the efforts, it is still unclear if the current setup between the EU legal framework and the US legal landscape addresses longstanding concerns that have been subject to discussions for a decade. Therefore, the objective of this thesis is to delve into the intricacies of the challenges associated with international data transfers, specifically examining how the existing framework governing these transfers between the EU and the US addresses these challenges.

The paper will delve into the technical aspects of international data transfers and the interoperability of legal frameworks, through a critical examination of existing literature. It will outline the elements involved in an international data transfer and pinpoint when each legal challenge occurs during its realization. Furthermore, the analysis will adopt the perspective of the EU and begin by examining the components of EU law, identifying which of these components may cause issues with the corresponding legal frameworks. It will then proceed to inspect the existing transfer methods between the US and the EU, assessing their

[15] European Commission, "Data Protection: European Commission adopts new Adequacy Decision for safe and trusted EU-US data flows" (10 July 2023) available at < https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721 > [accessed 3 March 2024]
[16] The White House "Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities." Order no. 14086, Federal Register (7 October 2022): p 5-9 [hereinafter "Executive Order"]
[17] Heck, Zachary S. "A Litigator's Primer on European Union and American Privacy Laws and Regulations", 44 LITIG.59, 59 (2018); p 59
[18] International Association of Privacy Professionals, "US State Privacy Legislation Tracker", (1 March 2024) available at < https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ > [accessed 3 March 2024 – hereinafter "IAPP Tracker"]
[19] European Convention on Human Rights (as amended), 213 UNTS 222, (3 September 1953); Article 8 (1) [hereinafter "ECHR"].

longetivity. While the paper will demonstrate aspects of a qualitative research method, it will follow a textualist approach to access every relevant detail on the laws related to these concerns and provide arguments for answering the following research questions:

- How do the legal and technical complexities of international data transfers interact with each other?
- What are the main aspects that cause complexities and challenges associated with the transfer of data internationally, particularly from the European Union to the United States?
- What are the limitations of the GDPR mechanisms for data transfers, and how effective are these mechanisms in practice?

To provide a comprehensive narrative and construct proper foundations for answering the research questions, the First Chapter of this thesis will establish the elements of data transfers. The Chapter will review the characteristics and technical aspects of domestic data transfers and then distinguish the additional variables involved in international data transfers. It will then examine how international data can be transferred between two entities, identify the flow, and highlight complexities that arise with the involvement of third parties. Both technical and regulatory aspects of data transfers will be covered in this part while potential issues will be identified for the arguments that will be presented in the upcoming Chapters. The final section of the Chapter will then delve into how subjective the definition of international data transfers has been. This section will explore the definitions that have been used in academia and by various institutions of the EU while also touching upon the impact of these definitions on the application of the laws. It will then proceed to present its own definition, constructed in a way that individually corresponds to the characteristics and technicalities outlined in earlier sections of the Chapter.

The Second Chapter will delve into the various tools created by the GDPR for data transfers. It will explore their effectiveness and the different aspects and notions that impact their application in the foreign jurisdiction. This Chapter will also examine the link between international data transfers and the provisions of the GDPR, particularly the core principles, uncover their impact through hypothetical scenarios and establish how they affect the efficiency of the transfer tools. It will also discuss the challenges faced when applying these core principles in foreign jurisdictions and the obstacles that arise when attempting to apply them across borders. Finally, this chapter will conclude with an analysis of how GDPR

responds to situations that do not comply with its principles. It will categorize these situations based on their characteristics and provide individual explanations of how they affect different countries.

In the third and Final Chapter, the paper will utilise the arguments from previous Chapters to delve into the issues arising from data transfers from the EU to the US. Considering the perspective and position of the paper, it will first address the requirements set forth by the EU for the facilitation of data transfers and explain the reasoning behind them. The subsequent sections of the Chapter will continue to utilise the same methodology. The upcoming discussions will focus on various scenarios involving the transfer of data, which can be carried out using the tools provided by the GDPR. These tools include transfer by adequacy decision, transfer by standard contractual clauses, and transfer by binding corporate rules. In addition, there will be discussions on voluntary self-assessments that have emerged from EU-US cooperation.

The paper will conclude by explaining the interrelation between technicalities and legal complexities, the impacts of variations in data protection laws, the extent of effectiveness of remedies designed for data transfer between the EU and the US, and the issues concerning these remedies.

CHAPTER I: LEGAL AND TECHNICAL INTERPLAY OF DATA TRANSFERS

1.1 Characteristics and Technical Aspects of a Data Transfer

During the early days when privacy was being conceptualized, data transfers were limited to direct physical contact or connection to nearby small networks called the Local Area Networks.[20] Today, we have different technologies that are able to transmit data from one place to another. From old-school broadband to various radio-based terrestrial wireless solutions to the utilisation of multi-distance orbit satellites,[21] the choice of transmission method or the possibility of a combination of techniques is plenty. However, since the scope of this thesis is not entirely related to the technicalities of telecommunications but its impact on privacy-related affairs, this chapter will illustrate a simplified outline of the landscape by providing information on packet-based networks to set a foundation for future arguments, as the circumstances demonstrated with these networks will apply to other transmission methods that are available today. The main purpose of this introduction is to illustrate how virtual borders and physical borders do not align and how this interplay impacts data protection and privacy laws while regulating interactions within the virtual domain.

In terms of privacy affairs, we could describe a data transfer as its technical definition; the act of sending and receiving data from one person or entity to another.[22] However, this description would only superficially summarize the whole structure of data transfers and fail to convey what is included in each necessary step to realise them. Additionally, it would not adequately demonstrate the process of data transfer between individuals or specify who is the primary parties that are initiating the transfer, who are the responsible parties among them, and how the responsibility is distributed between them. While it also neglects to identify any third parties that may be involved in the transfer process and how their involvement could potentially impact the data transfer, it would also fail to determine which jurisdiction becomes applicable to which party and at what time. As it will be explained in the next Chapters, all of these must be taken into consideration to efficiently regulate privacy related matters, and considering its cruciality, we must first thoroughly understand what a data transfer entails before delving into the topic of international data transfers.

---

[20] Clark, David D., Kenneth T. Pogran, and David P. Reed. "An introduction to local area networks." Proceedings of the IEEE 66.11 (1978): p 1498 col 2 & 1499 col 1.
[21] Su, Yongtao, et al. "Broadband LEO satellite communications: Architectures and key technologies." IEEE Wireless Communications 26.2 (2019): p 56 col 1 para 3.
[22] Walker, Stuart D., et al. "Data transmission." The Cable and Telecommunications Professionals' Reference. Routledge (2012); p 29 para 1.

1.1.1 Domestic Data Transfers

Regardless of whoever initiates a data transfer, unless a direct private network is involved between the interactions of the parties, these transfers usually occur within wide-area networks (hereinafter "WANs"), which cover a broad area and may connect across metropolitan, regional, or national boundaries.[23] It is crucial to make the distinction that WAN is a definition for identifying an extensive network,[24] and every WAN does not have to display the same characteristics because they have the potential to cover a single country or multiple countries at the same time. This characteristic of WAN is applicable to other methods of telecommunications as well, as WAN networks stack numerous networks on top of each other.

To best illustrate the differences between each WAN and how the networks are stacked, we can inspect the Internet in detail. As Sam Kelly says, "The Internet is a global network of computers. Every computer that is connected to the Internet is considered a part of that network"[25] though no matter if every computer and network connected to the Internet is considered to be part of the Internet, it would make the composition and size of the Internet a virtual construct. This is because there are no dedicated physical networks created exclusively for the Internet; the capability of the Internet to connect computers across the globe is due to its virtual networking architecture, encompassing several large physical networks in different continents made of smaller networks, which are interconnected through various means.[26]

While this unique structure allows us to consider the Internet as a single WAN[27], it also shows the virtual and physical distinction of such networks since the other large networks included on the Internet are also considered WANs on their own scale because they are composed of smaller networks. However, with this example, no matter if we have an understanding of how big the potential size of a WAN could be, it is still essential to grasp the structure of a WAN in detail, because it provides information on how it spreads across various geographical locations and interplays with different jurisdictions.

---

[23] Zhang, Yan, et al. "On wide area network optimization." IEEE Communications surveys & tutorials 14.4 (2011): p 1090 col 1 para 3.
[24] Cloudflare. "What is a WAN? Understanding Wide Area Networks." (2023); para 2 available at < www.cloudflare.com/en-gb/learning/network-layer/what-is-a-wan/> [accessed 21 March 2024].
[25] Kelley, Sam. "Global Network System" Bibliotex Digital Library (2022); p 1 para 1.
[26] Wang, Feng, and Lixin Gao. "Interdomain Routing and Reliability." Guide to Reliable Internet Services and Applications (2010): p 181 para 1.
[27] Pine, John C. "Technology and Emergency Management". John Wiley & Sons, (2017): p 39 para 1.

The smaller networks that WAN's coverage is dependent on are also divided in accordance with their own coverage. Following the size and the type of area the network covers, they are either called metropolitan area networks (hereinafter "MAN") or regional area networks (hereinafter "RAN"). A RAN is larger compared to a MAN, and as the name suggests, MANs cover urban areas, while RANs cover larger areas including municipal regions and rural areas that are not covered by a MAN.[28] Considering this distinction and WAN's potential to virtually cover more than one country, one of the additional benefits of determining the smaller networks in such a way is that it makes it easier to distinguish where the transfer is physically happening.

These networks are supported by the frameworks provided by different or the same big telecommunication companies but are always managed by specialised entities called ISPs, which facilitate communication-related operations.[29] It is important to note that not all networks are required to operate on the same physical network framework owned by a single telecommunications company; while there can be multiple ISPs on a single network framework, there could also be only one ISP which occupies the whole network. Naturally, in such cases, ISPs will require direct connections to allow communication between different networks, and as will be demonstrated in Figure 2 and further in Figure 6, this situation allows for the involvement of more than one ISP in the process of a data transfer, because the data may need to be forwarded to a recipient who falls outside coverage of the physical framework of the originating ISP's network.

Initiation of a domestic data transfer happens two-fold, and it is relatively simple when compared to an international data transfer. The first part occurs between the initiating party and the ISP, and the second part happens between the ISP and the receiving party. The first part begins in the terminal of the initiating party, where the personal data must be first turned into an electronic package and be prepared for transmission through a connection established with their ISP.[30] This process typically occurs automatically and adheres to universal protocols through the interface utilised by the initiating party, additionally, the package may

[28] IEEE Computer Society. LAN/MAN Standards Committee, International Electrotechnical Commission, and IEEE Standards Board. "Information technology --Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Overview and Architecture" No. 802. IEEE, (2015); p 8.
[29] Doverspike, Robert D., K. K. Ramakrishnan, and Chris Chase. "Structural overview of ISP networks." Guide to Reliable Internet Services and Applications (2010): p 19 para 1.
[30] Kalmanek, Charles R., Sudip Misra, and Yang Richard Yang, eds. "Guide to reliable internet services and applications". Springer Science & Business Media (2010): p 19 para 1.

be encrypted to ensure security and privacy[31], but, as will be explained in Chapter III, it does not guarantee the expected protection. Regardless, once the electronic package is prepared for transmission, it will be released to the originating network from the terminal, making its way to the ISP and concluding the first part of the transfer. The second part of the transfer is almost identical to the first part. The only difference is that the ISP locates the terminal of the recipient and then repeats the same steps in reverse, concluding the second part and the data transfer by delivering the package.

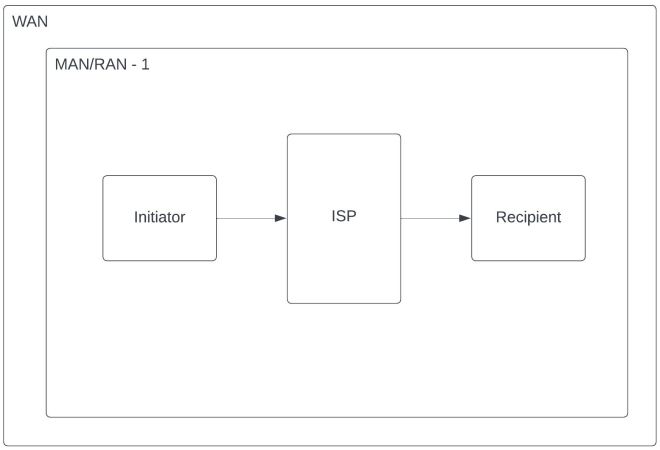

Figure 1: Domestic Data Transfer Between Two Parties in the Same Network

The reason why this package does not head to the recipient directly from the initiating party is that the involvement of an ISP is required for locating the recipient in the network and transmitting it because it manages the traffic within the network and must direct the flow of package inside and outside the network to do that.[32] As will be explained further in the next pages, aside from being a technical necessity, there are additional benefits to this, especially with international data transfers. For example, if the package is sent to a network outside the physical borders, the location of the recipient would be guaranteed in the foreign network, and it will be easy to distinguish when the personal data has left the national borders.

Regardless, it is important to note that this two-part process is only applicable in situations where the initiating party and the receiving party are on the same network. In cases when they are not in the same network, the involvement of only one ISP becomes insufficient since

[31] Popek, Gerald J., and Charles S. Kline. "Encryption and secure computer networks." ACM Computing Surveys (CSUR) 11.4 (1979): p 346.
[32] Terzis, Andreas, et al. "A two-tier resource management model for the Internet." Seamless Interconnection for Universal Services. Global Telecommunications Conference. GLOBECOM'99.(Cat. No. 99CH37042). Vol. 3. IEEE, (1999): p 1780 col 2 para 3.

the originating network does not cover both the Initiator and the Recipient. This means that interaction with other ISPs will be necessary to handle the transmission, and the transfer process becomes technically more complicated because the package that has been sent to the originating network's ISP cannot be forwarded directly to the recipient as initially planned. Therefore, the originating ISP will be required to forward the package to another ISP and add another layer to the process. The same circumstances are also applicable when the package is being transferred internationally because the ISP of the originating network will be required to route the data to the ISP of the receiver's network during both cases, which is the only way to transmit the data to the receiver on behalf of the originating ISP.

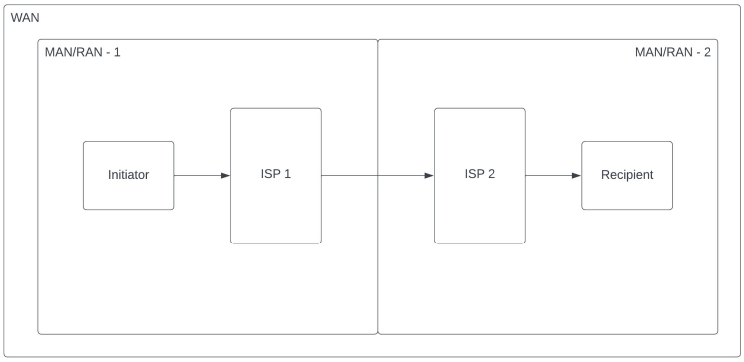

Figure 2: Domestic Data Transfer Between Two Parties in Different Networks

After analysing the Figures provided for both scenarios, where parties within the same country initiate a transfer, it can be concluded that a clear legal distinction can be made for regulatory purposes. This is because the execution of the transfer in the virtual domain and the composition of the network in the physical domain both fall under the jurisdiction of the same country. Thus, the parties involved in the transfer can be identified accurately, and their responsibilities can be easily allocated according to the scope of the law. Even when the Initiator communicates with the Recipient through an instant messaging application or an email service provider located in another domestic network, these circumstances will remain and keep the legal affairs relatively simple since the only thing that will change during the transfer will be the number of networks used and the number of ISPs that were involved. Consequently, there will be no significant impact on the identification of the third-party service provider and assigning corresponding responsibilities.

However, this minor adjustment makes a significant change in the technical process of transferring the data because the Initiator must first make a request to the Service Provider, then forward the electronic package through the originating network’s ISP and have it

delivered to the Service Provider with another ISP, the Service Provider will then process this request and forward it to the Recipient on behalf of the Initiator by sending it to the ISP of its own network. This means that the transferring procedure that involves a third-party service provider will place the Service Provider in the middle of communication like an intermediary, and the whole two-step process previously described in Figure 1 will be required to be repeated twice for all sides of the transmission.

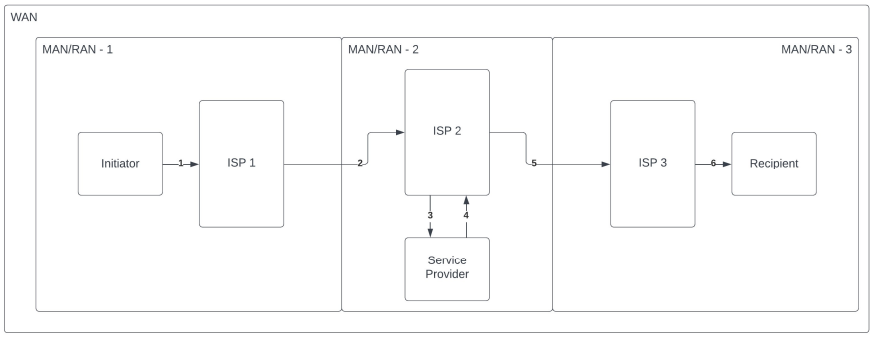

Figure 3: Domestic Data Transfer Including a Third-Party Service Provider

The Figure above illustrates data being transferred domestically through a third-party application; the process is linear in the technical sense, and the entire data processing cycle takes place within the physical and virtual jurisdictional borders of the same country. As previously referred, these additional steps are manageable in domestic transfers from a legal perspective and will not have a significant impact on regulatory affairs, but they become much more substantial when transferring the data internationally. As will be explained in the next Sub-section, although these changes may appear insignificant and presumed to have little impact, the involvement of third parties located in other jurisdictions during the transfer process increases regulatory exposure which could affect how data protection should be facilitated.

Consequently, determining the applicable jurisdiction and enforcing rules in the corresponding jurisdiction would be difficult because the virtual domain is not identical to the physical domain, and territorial sovereignty is the base of the jurisdiction.[33] This means there will be circumstances where overlapping happens between the jurisdictions. Furthermore, if we also consider that the concept of transferring does not only involve the complete movement of an electronic file from one terminal to another or the process of creating an

[33] Osula, Anna-Maria. "Transborder access and territorial sovereignty." Computer law & Security review 31.6 (2015): p 719-735.

electronic copy but also viewing it remotely, the situation becomes even more complicated due to the technical nature of these actions.

1.1.2 Differences of an international data transfer

It was illustrated in Figure 2 and Figure 3 that when the data is sent to a recipient in another network, the ISP of the originating network transmits the data to the ISP of the Recipient after locating its network. A similar process happens with international data transfers, until the moment the package reaches the ISP of the originating network. Once the package is delivered to this ISP, differences arise, because no matter whether international data transfers are similar to domestic data transfers from the technical point, the interactions that are necessary for facilitating the data transfers are no longer taking place within a WAN. The interactions concerning the data transfer now occur between various WANs, where it starts and ends in different MANs and RANs that are physically located in other countries.

This means that the originating ISP will have to take a more complicated route compared to domestic transfers and navigate through different networks until it can arrive at the destination ISP that is operating the network of the Recipient. Usually, to do this, the package must end up in the Internet Backbone, which is "a collection of large networks owned by communication companies"[34], connecting different WANs with each other. However, before that, the data package must traverse between three tiers of ISPs. The name given to each tier may vary in the literature, but they are always listed in ascending order, and their position in the hierarchy is always the same and determined by their relationship with other ISPs and the geographical area they physically cover.[35]

The type of ISPs, which include those operating the networks of both the initiating and receiving parties, are categorised as "Tier 3" ISPs, and their networks are significantly limited in scope compared to those of the other two tiers.[36] They are usually the ISPs that manage the MANs, however, it is not uncommon that some of them also have direct control over RANs. It is worth mentioning that these ISPs are always the starting and ending point of any data transfer because the Initiators and the Recipients are located in the networks operated by these ISPs. Regardless, the Tier 3s are dependent on "Tier 2" ISPs, as these ISPs connect

[34] Pine (n 27): p 23 para 2.
[35] Winther, Mark. "Tier 1 isps: What they are and why they are important." IDC White Paper (2006): p 3 at Figure 1.
[36] ibid, p 5 para 2

different geographical regions of a country together by providing infrastructure and telecommunication-related services to the Tier 3 ISPs that are physically within the coverage of their network.[37] We can view them as the second third party that gets hold of the personal data when an international data transfer is taking place, however, they are just a transit, and they do not directly deal with the data. Similar to their relationship with the Tier 3s, the Tier 2s are dependent on the "Tier 1", which is the largest among all tiers, as they own a constellation of large networks that directly connect different Tier 2s with each other within their physical and virtual network.[38] As a result of this, the Tier 1s are the main actors that are facilitating the data transfers between countries.

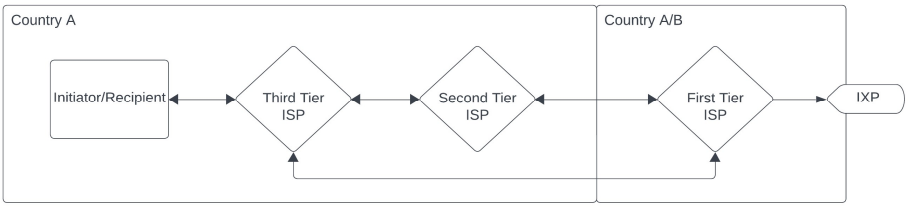

Figure 4: A linear overview of ISP Tier's Hierarchy

An essential trait that further distinguishes ISP Tiers from each other is that Tier 1 and Tier 2 ISPs usually do not provide direct services to the end-user like the Initiators and the Recipients as Tier 3s do because, unlike Tier 3s, the clients of these Tiers are the ISPs that are a tier lower than themselves, which creates a pyramid-like structure, fundamentally makes them framework service providers.[39] This is also the reason why direct connections between Tier 3 and Tier 1 are not so common, and there is almost always a Tier 2 as a transit between them. Furthermore, what makes Tier 1s different from Tier 2s is that they may have a connection to the Internet Exchange Points (hereinafter "IXP"), which makes them a gatekeeper connecting the networks under it to the so-called Internet Backbone[40], as demonstrated in Figure 4. However, it is important to mention that the connections of networks are not as linear as they are illustrated in this Figure; usually, there are multiple Tier 2s under a Tier 1 and numerous Tier 3s under Tier 2s, which may or may not have a

[37] Winther (n 35)
[38] Sharma, Ashlesh, et al. "On the rise and fall of ISPs." Proceedings of Netecon 9 (2009); p 10 col 2 para 4.
[39] Winther (n 35)
[40] Xu, Kuai, et al. "On properties of internet exchange points and their impact on as topology and relationship." International Conference on Research in Networking. Berlin, Heidelberg: Springer Berlin Heidelberg, (2004); p 284-286.

connection between each other but are always connected to an ISP of a higher tier and forming the large virtual network.

Consequently, this explains to us that personal data is always transmitted between these tiers when an international data transfer is happening because the only way to the destination network is through their Tier 1. However, this does not mean that the package will be directly sent to the destination network when the package reaches a Tier 1 because even the Tier 1s may require assistance from other neighbouring Tier 1s to realise the desired transfer since not all Tier 1s have direct access to each other or to an IXP.[41] In such circumstances, the only way to reach the destination network is through transmitting the package between the neighbouring Tier 1s until it reaches the destination network or to a Tier 1 with a connection to IXP and benefits from their access.[42] This means the personal data may have to get through the jurisdiction of a third or fourth country when an international data transfer is taking place.

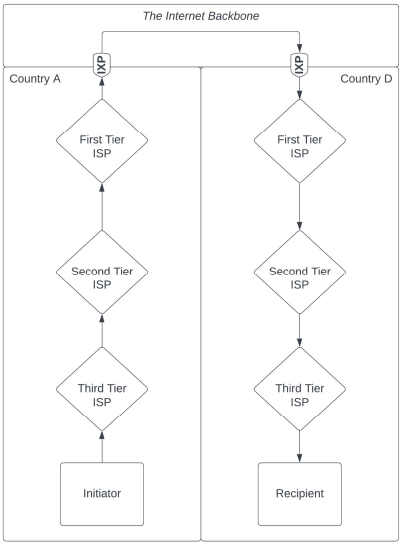

Figure 5: A Direct International Data Transfer

The illustration above showcases an international data transfer where data is directly collected from the Initiator in Country A. The Initiator does this by using the interface belonging to the Recipient in Country D through their terminal. As previously described, the personal information gets digitalised by the interface and released to the originating network. It first reaches the Tier 3 ISP and gets forwarded all the way up to the Tier 1 ISP of their

[41] Shavitt, Yuval, and Udi Weinsberg. "Topological trends of Internet content providers." Proceedings of the Fourth Annual Workshop on Simplifying Complex Networks for Practitioners. (2012): p 5 para 6.
[42] Valancius, Vytautas, et al. "How many tiers? pricing in the internet transit market." Proceedings of the ACM SIGCOMM 2011 Conference (2011); p 195 col 2.

network, where it is transmitted to Country D through the Internet Backbone by using the IXPs. The personal data finally reaches the Recipient when forwarded down through all tiers of ISPs in its own network.

If we closely examine this scenario from a technical perspective, it could be argued that this entire interaction has taken place in a single WAN. Consequently, when the data is sent from one point to another within this network, despite passing through various physical frameworks and different entities subject to different jurisdictions, it will still be considered that the data transfer has happened in a single network. This would mean that virtual constructs like networks do not differentiate between the borders of countries and do not reflect Westphalian System, given that the virtual world lacks physical borders comparable to those in the real world.[43] Just like with many other issues associated with the virtual domain, this situation leads to complications with privacy regulations because borders define the political and geographic scope of a state's authority by distinguishing its territory from others.[44] When these defining characteristics are absent, it will prompt the question of whether an international data transfer has really taken place because it could also be argued that the data did not leave the national borders, which means that there will be a dispute over which legislation becomes applicable and continues to be applicable until what point of time.

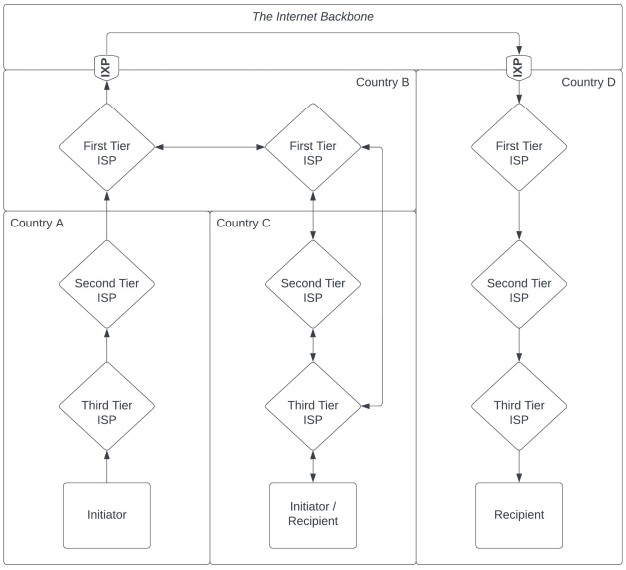

Figure 6: International Data Transfer through a Third-Party Service Provider

[43] Herrera, Geoffrey L. "Cyberspace and sovereignty: thoughts on physical space and digital space." Power and security in the information age. Routledge, (2016); p 69 para 3.
[44] Tsaugourias, Nicholas. "Law, borders and the territorialisation of cyberspace." Indonesian J. Int'l L. 15 (2017): p 523 para 2.

The way how this dispute becomes a growing issue could be seen better with the diagram provided in Figure 6. This scenario includes more countries that are providing the physical framework for the network where the transfer happens, and there is also a third-party service provider as an intermediary facilitating the communication between the main parties. Considering the involvement of the Service Provider, instead of following the same order shown in Figure 5, the transfer must be conducted like in Figure 3, and the package will be sent directly to Country C instead of Country D. However, as it can be observed, both the physical frameworks of Country A and Country C are managed by two separate Tier 1 ISPs that are located in Country B. Although both of these Tier 1 ISPs directly connect these two smaller networks together, they force the transfer of data to happen between 3 different countries before it reaches the actual destination because the frameworks are divided between countries. Regardless, once the package reaches the Service Provider, the package is sent back to Tier 1 of its network to be forwarded to the Recipient in Country D. To do that, the package is once again handed to Tier 1 of originating network because it has direct access to an IXP, which is the only way to reach to the Tier 1 of destination network in Country D. During this process, the personal data was passed through nine different third parties, yet only two of these parties were intended to receive it. However, it could still be argued that the transfer happened in a single network, and it was no different than a domestic data transfer.

Without considering whether there are more third-party service providers involved in the background, there are already significant legal concerns based on whether the data has crossed different physical borders because, from the legal perspective, it is still unclear which jurisdiction governs the data transfer and which jurisdictions are simultaneously eligible for applying their own privacy rules. As argued for Figure 5, while this transfer could be observed as virtually taking place in a single network that is subject to a particular jurisdiction, it was physically contained within three different frameworks, traversed across four other countries, and processed in two countries. In such a case, every country can argue that its jurisdiction is applicable to a single party or all of the parties and claim partial or total authority over the entire transferring process.

1.2 Definition of international data transfers

From a legal perspective, it is still unclear what exactly constitutes an international data transfer, as there is no universally agreed definition for it. Although the technical

characteristics of the transfers provide some limitations on how subjective views can be, lawmakers and scholars still hold different opinions on what an international data transfer really is. Regardless, over the years, although different legal instruments still shared relatively similar definitions, the majority of differences emerged from academia because the perspectives of scholars were significantly influenced by the technological advancements of their era.

1.2.1 Evolution of the definition in academia

In 1982, Gupta defined international data transfers as an action where a "unit of information transferred and processed in more than one nation-state"[45], but he did not provide a description to understand how this unit of information is being transferred. Regardless, the definition still provided the foundations with introducing the necessity to involve more than one country in the data transfer and also conducting processing activities in the same country where the data is transferred. This is important since he divided transfers and processing activities into separate activities, and as observed in Figure 6, a processing activity does not have to be conducted in the country the data is transferred. This means that Gupta's definition would not classify transmission made to Country C as an international data transfer, and only acknowledge the transmission made to Country D, staying short on covering interactions related to third-party service providers.

Fishman, on the other hand, defined international data transfers as "the electronic movement of data between countries"[46], providing the missing link in Gupta's definition by describing a transfer as an electronic movement. However, he did not fully explain what kind of electronic movement is required and what needs to happen as a result of this electronic movement. Considering Fishman coined this definition in the 1980s, we can presume that he meant the direct movement of the data, meaning creating a copy of the data in the terminal of the Recipient. However, with the technology that is available today, this notion would significantly limit the scope of the definition because we now have the possibility to share the data without actually moving it between terminals. One way to do that is through videoconferencing, where we can directly collect the information from a person as the

[45] Gupta, B. M., and S. P. Gupta. "Transborder data flow debate." (1982); p 51 col 1 para 2.
[46] Fishman, William L. "Introduction to transborder data flows." Stan. J. Int'l L. 16 (1980): p 1 para 1.

scientists did during the COVID-19 pandemic[47] or by sharing our screen with people in different countries, allowing them to view the data without actually moving the data from one terminal to another. While this shows the limits of Fishman's definitions, it also shows that technological advancements significantly impact the scope of international data transfers since videoconferencing was not possible until the mid-1990s[48], meaning Fishman's definition was able to describe what a data transfer is and what was not until their invention.

Another distinctive definition, which reflects the problem illustrated in the previous Section, was made in the late 1980s by Briner and later referred to by Jiang in 2022, where they defined international data transfers as "transmission of data across national borders"[49], and "the transfer of data between different jurisdictions"[50]. Just like Gupta, their definitions do not provide a description of what a transfer is and how it happens, but they model their definition around physical concepts, which, as explained, is difficult to reflect in the virtual domain because; jurisdictions are dependent on national borders, and national borders are dependent on the geographical characteristics of a country, which is not represented in the virtual domain.[51] The important takeaway from these two definitions is that we are still struggling to acknowledge that certain concepts do not exist in the virtual domain, thus unable to describe the interplay that is happening between them. However, this does not mean that all scholars are providing definitions with vague or difficult notions that would not be possible to apply in the virtual domain.

In 2023, Xiao isolated the definition of transfers with more regulatable constructs and provided that an international data transfer is "the flow of data between servers in two countries or regions "[52] which highlighted the electronic movement mentioned by Fishman as an interaction between different servers and required them to be physically located in other countries, turning the ideas of Briner and Jiang into something applicable in both domains. However, by structure, this definition is also limited because it only acknowledges

[47] Boland, Joshua, et al. "A COVID-19-era rapid review: using Zoom and Skype for qualitative group research." Public Health Research & Practice 32.2 (2022); p 2 col 1 para 2
[48] Galbreath, Jeremy. "Compressed digital videoconferencing: An overview." Educational Technology 35.1 (1995): p 31 col 1 para 2.
[49] Briner, Russell F., and Sid R. Ewer. "Financial information flow and transborder restrictions." Journal of Systems Management 38.8 (1987): p 32 para 3.
[50] Jiang, Chengze. "Research on Applying the WTO Security Exception Clause to the Security Dispute Caused by Cross-border Data Flows." 2021 International Conference on Social Development and Media Communication (SDMC 2021). Atlantis Press, (2022); p 1370 col 1 para 4.
[51] See Tsaugourias supra note 44.
[52] Xiao, Yineng, and Yi Li. "On the importance of coordinated international rules in cross-border circulation of data." International Journal of Frontiers in Sociology 5.2 (2023); p 85 para 3.

interactions made between servers as international transfers. This means that if the interaction in Figure 5 was happening between two natural persons and their terminals were normal computers or smartphones, the transmission made between them would not be considered as an international data transfer. Furthermore, building up on the example of videoconferencing provided for Fishman's definition, even if we can classify the Initiator as the server because they are streaming media from their terminal, it would technically classify the Recipients as the clients that are requesting the information from the Initiator[53] and still would not acknowledge such interaction as an international data transfer.

These definitions provided by the scholars show that the ideal definition of an international data transfer does not depend on the concepts that exist in the physical domain, does not limit the interactions between certain device types or specific kinds of parties, and thoroughly provides what kind of action or actions can be included when explaining what an international data transfer could be. Furthermore, this ideal definition must also be articulated in a way that it would not be outdated by technological advancements. This is naturally difficult and turns the formulation phase into a guessing game. However, following the arguments on Fishman's definition, it is almost guaranteed that any definition that is hardly embedded in the current technological capabilities to be outdated in 10 to 20 years.

1.2.2 Definition in the EU Law

The EU law consists of different sources that can be used to define what an international data transfer is and how the responsibilities are divided among the parties that are involved with it. As it could be expected, the GDPR is the legal instrument that provides these definitions, since it is currently the main regulation governing data protection and privacy-related affairs in the EU.[54] According to the Article 4 of GDPR, any affair concerning the international transfer of personal data happens between three different parties: the Data Subjects (hereinafter "Subject")[55], the Data Processors (hereinafter "Processor")[56], and the Data Controllers (hereinafter "Controller")[57].

[53] Vaida, Mircea-F., Ovidiu Buza, and Kalman Pusztai. "Streaming Audio-Video Content Over Internet with a Multimedia Presentation Generator." Web-Based Education: Proceedings of the Fourth IASTED International Conference, WBE-2005, (2005); p 1 col 2 para 1 & 2.
[54] GDPR (n 14), Article 1
[55] GDPR (n 14), Article 4 (1).
[56] ibid, Article 4 (8).
[57] ibid, Article 28 (1).

The Subjects are practically the donors of personal information that is required for generating the personal data that is transferred between entities. This means their personal information, like name, age, gender, race, identity number, address, phone number, financial status, or any other identifiable information, becomes personal data when digitalised.[58] As the name suggests, the data is processed by the Processors on behalf of the Controllers, who are the responsible parties and also accountable for any actions concerning the personal data when something happens to it.[59] However, the responsibilities can be shared with the Processors when an international data transfer is taking place[60], more on that will be explained later.

It is worth mentioning that while the Processor and the Controller can be separate entities, there are no limitations that prevent a single entity from attaining the roles of both the Processor and the Controller. However, often these entities are separate, and while there can be multiple Processors involved in a processing activity, there is always one Controller unless another Controller becomes a joint controller.[61] A similar relationship is also possible for the Processors when the Processor that is tasked with a processing activity requires the assistance of another Processor for the completion of the task, which makes the new Processor a sub-processor. [62]

While the definitions on the parties, provides us that a potential data transfer scenario always takes place between a Subject and a Processor, a Subject and a Controller, a Controller and a Processor, or a Processor and another Processor, the GDPR explains in Article 44 that for the transmission happening between them to be classified as an international data transfer, it must be "a transfer of personal data which are undergoing processing or are intended for processing after transfer to a non-EU Country or to an international organisation"[63]. Although this definition establishes a margin for intent and requirement for the involvement of a non-EU country or an international organisation in the process, it still does not provide information on how the distinction is made between the EU territory and non-EU territory in the virtual domain. However, some of the notions included in this definition have been sought and explained further with the decisions of the Court of Justice of the European Union

[58] GDPR (n 14), Article 4 (1).
[59] ibid, Article 4 (7).
[60] Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18 (CJEU, 16 July 2020); Section 131 [hereinafter Schrems II].
[61] GDPR (n 14), Article 26 (1).
[62] ibid, Article 28 (3).
[63] GDPR (n 14), Article 44.

(hereinafter "CJEU"), which has provided an understanding of what an international data transfer looks like from the EU's legal perspective.

Most notably, in the *Lindqvist* case, the Court examined whether an international data transfer takes place when individuals from non-EU countries access and view information from a website hosted in the EU.[64] Given the essence of the interaction, the CJEU has adopted a stance that aligns closely with the argument presented for Fishman's definition and mandated that the technical nature of operations should be considered when determining whether a transfer has taken place.[65] What was important with this statement is that, in the continuity of the case, CJEU acknowledged that the data could be viewed without actually transferring it outside of the server that is hosting the website, and while that data could be just accessed remotely in this way, a direct interaction between two parties would still be required to label it as a transfer.[66] Consequently, since the website in question was available to everyone and did not specifically target a particular group or groups of persons, it meant a data transfer did not take place.[67]

This position was later supported by the findings of the *Schrems I* case when CJEU reviewed the technical nature of operations happening between Facebook and its EU subsidiary, where these entities were transferring data between each other. The Court determined that, despite these transfers occurring between the same group entity, they were conducted across borders with the intention of further processing the personal data in the US.[68] The perspective CJEU adopted during this case was in line with Briner and Jiang's view of international data transfers because the Court established that while the transfers happening between these entities could be argued as internal transfers, they were qualified to be categorised as international data transfers since they were moving between different jurisdictions.[69]

While the findings of both Lindqvist and Schrems I have provided further insight on how to determine when an international data transfer occurs, they have also shown that the definition provided in Article 44 does not include what was found in them. Since there is no detailed description of the international data transfers in Article 44, we are only able to explore these specifics when a case is brought in front of the authorities. This means that in addition to

[64] Lindqvist v. Åklagarkammaren i Jönköping Case C-101/01 (CJEU, 6 November 2003); para 15 & 16.
[65] ibid, at para 57
[66] ibid, at para 61
[67] ibid, at para 59 & 71
[68] Schrems I (n 12); para 27
[69] ibid, at para 45

defining how EU and non-EU territory is divided in the virtual domain, there are plenty of different circumstances that require explanation as they impact the qualification of a data transfer to be either considered or not considered as an international data transfer. However, considering there are plenty of different methods and variables involved in the transfer of personal data, and these methods and variables are increasing with technological advancements, it would be extremely difficult to adequately capture all the technicalities of these circumstances in one try. Therefore, this thesis is in the position that there must be a system that allows for binding regular updates to keep up with the technological advancements to enable the inclusion of new methods.

Even though the proposed solution may seem like a burdensome and unrealistic idea, the GDPR has already established procedures that can achieve this with the European Data Protection Board (hereinafter "EDPB"), which is the governing body that is authorised by the EU and empowered by the GDPR to provide support in matters related to data protection affairs.[70] The EU lawmakers have noticed this aspect of affairs in the virtual domain while drafting the GDPR and imposed responsibility on the EDPB for developing guidelines, particularly on international data transfers whenever necessary.[71] EDPB has already taken advantage of this procedure and published guidelines that have set strong foundations for sketching out how jurisdiction is perceived in the virtual domain and how an international data transfer is realised between entities.

1.2.3 Position of EDPB Guidelines

The EDPB Guidelines built up on the CJEU's decision in the Lindqvist case by pulling attention to the necessity of a relationship between an importer and exporter and requiring at least one of the parties to be located outside of the EU[72], underlining that the existence of this relationship is essential to distinguish a domestic data transfer from an international data transfer.[73] EDPB's attention has also been attracted by various scenarios concerning international data transfer where this relationship would not be enough to reach a classification, particularly those that involves multiple entites that are located in different

[70] GDPR (n 14), Article 68
[71] GDPR (n 14), Article 70 (i), (j)
[72] European Data Protection Board. "Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR" 05/2021 (14 February 2023); at Section 22 [hereinafter Guideline 05/2021].
[73] Guideline 05/2021 (n 72), at Section 19

jurisdictions, and established specific distinctions with "territorial" and "accessibility" criteria to assess whether the jurisdiction of the EU extends to a foreign entity that is interacting with the EU in the virtual domain, by requiring several conditions embedded in these criteria to ensure a proper process has been conducted for its classification.[74]

As the name suggests, “territorial criteria” focuses on the location of parties that are involved with the data processing activities. It requires at least one of the parties initiating the transfer to be within the physical territory in which the scope of GDPR is applicable,[75] meaning either the importer or exporter must be in one of the Member States and the other in a non-EU Country.[76] However, to properly identify the importer and exporter relationship between the interacting parties, this criterion itself has additional requirements which can only be determined by “establishment” and “targeting” sub-criteria.[77] Both of these sub-criteria concern different kinds of parties that are defined in Article 4 of GDPR.

The “establishment sub-criteria” is only applicable to the Data Controllers and the Data Processors[78], and based on the nature of the relationship, also the significance of the activities related to this relationship and how it corresponds to overall processing activities taking place within the EU.[79] This means that the threshold provided in this criteria possesses a range that includes the smallest activity in the EU, and does not make any distinction on the role of the parties involved in the processing activities.

Data Subjects are covered in “targeting sub-criteria”, as it focuses on the relevance of any direct or indirect activity with them, aiming to uncover whether they are particularly aimed at the EU Data Subjects.[80] In other words, in a scenario where an entity is collecting personal data of Data Subjects located in the EU, even if this entity is not located within the EU, it will fall under the scope of this sub-criteria. However, an important exemption is that the extent of the EU’s jurisdiction in this matter will be limited and regulations become inapplicable if the Subject is not particularly targeted as an EU subject (citizen or a resident).[81] This means that, in scenarios where an EU subject benefits from the services of a foreign entity, the scope will

[74] Guideline 05/2021 (n 72), at Section 9
[75] Guideline 05/2021 (n 72), at Section 12 & 13
[76] Guideline 05/2021 (n 72), at Section 22
[77] GDPR (n 14), Article 3
[78] European Data Protection Board. "Guidelines on the territorial scope of the GDPR (Article 3) - version for public consultation." 03/2018 (12 November 2019); p 5 para 6 [hereinafter Guideline 03/2018].
[79] Guideline 03/2018 (n 78), p 6 para 3-4
[80] Guideline 03/2018 (n 78), p 14 para 3
[81] Guideline 03/2018 (n 78), p 15 para 3

not cover them, as long as they are not intended for EU Data Subjects or if the service becomes unavailable while they are in the EU.

On the other hand, the "accessibility criteria" provided by the EDPB are less complicated. It does not have any sub-criteria and it simply pulls attention to the interactions concerning the disclosure of personal data between the Controllers and Processors.[82] However, since this criterion applies solely to the Controllers and Processors, it exempts scenarios in which personal data is directly provided by the Subjects to these entities, resulting in preventing such direct data collection practices from being classified as granting access.[83] An important aspect of this condition is that the definition of "disclosure" includes any means that make personal data available to another entity, which covers disclosure by remote access.[84] This is important because, as observed with the arguments provided in the previous Sub-section, the scope of the definitions provided by Scholars has been undermined by technological advancements over time. Therefore, the definition of disclosures under this criteria provides enough room for considerations against new transfer methods that would become available with new technology.

Regardless, it should be noted that this criterion also complements the establishment sub-criteria because focusing on any interaction between the Controllers and Processors consequently extends the scope to the Joint Controllers and Sub-Processors. For example, if a Processor stores collected personal data in a server located in the EU and makes the personal data in the server available to a Sub-processor located in a non-EU country, it would extend the scope of the EU's authority and impose liability to this Sub-processor under accessibility criteria, even if the Sub-processor conducts its activities on the server of the Processor and would not move them directly to their possession.[85]

The content of the guidelines shows that the EDPB has established concrete foundations that could be applicable to every possible scenario concerning data transfers with our current technological abilities while also leaving a margin for future technological developments. Furthermore, the conditions determined for the extension of the jurisdictional scope are also not affected by the unique nature of the virtual domain concerning the borders, as the notions in the guidelines are isolated on the status of interacting parties. To summarize this Sub-

[82] Guideline 05/2021 (n 72), at Section 15
[83] Guideline 05/2021 (n 72), at Section 20
[84] Guideline 05/2021 (n 72), at Section 16
[85] European Data Protection Board. "Guidelines on the concepts of controller and processor in the GDPR - version for public consultation." 07/2020 (7 July 2021); at Section 159 & 160.

section and demonstrate the effectiveness of the EDPB's approach, we can test the provisions provided by the guidelines by viewing the three different scenarios that can be displayed in Figure 6 and also inspect how the results correspond to the questions raised in Sub-sections 1.1.2 and 1.2.1.

In a scenario where only Country A was under GDPR's jurisdiction, and the Data Subject was located here, we could easily determine that the entire process was subject to the jurisdictional authority of the EU following the targeting sub-criteria. Because no matter where the Data Processor and Service Provider were located, their operations would be considered to be particularly targeting an EU subject thus, the conditions of the GDPR would become applicable to them.

If Country C were under GDPR's jurisdiction, the Data Subject and the Service Provider located in A and D and the Data Processor located in Country C; we could determine that the EU jurisdiction becomes applicable to both the Service Provider and the Data Processor, following the establishment sub-criteria since when the data transfer is initiated by the non-EU-Data Subject in Country A, it would only become subject to GDPR's provisions once it reaches the Tier 2 ISP of Country C. The provisions would continue to be applicable even when it was transferred to Country D in accordance with the accessibility criteria because no matter whether the Service Provider is located in a non-EU country, there is an importer and exporter relationship between the Data Processor and the Service Provider and the Service Provider has direct access to the personal data.

Finally, if Country D were under GDPR's jurisdiction, the Data Subject and Service Providers are in Country A and C, while the Data Processor is in Country D; we could see that the jurisdiction of the EU would only become applicable from the moment it reaches to the Tier 1 ISP of Country D, as, no matter the main processing activities are taking place in Country D and Service Provider is assisting the collection of personal data from a Data Subject, only establishment sub-criteria would be fulfilled since the Data Subject is a non-EU subject, thus would not have necessary grounds for extending the EU's jurisdiction over the Service Provider.

The analysis of all three scenarios shows how vital each criterion provided by the EDPB is and proves that a simple definition would not be able to describe these conditions and provide the necessary information for navigating through the complexities of networks and physical borders that data must traverse. However, no matter whether the thesis is on the position that

does not favour simple definitions to describe what an international data transfer is, the remaining Chapters rely on a concrete definition of international data transfer to properly address the issues surrounding international data transfers. While still acknowledging that a brief definition falls short and a system requiring constant updates is necessary to keep pace with technological advancements and properly describe international data transfers, this thesis defines these transfers as “the interactions in the virtual domain based on the processing of personal data or concerning processing of personal data, involving network or networks supported by geographically distributed infrastructure, containing a controller or processor relationship, where the personal data is either electronically moved between different terminals or mirrored for viewing” which gives enough room to make necessary distinctions in detail and understand the aspects of the transfer, especially the determination of when and how international data transfers are realised.

CHAPTER II: ISSUES CONCERNING INTERNATIONAL DATA TRANSFERS

2.1 Inherent issues of GDPR

The relationship between the ISPs, networks, geographical locations, and the correct definition of international data transfers sets the groundwork for properly understanding how international data transfers happen from a technical perspective and assists us with adapting the legal requirements for their effective regulation. As the previous Chapter demonstrated, these matters have issues of their own, and they are addressed subjectively. However, while we can categorise them as general issues that surround international data transfers, there are also those that are specific for legal instruments on privacy, such as; accountability for actions, cooperation between governments, and enforcement of rules, which, as will be explained in this Chapter, play a vital role in effective regulation of privacy related affairs concerning international data transfers.[86]

Naturally, this means that when transferring data, the focus shifts to the parties initiating the transfer from the ISPs or network locations, which has been highlighted by the EDPB guidelines. The reason is that operating in a virtual domain increases the likelihood of bypassing national data protection and privacy laws, and regulatory authorities are left with the responsibility for actively providing protections against data processing risks in other countries by asserting provisions of data protection and privacy laws and individual rights abroad, increasing the confidence of consumers and individuals.[87]

For this reason, the legal transfer of personal data outside the EU's jurisdictional borders is a strictly regulated process by default because the GDPR prohibits the export of personal data as a precaution against such practices and only allows the transfer of personal data when accountability and enforcement can be guaranteed until a certain margin.[88] However, specific to the EU, some of the issues concerning accountability and enforcement do not come from the effectivity of tools of transfer that are created by the GDPR for the safe transfer of personal data to non-EU countries.[89] Some of these issues come directly from the core principles of the GDPR, which are created for the coherent protection of personal data.[90] This

[86] Jehovantodistajat v. Finland, Case C-25/17, (CJEU, 10 July 2018); at para 65 & 66
[87] Kuner, Christopher. "Regulation of Transborder Data Flows Under Data Protection and Privacy Law." (2011); p 23-24.
[88] Dhont, Jan Xavier. "Schrems II. The EU adequacy regime in existential crisis?" Maastricht Journal of European and Comparative Law 26.5, (2019): p 598 para 4.
[89] GDPR (n 14), Article 44
[90] GDPR (n 14), Article 4

means that the solutions developed by the EU lawmakers also become the cause of issues that mainly surround international data transfers.

2.1.1 Means to Transfer Personal Data

Chapter V of the GDPR outlines the key rules that govern the transfer of personal data between the EU and non-EU countries, as well as international organisations.[91] It also introduces several tools that can be employed to legitimise each transfer. While some of these tools are created for securing accountability and enforcement, considering the frequency of issues on cooperation that could be faced in non-EU countries, enforcement of GDPR on foreign soil may be ineffective, and these tools may not always provide adequate protection as expected.[92] One of the reasons why cooperation issues arise is because of how the EU data protection laws assert their own authority over foreign ones.[93] This is naturally not always welcomed by governments of other countries. This makes international data transfers from the EU more challenging than they should be; however, considering some countries favouring good relations with the EU, they face a dilemma and are forced to acknowledge the supremacy of EU data protection laws in their own territory, which leads them to make adjustments in their regulatory system to allow smoother transfers.[94]

In such cases, the data can be easily transferred through Adequacy Decisions, which certifies that the non-EU country is providing sufficient protection.[95] While the Adequacy Decision shows that there will not be any disputes over the application of GDPR provisions, it also implies that issues with accountability and enforcement are unlikely to occur as both countries are actively cooperating. On the other hand, if this is not the case, the entities that wish to transfer the data must utilise other tools that are suitable for their circumstances,[96] which does not guarantee enforcement on foreign soil as an Adequacy Decision does, but at least establishes grounds for accountability. However, regardless of which way the entities choose, when there are no Adequacy Decisions in the target country, they face a predicament

[91] GDPR (n 14), Article 50 (1)
[92] Greze, Benjamin. "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives." International Data Privacy Law 9.2 (2019): p 110 col 2 para 3
[93] Streinz, Thomas. "The evolution of European data law." The Evolution of EU Law (OUP, 3rd edn 2021) (2021): p 21 para 2
[94] Mattoo, Aaditya, and Joshua P. Meltzer. "International data flows and privacy: The conflict and its resolution." Journal of International Economic Law 21.4 (2018): p 769-789.
[95] GDPR (n 14), Article 45 (1)
[96] GDPR (n 14), Article 46

of being accountable due to these disagreements, as adherence to the legal requirements is not just an obligation but also a way to prevent economic and reputational damage.[97]

2.1.1.1 Adequacy Decisions

As previously referred, the simplest method for transferring data is through an Adequacy Decision, which is available in the GDPR and its public sector counterpart, the Law Enforcement Data Protection Directive (hereinafter "LEDPD").[98] This is because Adequacy Decisions certify that the corresponding country provides protections for personal data equal to or comparable to the provisions outlaid in the laws of the EU, and transfers can be made without needing any further authorisation.[99] This does not mean, however, that the Adequacy Decision limits the application of GDPR's provisions from being applied on foreign territory.[100] In most cases, these provisions become equally embedded in the legislation of the foreign country, but the cooperation that is established between the countries allows the application of extra measures during most cases, guaranteeing enforcement.

The aspect of cooperation becomes even more visible during the process of obtaining an Adequacy Decision for either regulation, as it is a lengthy and complex process. It involves the relevant governmental bodies of the foreign country coming together with the European Commission (hereinafter "the Commission") to review certain practices, such as if the foreign country respects the rule of law[101], has a supervisory authority with an effective presence[102], also if the country in question respects their commitments in the international theatre.[103] Considering this lengthy process, transferring data according to Adequacy Decisions is naturally limited since the EU was only able to grant Adequacy Decisions to 15 countries, and even though the US is one of them, it only applies to transfers made in

[97] Chang, Younghoon, et al. "The role of privacy policy on consumers' perceived privacy." Government Information Quarterly 35.3 (2018): p 450 col 2 para 1
[98] Drechsler, Laura. "Comparing LED and GDPR adequacy: One standard two systems." Global Privacy Law Review 1.2 (2020); p 94 col 2 para 2.
[99] Law Enforcement Data Protection Directive, Directive (EU) 2016/680, OJ L 119/89 (27 April 2016); Article 36 [hereinafter LEPD] & GDPR (n 14), Article 45.
[100] European Commission, "Commission Implementing Regulation (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" (28 June 2021); Recital 7 < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D1772> [accessed 20 March 2024].
[101] LEDPD (n 99), Article 36 (2) (a) & GDPR (n 14), Article 45 (2) (a)
[102] LEDPD (n 99), Article 36 (2) (b) & GDPR (n 14), Article 45 (2) (b)
[103] LEDPD (n 99), Article 36 (2) (c) & GDPR (n 14), Article 45 (2) (c)

accordance with DPF[104], which, as it will be explained in the next Chapter, means it has limited adequacy.

One thing worth mentioning is that, from a general perspective, decisions involving the free flow of international data transfers are heavily affected by economic aspirations[105], and this could also be the case for the EU. Kuner views Adequacy Decisions as inefficient because they are untransparent and heavily subject to political influence.[106] Considering limitations to international data transfers are also a limit to global business and trade[107], we may never know whether the Adequacy Decision has been really given because the protections of GDPR are provided in that country or if the EU is substantially dependent on its economic relations with that country. Regardless, one takeaway from the ratio of requirements and the limited number of countries that have received an Adequacy Decision to date is that, even if the EU is granting an Adequacy Decision due to economic and political reasons, it is still considering the rights of the EU subjects and heavily projecting its own values onto foreign countries that wish to obtain an Adequacy Decision. Otherwise the number of Adequacy Decisions would be significantly higher.

However, as much as we can see such a projection from the EU as beneficial commitment, it must also be considered that demanding such standards has the potential to cause issues because of the differences in the customs and values that have played a role in the creation of each country's laws, which has the potential to lead the EU to approach its counterpart with an unrealistic expectation. One of the primary reasons the EU would have an unrealistic expectation is because the core values that played a role in the creation of the EU, particularly the provisions outlaid in its foundational treaties, forcing the EU to ensure that any country or organisation that the it interacts with is adhering to its treaty principles involving the human rights and foundational values of the EU.[108]

This concerning, particularly for privacy related affairs, especially when we consider that not all countries have developed their data protection and privacy-related laws like the EU. For example, if we compare the EU and the US in this matter, we can easily see that the concept of privacy has developed fairly different: In the EU, it is mainly the result of the European

[104] European Commission. "Adequacy Decisions." < https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en > [accessed 20 March 2024].
[105] Schwartz, Paul M. "Global data privacy: The EU way." NYUL Rev. 94 (2019): p 791 para 4.
[106] Kuner, Christopher. "Reality and illusion in EU data transfer regulation post Schrems." German Law Journal 18.4 (2017): p 911 para 1.
[107] See Eger supra note 2.
[108] Consolidated Version of the Treaty on European Union [2008] OJ C115/13; Article 3 (5).

Convention on Human Rights, which perceives the right to privacy as a fundamental human right.[109] On the other hand, in the US, the same concept is based on norms created with case laws, which acknowledge the right to privacy not particularly as a fundamental human right but as an extension of constitutional rights.[110]

This distinction is crucial, as the EU regards human rights as sacred and does not permit their derogation unless extreme circumstances arise and require them to be violated. [111] In contrast, the US has a notorious history of allowing the violation of constitutional individual rights and liberties, largely because the US Courts tend to defer to government agencies and fail to address these violations in an effective way. [112] Which means that there is a significant risk that countries seeking an Adequacy Decision may have similar conditions that the EU would not approve of.

Thankfully, the lack of Adequacy Decision is not a hard block for data transfers from the EU, but their absence makes the transfers more complicated than they should be since accountability and enforcement are not as strong with them as it is with the Adequacy Decisions. Regardless, when there are no Adequacy Decisions in place with a country where an EU entity wishes to transfer data, GDPR allows transfers with methods which are collectively called “appropriate safeguards” or “transfer tools”, where Binding Corporate Rules (hereinafter “BCRs”) and Standard Contractual Clauses (hereinafter “SCCs”) are the most popular among them.[113] Also, as previously mentioned, there are specialised tools designed especially for transferring data between the EU and the US, and as of 2023, this is DPF, which is a self-certification method, certifying that participating entities are individually committed to GDPR's provisions.[114]

2.1.1.2 Binding Corporate Rules

Essentially, BCRs and SCCs share some similarities; however, there are some differences that set them apart from each other from an operational perspective. BCRs are basically

[109] See ECHR supra note 19.
[110] Whalen v. Roe, 429 U.S. 589 (SCOTUS, 22 February 1977).
[111] ECHR (n 19), Article 15.
[112] Berger, Eric. "Individual Rights, Judicial Deference, and Administrative Law Norms in Constitutional Decision Making." BUL Rev. 91 (2011): p 2038-2047.
[113] GDPR (n 14), Article 46
[114] Terpan, Fabien. "EU-US data transfer from safe harbour to privacy shield: back to square one?." European Papers-A Journal on Law and Integration 2018.3 (2019): p 1051.

contractual obligations based on corporation groups, which are used by multinational companies to conduct internal transfers across EU borders on a regular basis.[115] This means that from a general perspective, the accountability of actions is limited to the members of this corporate group and does not include all the entities that are located in the target country.

They are usually utilised for transfers that could be categorised as remote access, as demonstrated in Chapter 1 of this thesis; however, they can also be used for regular processing activities in foreign jurisdictions. The entities interested in using the BCRs are required to describe in the BCR which non-Adequacy Country these transferring activities will take place and also what kind of personal data will be involved with the processing activities when they arrive at their destination.[116] This means that no matter where the entity is located, it can lawfully initiate a data transfer with its corporation group for any processing activity based on BCR, freely, without distinguishing which country they are in.

Furthermore, BCRs establish tailored and interchangeably usable protocols for the corporate group they are created for, which guarantees that entities acting as the Controllers or the Processors handle personal data in accordance with the rules reflecting the GDPR, specifically the Six Principles, which becomes applicable to all personal data generated in the EU, from the moment of its creation.[117] As it will be explained in the next Sub-section, these principles play a significant role in the correct handling of personal data throughout its life cycle and require strong enforcement for their compliance. While finding the required enforcement might be challenging under certain circumstances, integrating it with the BCRs and SCCs ensures that the data is properly managed, at least theoretically.

One of the drawbacks concerning the BCRs is that, since they are based on particular organisations, there are no standard procedures that can be immediately adopted to allow them to start executing their transferring activities right away. The cost of time becomes even more significant if we also consider that the corporate groups require approval from their national EU DPA for the BCRs to be considered valid.[118] Despite this procedure consuming a lot of time, it also reveals that the enforcement of the BCRs is one-sided, meaning that it relies on the commitment of the entities to the rules that they have presented before the DPA.

---

[115] Tehrani, Pardis Moslemzadeh, Johan Shamsuddin Bin Hj Sabaruddin, and Dhiviya AP Ramanathan. "Cross border data transfer: Complexity of adequate protection and its exceptions." Computer law & security review 34.3 (2018): p 592 col 2 para 1.
[116] GDPR (n 14), Article 47 (2) (b)
[117] GDPR (n 14), Article 4 (20)
[118] GDPR (n 14), Article 47 (1) (a)

While this may offer a configuration that lacks supervision, the effectivity of enforcement is strengthened by requiring the delegation of a responsible party; an entity from the corporate group and the DPA of the accountable entity's choice, forcing constant coordination as a requirement for the regulatory side of the transfers.[119] However, no matter whether this guarantees both accountability and enforcement from the EU side, they remain absent in the countries that are designated to be involved with the data transfers.

Considering non-EU DPAs or other foreign regulatory authorities do not get involved in the enforcement of BCRs, this task is exclusively up to the corporate group, which is required to establish necessary contractual means to make BCRs binding for their activities and to internally enforce them for this limited self-regulation to be effective.[120] While violations could still have consequences for the EU entity, and act as a valuable deterrence and a means to remedy victims of such malpractice[121], there are no guarantees for punishment in the foreign jurisdiction for the provisions of GDPR. However, there is the possibility that the authorities in a foreign jurisdiction may penalise one of these corporate entities if they refuse to perform a particular act or do not comply with other requirements that are acceptable under national legislation but not in accordance with provisions of the GDPR. This shows that entities that are operating under BCRs are risking penalisation to be compliant with GDPR and must deal with complexities occurring due to regulatory disputes since there is no cooperation between the EU with these countries while they remain liable to them both.

2.1.1.3 Standard Contractual Clauses

When compared to the BCRs, the SCCs possess completely different complications, risks, and problems that do not exist with BCRs since they are not controlled as strictly as them. For example, unlike BCRs, SCCs are utilised for the transfer of personal data between different corporate groups or organisations, which means that the transfers utilising SCCs usually involve a counterpart that does not have an establishment within the jurisdiction of the EU.

---

[119] Tehrani (n 115); p 592 col 2 para 3

[120] European Data Protection Board, "Recommendations on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)" 1/2022 (20 June 2023); Section 9.

[121] Naef, Tobias. "The Restrictive Effect of the Legal Mechanisms for Data Transfers in the European Union." Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law. Cham: Springer International Publishing (2022): p 190 para 2

Similar to the BCRs, SCCs also recognise that there are different roles that are attained during the data transfers, however, these SCC protocols cannot be used interchangeably like BCRs. Thus, while the SCCs are created for specific countries involved with the transfers, there are particular SCC types that are made by EU authorities to be used for processor-to-processor, controller-to-processor or controller-to-controller interactions.[122] This adds to the bureaucratic burden from different fronts, as the EU entity must install each one of them every time, depending on its relationship with the foreign entity that it wishes to make the transfers. But despite that the structure is complicated, they can be employed faster than BCRs as they do not require authorisation for their validity.

Related to this, it is worth mentioning that the extent of protections provided by SCCs cannot be more than what is allowed by foreign law, regardless of how detailed the provisions related to these protections may be.[123] This is critical because it highlights issues with accountability and enforcement since there is a high chance that a foreign entity might not have a subsidiary in the EU, and there could be no leverage to compel the foreign entity to take necessary actions in compliance with the provisions of GDPR. Furthermore, these characteristics of the SCCs show that they display a weak form of extraterritoriality during their conception because they are essentially agreements between EU institutions and entities operating in a foreign jurisdiction. Similar to BCRs, this is where issues related to cooperation begin, as it gives the impression that this relationship is displacing the authority of local government. However, in reality, SCCs only add an extra layer of protection by contractually requiring foreign entity submitting to the jurisdiction of EU authorities as they do not have a direct leverage to assure the foreign entities will abide the rules. [124]

Aside from their general popularity, specifically for transfers to the US, the use of SCCs has been the go-to method for EU entities when dealing with their US counterparts. Especially during the transition periods when the predecessors of DPFs were invalidated, SCC 2021/914 was the method that was used the most.[125] This rise in the use of SCCs has brought the spotlight on them, and naturally, questions have been raised about their effectiveness. Especially during the *Schrems II* case, the efficacy and the extent of adequate protection

[122] Paull, Burness. "International Data Transfers: European Commission publishes final version of New Standard Contractual Clauses." (2021): p 4.
[123] Schrems II (n 60), Section 90.
[124] Bradford, Laura, Mateo Aboy, and Kathleen Liddell. "Standard contractual clauses for cross-border transfers of health data after Schrems II." Journal of Law and the Biosciences 8.1 (2021): p 20 para 4.
[125] Tracol, Xavier. "“Schrems II”: The return of the privacy shield." Computer Law & Security Review 39 (2020): p 7 col 1 para 1.

provided by the SCCs have been a major concern and have led CJEU to investigate their functional components in detail.[126]

During the case, CJEU recognised that in order to certify that an SCC provides sufficient protection, it is necessary to have grounds that ensure equivalent protection to that is offered by the EU, and it was stated that the protections provided by SCCs should ideally be able to achieve the level of protection promised by the GDPR.[127] This consequently meant that the steps that are taken during the evaluation of Adequacy Decisions have to be also taken into consideration when SCCs are in use, so that they can guarantee the EU standards.[128] This brings quite a challenge as while there is strong cooperation between the EU and the country with Adequacy Decision; such cooperation is not always guaranteed with SCCs, which means that the legal landscape where protections provided by SCCs will be always inferior to those that are provided in Adequacy Decision countries.

Furthermore, from a legal perspective, the most significant concern during this evaluation process is examining the adherence to the rule of law in the non-EU country, as it is essential to ensure that the country receiving the data is trustworthy and the legal landscape is capable of upholding legal obligations because the EU lacks substantial power to enforce its rules over foreign entities when there is no cooperation. If the non-EU country respects the rule of law, only then can the SCCs provide the level of protection they were designed for and ease concerns over accountability and enforceability because EU DPAs and other EU entities otherwise have absolutely no power against the violations that may occur on foreign soil.[129]

This, in general, shows that when a tool for transfer is being used, the EU would have to rely heavily on the rule of law and the willingness of foreign authorities to cooperate with them to ensure that the provisions of GDPR are applied and the rights of Data Subjects are respected, which shows that their protections are explicitly restricted. This also means that BCRs and SCCs used in countries that could not secure an Adequacy Decision due to significant concerns must be closely monitored because, at any given moment, issues could emerge concerning the effectiveness of the protections they offer.

It is worth mentioning that these concerns are not hypothetical, as they have also been recognised by the CJEU in the Schrems II decision, where the Court oversaw that temporarily

[126] Schrems II (n 60), Section 90
[127] Schrems II (n 60), Section 105
[128] ibid, at Section 102 & 103
[129] GDPR (n 14), Recital 116

or permanently halting the transfers by a DPA as a protective restriction has been considered to be plausible and an expected action, particularly in the case when international data transfers are relying on SCCs and are happening between the countries where such concerns are prevalent.[130] Furthermore, there has been an additional impact following this statement of CJEU, as it raised questions over the effectiveness of SCCs and the current state of the legal landscape concerning international data transfers from the EU. Because after this statement, CJEU did not decide to invalidate them despite raised concerns over their effectiveness[131], but the Commission later adopted a special set of SCCs that were announced to be improved versions of the existing SCCs and entirely replaced what was used before them.[132] Considering the shift between the views of two different EU institutions, it would not be bold to say that this indicates there are some uncertainties involving effectivity of SCCs.

2.1.2 Issues Sourced by the Six Principles

While the tools of transfer ensure that personal data is transmitted to an environment where it will be safe, as previously mentioned, the Six Principles of GDPR focus on the preservation of protections granted to personal data during its creation. This also applies to the circumstances when data is transferred to another jurisdiction and goes beyond the EU territory because, as EDPB states, the principles are designed "to ensure that the level of protection guaranteed by the GDPR is not undermined when personal data is transferred 'to non-EU countries or international organisations'"[133].

This intercalated structure shows that the GDPR provides a full cycle of protection to the personal data that originates from its jurisdictional territory. Although this fits the long-standing saying of Reidenberg that "simple rules might result in weaker data protection, while sophisticated rules offer stronger protection"[134] there must be a limit to how much

[130] Schrems II (n 60), at Section 121
[131] ibid, at Section 149
[132] European Commission, "Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council" (4 June 2021); Clause 4 (1) < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN > [accessed 22 March 2024 – hereinafter "Commission on SCCs"].
[133] Guideline 05/2021 (n 72); Section 1
[134] Reidenberg, Joel R. "The simplification of international data privacy rules." Fordham Int'l LJ 29 (2005): p 1136 para 2.

protection should be applied to personal data, as exceeding this limit may start to obstruct or hinder the whole process rather than aiding the achievement of the intended goal.

Since the principles become applicable as soon as personal information is collected from a Data Subject, they remain applicable until the moment that personal data is either appropriately destroyed or processed in a way that it is permanently impossible to associate it with the Data Subject from which the data was collected.[135] However, until that moment, the following principles remain applicable and protect personal data during its life span: "the principle of lawfulness, fairness, and transparency", "the principle of purpose limitation", "the principle of data minimization", "the principle of accuracy", "the principle of storage limitation", and "the principle of integrity and confidentiality".[136]

“The principle of lawfulness, fairness, and transparency” is a principle that corresponds to the accountability aspect that has been previously mentioned. It is also one of the most important principles among the six as it provides the threshold to determine the legitimacy of processing activities. However, this principle is made of three different features that are interconnected with each other but aim to achieve goals that are not directly related to one another. Therefore, to better understand the extent of protections provided by this principle, it is important that each feature is viewed individually.

The ‘lawfulness’ feature of this principle highlights the necessity of establishing a legal basis for legitimising a processing activity, which can be secured with options that are adopted by the Member States of the EU[137] or Article 6 of the GDPR.[138] Among them, obtaining consent is the most commonly used option for processing personal data[139], which also is a crucial tool for transferring it to another country, as informed consent opens ways to transmit the data to a jurisdiction that has the worst compatibility with the GDPR.[140] Regardless of the option chosen to satisfy the lawfulness feature of this principle, ‘fairness’ and ‘transparency’ act as a catalyst for it as they advocate for thorough disclosure of how the personal data will be handled and require both the Controllers and Processors to abide by what has been disclosed

[135] Crutzen, Rik, Gjalt-Jorn Ygram Peters, and Christopher Mondschein. "Why and how we should care about the General Data Protection Regulation." Psychology & Health 34.11 (2019): p 1349-1350.
[136] GDPR (n 14), Article 5 (1)
[137] GDPR (n 14), Article 6 (2)
[138] GDPR (n 14), Article 6 (1).
[139] Thobani, Shaira. "Processing personal data and the role of consent." Eur. J. Privacy L. & Tech. (2020): p 94 para 2.
[140] Phillips, Mark. "International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)." Human genetics 137 (2018): p 575 col 1 para 6.

to the Data Subjects.[141] This means that it is crucial for personal data to be used ethically, in a way that the processing of personal data would not result in harming or hindering the general status of the Data Subject, and the exercise of their rights must be respected.[142] For international transfers, what this means is that all the information provided to Data Subjects clearly outlines the circumstances in which the transferring entity and the receiving entity become accountable for their actions. If entities are acting in good faith, this also means that this principle acts as a soft restriction, as when the EU entities are preparing rules for BCRs or creating necessary procedures to comply with SCCs, they will have to avoid transferring personal data to foreign jurisdictions when the risk of violation is high.

The extent of these features goes beyond providing simple baselines; they also demand them to be enforceable and become the custom by requiring appropriate technical and organisational measures to be integrated to complement their effectiveness.[143] This also includes the necessity to keep the Data Subjects up to date with their rights, including the right to object to the transfer or processing of their data, even requesting the data to be erased at any point.[144] To emphasise, if a legal basis has been established with consent for transferring personal data to the US, specifically to California for processing, and the Data Subject requests that their data be erased or demands processing to be stopped in the US, then the necessary technical and organisational capabilities should be in place to coordinate the revocation process and ensure its successful execution.

This is crucial because when personal data is transferred to different countries, it does not have to stay in a specific place. Fragments of personal information may be scattered around different servers or may leave traces, as demonstrated in Figure 6 of Chapter 1. However, while this situation can impose an economic burden on entities, as will be discussed later, some countries may have different requirements for handling and storing personal data, which may place the receiving entities in the middle of another regulatory conflict that requires them to satisfy the provisions of both the local jurisdiction and the GDPR.

Regardless, this example can also be used for “the principle of purpose limitation”, which is the principle that corresponds to the enforcement aspect mentioned earlier. It is less complicated when compared to the principle of lawfulness, fairness, and transparency, and it

[141] GDPR (n 14), Recital 39.
[142] Malgieri, Gianclaudio. "The concept of fairness in the GDPR: a linguistic and contextual interpretation." Proceedings of the 2020 Conference on fairness, accountability, and transparency, (2020); p 156 col 1 para 2.
[143] GDPR (n 14), Recital 71.
[144] GDPR (n 14), Article 12, 17 & 21 (4).

particularly complements the transparency feature of it, as it requires personal data to be collected and used for "specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes–"[145] preventing arbitrary collection and use of the personal data for a purpose that was not disclosed to the Data Subject during the establishment of the legal basis. The advantage provided by this principle is that it aids against challenges that occur when there is a lack of enforcement by DPAs[146], particularly in foreign jurisdictions, as the entities have to outlay every possible processing route before getting a hold of the personal data from the Data Subject. Especially if a transfer is done with consent, the entity that is handling the data must provide a specific scope of operations and limit the use of the data accordingly, otherwise, the consent would be acquired without good faith and thus become invalid.[147] Meaning, that any action, even if required by the local laws, will be considered outlawed because if they were not described during the consent acquisition phase, these activities fall outside the consented scope.

The impact of this principle becomes especially important if we consider that there are no DPAs in some countries, and both the function of regulatory supervision and enforcement are either defunct or insufficient. For example, in the US, there are no DPAs that are comparable to those in the EU; the ones that exist have limited jurisdiction and only cover certain sectors or have no enforcement capabilities at all.[148] No matter whether the protections of a DPA cannot be provided simply by outlaying all the processes that will potentially involve the personal data, at least for the BCRs, it would be able to mitigate the risk to a certain degree by providing grounds for the Data Subjects to understand when a violation has happened, which would allow them to take action from the EU side. However, it would still mean that there will be issues with enforcement on the US side when one of the interacting entities does not have an establishment in the EU and is utilising SCCs to facilitate international data transfers.

Similar problems also exist with "the principles of data minimization" and "the principle of accuracy", which dictate that personal information must not be collected beyond what is

[145] GDPR (n 14), Article 5 (1) (b).
[146] Hahn, Isabel. "Purpose Limitation in the Time of Data Power: Is There a Way Forward?." Eur. Data Prot. L. Rev. 7 (2021): p 37 col 1 para 1.
[147] Gruschka, Nils, et al. "Privacy issues and data protection in big data: a case study analysis under GDPR." 2018 IEEE International Conference on Big Data (Big Data). IEEE, (2018); p 5028 col 1 para 4.
[148] Hamm, Andrew, et al. "Data Protection Laws and Regulations USA 2023-2024" (7 July 2023); Section 1.4 < https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa > [accessed 12 March 2024]

necessary[149] and if the data has been collected from the Data Subject by mistake or any inaccurate information has been acquired for any reason, then it must be erased or corrected to make it appropriate for the lawful use.[150] But, to do these, these principles introduce concepts of "necessity", "proportionality", and "reasonability", which allows the Data Controllers and the Data Processors to assess whether their actions are plausible under these principles in an unregulated foreign jurisdiction.

The concept of necessity provides that information is to be collected only if it is necessary for the purposes provided while establishing the legal grounds for processing the personal data,[151] which complements the principle of purpose limitation by not allowing the possibility of arbitrary processes that may arise during its lifespan. The concept of proportionality also upholds this, as it ensures that the data collected from the Data Subject is pertinent and does not permit the collection of any information that would be in any form deemed as excessive.[152] This does not mean, however, that these requirements become obsolete once the data is collected and transferred to another entity that is not within the EU jurisdiction. No matter whether a BCR or an SCC is used, the concept of reasonability dictates that from the moment the data comes into the possession of an entity, it is still required that they undertake necessary measures and reasonably tend to the personal data by ensuring that the concepts of necessity and proportionality are adhered to.[153]

This is also a benefit derived from the fairness feature of the principle of lawfulness, fairness, and transparency since if the entity does not reasonably tend to personal data, it would be considered to be not acting in good faith. Furthermore, in order to properly manage the data they possess, entities must consider the effects of their actions involving the collected data, and this also extends to transferring the data to other jurisdictions and spreading it among different entities, which, as previously mentioned, could mean fragmentation of personal data and leaving traces in various entities, making it harder for substantial action to be taken for the disposal or correction of the data.[154]

However, it is important to keep in mind that functional and organisational concerns are not the only issues this principle imposes on international data transfers. Non-EU countries may

[149] GDPR (n 14), Article 5 (1) (c).
[150] GDPR (n 14), Article 5 (1) (d).
[151] GDPR (n 14), Recital 156.
[152] GDPR (n 14), Recital 64.
[153] GDPR (n 14), Recital 39.
[154] Li, Jun, et al. "Managing data retention policies at scale." IEEE Transactions on Network and Service Management 9.4 (2012): p 395 col 1 para 1.

have different perspectives on how to minimise personal data and to what degree it should be minimised.[155] Especially in certain circumstances, the action taken in accordance with the limitations provided by a foreign authority might not be compatible with EU standards and prevent their performance, once again resulting in a dispute of jurisdictions due to differences in regulatory approach, especially if there is a lack of cooperation with the EU.

These are also observed with "the principle of storage limitation", which mandates that personal data must be destroyed or anonymised after it has served the purpose for which it was collected, meaning that the data should not be retained for longer than necessary.[156] This can be done in several ways, but regardless, it is required to establish lifespans for the collected personal data and subject them to routine checks on whether the retention period has been exceeded.[157] One thing to keep in consideration is that, together with the principle of data minimisation, this principle prevents personal data from being kept for possible additional scenarios, which has not been disclosed to the Data Subject during the time of collection, even if it is slightly in accordance with the purposes that have been established during its collection. Related to this, it is important to consider that when personal data is transferred to a non-EU country, their local laws may require specific data to be kept for a certain period of time or allow the preservation of personal data when the new purpose is related to the original purpose.

This can complicate international data transfers, especially when data is sent to a non-EU country where such a situation is present because while this might be observed as legal in the transferred country, it would be observed by the GDPR that the data is being kept longer than it should and used for purposes other than those that are allowed in the EU. For example, the US Federal Law require certain kinds of healthcare entities to retain health data in the US for at least 6 years.[158] A similar situation also exists for the finance sector in most countries, where it is possible to come across legal requirements to retain data for even longer periods for anti-money laundering purposes.[159] This essentially means that if an EU entity transfers

[155] Shanmugam, Divya, et al. "Learning to limit data collection via scaling laws: A computational interpretation for the legal principle of data minimization." Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency. (2022); p 840 col 2 para 3.
[156] GDPR (n 14), Article 5 (1) (e).
[157] GDPR (n 14), Recital 39.
[158] The Code of Federal Regulations, "Notice of Privacy Practices for Protected Health Information." (1938); Title 45, Part 164, Subpart E, § 164.530.
[159] Pavlidis, George. "Financial information in the context of anti-money laundering: Broadening the access of law enforcement and facilitating information exchanges." Journal of Money Laundering Control 23.2 (2020): p 376-378.

personal data to a non-EU country, which requires that particular type of personal data to be retained for 10 years, and the Data Subject requests it to be deleted, the EU will attempt to assert its authority over the local jurisdiction and require it to be erased, which naturally will not be accommodated.

This kind of conflict is also happening with "the principle of integrity and confidentiality", which requires personal data to be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"[160], setting the notion that personal data should be protected from direct and indirect threats. Following the example provided for the previous principles, it's possible for the personal data of an EU citizen, which is stored on a server located in a non-EU country, to be requested by the government of that country in accordance with their local laws.[161]

While not complying with this request may satisfy the requirements of the GDPR, it might result in certain penalties as per the local laws, and this would still not guarantee its security because the server is physically located in their jurisdictional borders, and any action can be physically taken for the retrieval of the requested data. This is not a hypothetical scenario. It was exposed in the Snowden Revelations that some of the intelligence agencies in the US resorted to purchasing personal data from companies, and they would attempt to steal it if it was not freely given to them.[162] This shows that the entities in the US partaking in international data transfers with the EU are facing threats from both the EU and the US, which are obviously beyond their control. They constantly face the possibility of punishment from both sides since it is almost guaranteed that complying and not complying with the local request will end up in a violation of provisions provided in this principle.

No matter the tools assert the jurisdiction of the EU by contractual means and the Six Principles supporting them, they make the EU's laws incompatible with most jurisdictions. Considering that the authority acquired with them is virtual, the only thing that remains is disputes over the enforcement of the regulations due to conflicting views. Such circumstances, regardless of whether an SCC or BCRs are used, bring us to the statement of CJEU in Schrems II concerning the restrictions because the invalidation of a transfer appears

[160] GDPR (n 14), Article 5 (1) (f).
[161] See Pavlidis supra note 159.
[162] Andregg, Michael. "Ethical implications of the Snowden revelations." The International Journal of Intelligence, Security, and Public Affairs 18.2 (2016): p 121 para 1.

to be the only option to preserve the rights of the EU Data Subjects[163] and protect the personal data against risks that are present in jurisdictions where there is lack of cooperation.

2.2 Responsive issues concerning international data transfers

The issues discussed in the previous Section arise from the lack of universally accepted privacy laws and standards, along with the conflict between local laws that are not compatible with each other. The regulations that govern national data transfers across countries often conflict with the laws of different jurisdictions, and as demonstrated, enforcement becomes problematic, especially when there is no cooperation. EU is a good example of this, as it has established rules to govern data transfers and rules for the handling of personal data across its borders, but it still faces these issues. As a result, restrictions are put in place as a precautionary measure. However, this practice is not unique to the EU.

This interplay between different legislative requirements may lead to restrictions on the export and import of personal data since enforcement of privacy laws is difficult in foreign territories for any country. One of the motives that leads governments to introduce these restrictions is closely linked to data sovereignty, as the countries try to assert their power and establish authority over cyberspace.[164] One of the approaches that can be used to realise this is by limiting interactions within their own territory due to the gap between the virtual and physical domains. This means the only solution to close this gap is by asserting control over things with more tangible properties inside their borders. As illustrated in the First Chapter, this is because the virtual domain presents significant challenges in establishing control, as its borders do not match those of the physical domain, no matter whether the infrastructure in the physical domain supports the existence of the virtual domain.[165] However, no matter whether these restrictions are enforced as a means to prevent violations, depending on their scale, they have the potential to disrupt international business and trade, which makes them a significant issue that surrounds international data transfers.

Regardless of the motive behind these restrictions, they may target specific outgoing transfer streams to an organisation, transfers based on a country, or impose a general limitation on a

[163] Schrems II (n 60), at Section 121
[164] Mueller, Milton L. "Against sovereignty in cyberspace." International studies review 22.4 (2020): p 791 para 2.
[165] Jensen, Eric Talbot. "Cyber sovereignty: The way ahead." Tex. Int'l LJ 50 (2015): p 296 para 3.

type of data. However, they can briefly be categorised as "preventive measures" and "means of protection". While both methods are essentially related to each other, the time they are imposed and how they are done is significantly different. And despite their cost, these restrictions ensure the efficacy of data protection laws by force, guaranteeing that the rules are respected and not circumvented[166], especially during circumstances where schemes similar to those illustrated in Figure 6 are in place.

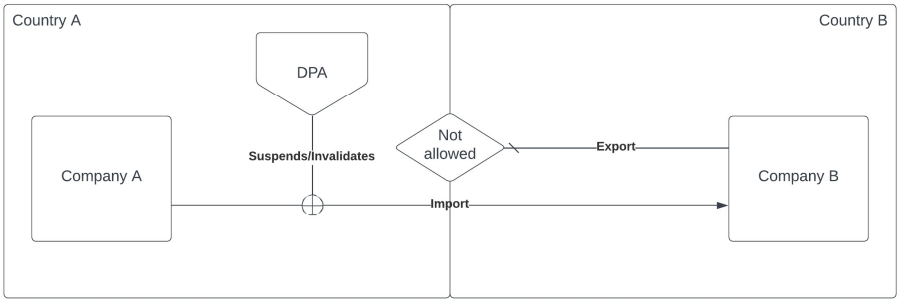

Figure 7: Restrictions on International Data Transfers

2.2.1 Disruption as Protective Restriction

Usually, if a data transfer is restricted as a means of protection, it is because there are serious concerns about the safety of personal data in one of the countries involved in the transfers. This is usually because there is either a lack of cooperation or the enforcement of the rules are not as effective as they should be. Though to call a restriction measure “a protective restriction”, it needs to occur when a continuous data transfer is already taking place, and at least one of the relevant authorities requires these transfers to be suspended. Considering these conditions, the scope of protective restrictions covers transfers to specific entities. When suspensions are introduced in mass, they become a major issue as they may significantly impact business and trade while forcefully asserting data protection and privacy laws through these restrictions.

Nonetheless, protective restrictions are generally smaller in scope than preventive restrictions since they are only implemented when there are no major concerns with all transfers with a specific country, which would require significant intervention. As a result, these restrictions

[166] Christopher Kuner, “Data Nationalism and Its Discontents,” Emory Law Journal 64 (2015): p 2093.

are usually temporary, and their purpose is to ensure the protection of the transferred personal data. From the EU's perspective, these restrictions may be introduced due to the lack of Adequacy Decisions for the country in question or concerns about the effectiveness of appropriate safeguards that were deployed, which, as explained, are closely connected with each other. Particularly for the transfers between the EU and the US, this means utilisation of BCRs and SCCs, which as discussed in the previous Section, possess several shortcomings that would cause these resrictions.

It was mentioned in the previous Section that the CJEU recognises such restrictions as reasonable if there are concerns about the security of personal data, but it should also be noted that this stance by the CJEU reflects a consistent approach rather than an *ad hoc*, or improvised, solution. Supervisory authorities are already empowered to impose such restrictions under Articles of the GDPR[167], but the view of CJEU provides context on when it would be appropriate to use them.

A recent example of this kind of restrictions made in the EU is the order issued in March 2024 by the European Data Protection Supervisor (hereinafter "EDPS"), the institution established before GDPR to monitor the personal data-related activities of other EU institutions[168], where EDPS suspended the data transfers made by the Commission to the US with the use of Microsoft 365.[169] The primary reason for this order was that, since there was no Adequacy Decision for the US, additional safeguards were implemented to facilitate the transfers, however, it was found that they were not properly established by the Commission and not providing necessary protections as they are intended.[170] The restriction in question is temporary, and before the Commission resumes the transfers with Microsoft, EDPS requires the Commission to take necessary actions to ensure that violations that have happened because of failure to properly implement essential safeguards are corrected.[171] The case is ongoing, however, considering the issue directly concerns a transfer that is initiated by the Commission, it will be expected from the Commission to ensure the effectiveness of the

[167] GDPR (n 14), Article 58 (2) (j).
[168] Council Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data OJ L 8 (12 January 2001); Article 2.
[169] European Data Protection Supervisor, "European Commission's use of M365 infringes data protection rules for EU institutions and bodies." Press Release, EDPS/2024/05 (11 March 2024); p 1 para 4 [hereinafter "EDPS Press Release"]
[170] European Data Protection Supervisor, "EDPS investigation: European Commission's use of Microsoft 365." Case 2021-0518 (8 March 2024); Section 207, 364 & 376.
[171] EDPS Press Release (n 170); p 3.

safeguards. However, it is worth mentioning that such restrictions are not only issued by the CJEU nor only because of the incompetence displayed by the EU entity that is directly initiating these data transfers.

In 2021, the Portuguese DPA has issued an order for the National Statistical Institute in Portugal (hereinafter "the Institution") to suspend all data transfers that are realised on Cloudflare's network.[172] The main concern was that the personal data of the EU Data Subjects were collected as a means of authentication and considering Cloudflare was based in the US, there were no guarantees that the collected data would be stored or processed within the EU.[173] Which means that the Institute was not directly conducting the transfers, but its Service Provider, Cloudflare, was executing these transfers to be able to provide its promised services to the Institute. The main concern raised was that Cloudflare always routed the traffic to the nearest data centre that was available, however, there were no guarantees that when an EU Subject was within the network, they would be directed to an EU server, which would create the chance that personal data of EU subjects could be stored in various Non-EU Countries.[174] Considering the data was indirectly collected to provide services to the Institute, according to the guidelines of the EDPB discussed in Chapter 1 of this thesis, the Institute was deemed the Data Controller of these transfers, and thus declared the responsible party for the data. This meant that even though the Institute did not intend international data transfer, it had to cease its interaction with Cloudflare because the transfers were an essential part of the service that was required to be provided.[175]

Both of these cases give us a unique opportunity to assess the likelihood of such restrictions to be presented by the DPAs and other EU authorities, which could be claimed as relatively high because, as explained in the previous chapter, these kinds of relationships established are no longer unique, and outsourcing has become more common than ever thanks to the globalisation. The reason for this is that not only the primary parties but also the third parties that provide additional services are being monitored when considerations are made for these restrictions, creating a larger scope of stakeholders. Additionally, the number of Adequacy Decisions available is limited to only 15, which further increases the risk because transfers to countries other than those 15 will require the implementation of appropriate safeguards. As it has been demonstrated with the examples, it may result in encountering restrictions due to

[172] Comissão Nacional de Proteção de Dados, Deliberação 2021/533 (28 April 2021); at para 42.
[173] ibid, at para 27 & 28.
[174] ibid, at para 38.
[175] ibid, at para 12.

organisational or regulatory complications, or other issues due to the business relationships. Even when actions are taken in good faith, situations similar to that between the Commission and Microsoft or the Institute and Cloudflare can potentially occur at any moment, as internal and external risks always have the possibility of gathering enough magnitude to result in a significant impact that would attract the attention of authorities to restrict the transfer. While it is good to see that the EU authorities are actively supervising and taking necessary actions for the protection of the EU Data Subject's personal data, these resrictions are bad for the business as it disrupts economic operations.

2.2.2 Prohibition and Localisation as Preventive Restriction

Aside from the disruptions by the DPA's and other EU authorities, when a data transfer is restricted as a preventive measure, it is often done in compliance with data localisation laws or orders of invalidations to transfer measures, which result in prohibiting international data transfers for a prolonged period of time. Naturally, while the data localisation laws result in total prohibition that is usually not aimed at a particular country, invalidations of transfer measures result in limited prohibition targeted at a specific country. Unlike restrictions put in place for protection, the safeguards mentioned in the previous Section of this thesis usually do not affect the outcomes of restrictions, especially for a general prohibition with data localisation. Because, in addition to asserting authority and ensuring sovereignty, the prohibition of data transfers to a specific country or the creation of localisation laws that trap personal data within the jurisdictional borders is driven by the desire to protect their data subjects' personal data from unfair or unlawful practices like foreign intelligence surveillance practices[176] or general concerns over data security due to state practices.[177] This means that consideration is often given to the actions of the foreign government or to events that have occurred repeatedly and could not have been prevented or were purposefully allowed by them. Therefore, as it will be explained in this Sub-section these restrictions differ from protective measures and are not aimed at specific parties and their activities to resolve them on a case-by-case basis. Instead, they represent a general stance against events that have

[176] Ursic, Helena, et al. "Data localisation measures and their impacts on data science." Research Handbook in Data Science and Law. Edward Elgar Publishing (2018); p 333 para 1.
[177] Aaronson, Susan. "Why trade agreements are not setting information free: The lost history and reinvigorated debate over cross-border data flows, human rights, and national security." World Trade Review 14.4 (2015): p 682 para 1.

precipitated the need for such measures, as the safeguards provided by them are either purposefully violated or become ineffective due to different variables.

The invalidation of the Safe Harbor and Privacy Shield is a good example of the limited prohibition aspect of preventive restrictions that concern the US. Because, in Schrems I, CJEU stated that due to the surveillance activities of the US, it was apparent that Safe Harbor has failed to recognise the individual rights of the data subjects and thus failed to provide the protections that must be secured with this instrument; hence it was decided that it should be invalidated.[178] A similar decision was also given in the Schrems II as the CJEU viewed the practices performed for national security purposes as unlawful under GDPR and agreed that the practice of such activities is incompatible with the protections provided by the Privacy Shield, thus invalidating it.[179] While the entities interacting between both countries were conducting their transfers in accordance with these frameworks, significant concerns arose regarding the US's practices on its own soil and its inability to ensure the protections granted by the GDPR.[180] Both of these decisions have disrupted and temporarily blocked transfers to the US, and some companies had to halt them until they could come up with other ways to realise the transfers.

What differentiates these from protective restrictions is that the main target was not the parties that were realising but the tools that were allowing the transfers to the US. And when the CJEU decided to invalidate these frameworks, more than one party was affected by the outcomes resulting from this decision because there were a considerable amount of entities realising their transfers through these frameworks to benefit from the lesser bureaucratic burden. It must be emphasised that, this is not the same as invalidating a BCR or a set of SCCs, since those tools of transfer are created as templates for general use, as in, for any transfer that could be made across the borders of the EU. Safe Harbor and Privacy Shield, on the other hand, were specialised frameworks that were created particularly for the US. Although the decision of CJEU had a sudden and damaging impact, it did not last too long as the EU and US reached another agreement.

On the other hand, permanent restrictions are more complicated and thus, their impact is stronger. They are usually supported by the localisation laws, which scholars describe them

[178] Schrems I (n 12): para 31, 33 & 107.
[179] Schrems II (n 60) para 115, 191 & 203.
[180] Rotenberg, Marc. "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection." European Law Journal 26.1-2 (2020): p 149 para 1.

as those that "limit the storage, movement, and/or processing of data to specific geographies"[181] or those "that limit the companies that can manage data based upon the company's nation of incorporation or principal sites of operations and management"[182]. Similar to the description of Xiao, these laws essentially view data transfers as interactions between two servers in different geographic areas and are specifically aimed at regulating what is stored in them. Consequently, they target entities within their supposed virtual borders where their interactions are performed through the networks supported by their own physical infrastructure, as enforcing the requirements imposed for handling personal data is easier within their own territory.

Although the intention behind the practice may be pure, it carries an inherent ethical dilemma as it can easily be misused. Thus, these kinds of rules are not always perceived positively due to economic reasons and concerns about personal data, particularly by those whose personal data and business operations are at stake. For example, some scholars see Turkey as one of the leading countries requiring forced localisation.[183] This is because the Turkish Government has increasingly required foreign entities to store specific types of personal data related to Turkish citizens on servers that is within the geographical borders of Turkey. The first localisation requirement was introduced in 2016, mandating that all finance-related entities operating in Turkey must conduct their data processing activities within the jurisdictional borders[184], which has led to PayPal withdrawing from the local market because it did not establish a data centre in the country.[185] However, as time passed, the regulations pertaining to localisation rules became increasingly alarming. During the second wave in 2020, social media companies were required to localise the personal data of Turkish citizens, and with the third wave in 2022, it was uncovered that the government intended to enforce laws with arbitrary circumstances to penalise individuals for their actions in social media, which then lead to concerns regarding overall privacy and security of individuals on the web.[186]

---

[181] Panday (n 194): at p 513 para 1.
[182] Hill, Jonah Force "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," Lawfare Research Paper Series 2, no. 3 (2014): p 3 para 5.
[183] Shekhar, Raj, and Aman Yuvraj Choudhary. "Data Localisation and Cross-Border Flow of Data: Balancing the Incongruent Dimension of Barriers, Safeguards and" Free Flow of Data"." RGNUL Fin. & Mercantile L. Rev. (2022): 19.
[184] Ursic (n 176), p 329 para 4.
[185] Business Insider "PayPal is Shutting Down in Turkey", Insider Intelligence (1 June 2016) < https://www.businessinsider.com/paypal-is-shutting-down-in-turkey-2016-6 > [accessed 24 March 2024]
[186] Vurkır, Namık Berk. "Concerns over the new trends of censorship in Türkiye." Estonian Human Rights Centre, (25 October 2022) < https://humanrights.ee/en/2022/10/censorshipturkey/ > [accessed 24 March 2024]

This shows that data localisation rules can be employed for the protection of personal data by removing all the interference depicted in Figure 5 in the previous Chapter, or at least limiting it until a certain degree and forcefully housing the full circle of processing activities within the same geographical borders, while they can also be utilised for other unethical purposes that may negatively and directly interfere with privacy. Thus, this example illustrates consequences on three fronts: impact on individual privacy, impact on business, and impact on government practices. Furthermore, the practices of the government can escalate to a point where they enhance the capabilities of surveillance programs run by government agencies. This is because the government in the country where the servers are located can easily access them. This was highlighted in the Snowden Revelations, which exposed how intelligence agencies resort to stealing it by tapping into the Tier 1 ISPs of their networks if the requested data was not provided to them willingly.[187]

GDPR still allows the transfers of data to countries with localisation laws, as long as explicit consent is taken from the Data Subject.[188] However, considering complexities surrounding the enforcement in foreign territory, it is hard to predict what would happen to personal data that is requested to be erased by the Data Subject but has once transferred with proper consent and is now required by local laws in the Non-EU Country to be preserved. Related to this, what makes these kinds of restrictions an issue is not only because different countries may require localisation of certain data when it is transferred to their territory but also because the EU may require this in the future. Experts have been discussing after Schrems whether the EU should localise the personal data of the EU Data Subjects and only allow the processing of their data within its jurisdictional borders[189], where Kuner stated a few years ago that there have been incentives and willingness for the EU data localisation in the market.[190]

Considering the EU's position in the global market, there could be a standoff between EU Member States and non-EU countries. This situation could also affect countries with Adequacy Decisions, potentially leading to a form of Balkanization. Such an outcome would have catastrophic consequences for both the EU and the global economy.[191] Additionally,

[187] See Andregg supra note 163.
[188] GDPR (n 14), Article 49 (1) (a).
[189] Christakis, Theodore. "'European Digital Sovereignty': Successfully Navigating Between the'Brussels Effect'and Europe's Quest for Strategic Autonomy." SSRN 3748098 (2020); p 69-74.
[190] See Kuner supra note 106.
[191] Bauer, Matthias 'The Economic Importance of Getting Data Protection Right' ECIPE (2013); p 7-8.

there would be a technical impact, as discussed in Chapter 1 of this thesis. Tier 1 ISPs, which are crucial for the global network and routing packets on behalf of other ISPs, would be significantly affected as, if Balkanization were to occur, it would not be wanted by companies to have their packets enter the EU zone and would need to find a new route. Moreover, following the example of Turkey and PayPal, there might be similar instances where companies refuse to comply with these regulations and entirely exit the EU market. Furthermore, it is still possible that certain activities like surveillance can be done by remotely accessing the data and simply viewing it[192], meaning that localisation would not fully provide the protections that are desired as long as a full lockdown is set. Therefore, the isolation of the EU market with localisation laws may not be as beneficial, however, it is still a possibility that is not far from reality.

The primary takeaway from this chapter is that EU laws, due to their ethical and foundational obligations, serve as both a solution and a problem regarding international data transfers. In particular, the GDPR, while offering necessary protections for the digital rights of EU Data Subjects, provides solutions with extraterritorial characteristics that seek to assert EU authority by extending its scope. The Six Principles primarily drive this, influencing the laws of foreign countries interacting with the EU in such a way that necessitates their alteration or modification.[193] If entities do not comply with the EU's data protection laws, it leads the EU to adopt an overly protective stance, halting all interaction. This demonstrates that EU privacy laws are structured in such a way that they cannot engage with any jurisdiction that does not fully acknowledge their authority. Even the flexibility offered through BCRs and SCCs demands complete cooperation from foreign jurisdictions. Consequently, the EU encounters challenges with the GDPR concerning territorial scope, enforcement, and jurisdictional conflicts. Scholars argue that such restrictions are a barrier to trade[194], and the reactions of GDPR have the potential to create a worldwide impact.

However, it's crucial to acknowledge that this situation is also a result of the EU's purposefully dismissal of its impact. The European Parliament (hereinafter “the Parliament”) has emphasised that data protection and the right to privacy are paramount, outweighing

[192] Hill (n 182), p 29.
[193] See Mattoo supra note 94.
[194] Panday, Jyoti, and Jeremy Malcolm. "The political economy of data localization." Partecipazione e conflitto 11.2 (2018): p 513 para 2.

economic gains, and should not be compromised for profit.[195] Meaning that every interaction in cyberspace involving the EU will be strictly governed by EU regulations, without exception. This leads us to consider how the interplay between different jurisdictions can be resolved without sparking a conflict that could trigger a reaction. Particularly when the transfers are happening with the US.

[195] European Parliament "Resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI))" Official Journal of the European Union, C 35/21 (31 January 2018); Clause M.

CHAPTER III: TRANSFERING DATA BETWEEN THE EU AND THE US

3.1 Current Landscape for Transfers

As Kuner says, “the regulation of international data transfers relies heavily on bureaucratic, formalistic measures--”[196] and navigating through complexities caused by these measures is essential for finding solutions to the issues related to international data transfers. Currently, there are three possibilities for transferring personal data from the EU to the US: BCRs only for transfers to the group companies, SCCs and the DPF for any transfer for any company. All of them come with a comparable bureaucratic burden and unique issues, which consequently impact the handling of personal data in the US. The main reason why these issues still exist today is due to the lack of an Adequacy Decision for the US. Considering the shortcomings of the US legal landscape, there have been no Adequacy Decisions to date, thus, free transfers of personal data were never been allowed, and this puts a strain on both EU and US entities. As previously mentioned, one solution that both parties came up with was to facilitate the safe transfer of personal data through various frameworks, which require the active participation of the interested parties and do not have proper backing from US laws. However, the reason why the Adequacy Decision was not given also had an impact on these frameworks and ultimately led to arguments about the protections they provide when the data is transferred to the US with them.

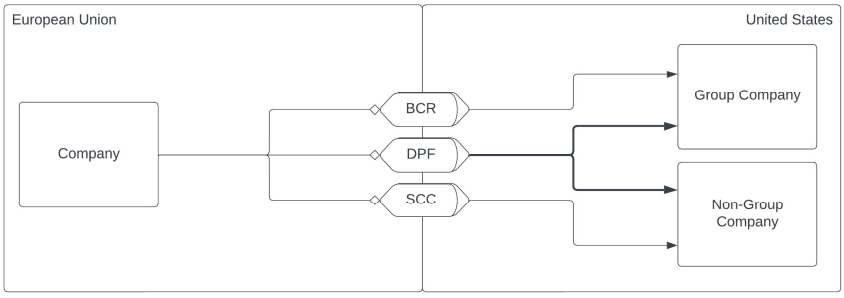

Figure 8: Methods for transferring data between the EU and the US - highlighting the scope of DPF.

After the DPF was introduced and the Commission revealed its plan to renew the specialised transfer mechanism by granting an Adequacy Decision to the US through the DPF, the Parliament expressed its objection with a resolution concerning the Adequacy Decision for the DPF, confirming that the US has yet to meet the GDPR's criteria necessary to obtain

[196] See Kuner supra note 106.

one[197], indicating that there have not been any substantial differences with the US law since the invalidation of the previous framework. Despite this, the Commission decided to proceeded with adopting the Adequacy Decision.[198] However, as repeatedly mentioned, the Adequacy Decision in question is not a standard one, it is limited *per se*.

What differentiates the Adequacy Decision that has been given to the US and the other countries that possess an Adequacy Decision is that this so-called Adequacy Decision permits the free flow of personal data only to the US entities recognised by the US Department of Commerce as 'safe', when they are compliant with the provisions of the DPF.[199] Therefore, the scope of the Adequacy Decision is limited to those participating in this framework and does not cover every US entity. Consequently, this means that unlike other countries that have received an Adequacy Decision, direct transfers from the EU to the US without any safeguards are still strictly forbidden. Should an EU entity wish to transfer data to a non-DPF-certified US entity, it can still do so with the BCRs and SCCs. However, as it will be explained later, this Adequacy Decision also has no impact on the requirements and procedures concerning the BCRs and SCCs, it only covers interactions and the structure concerning the DPF.

This structure establishes a legal order featuring duality that sets forth different requirements from both EU and US entities, raising questions regarding the real condition of the US legal framework: The Commission's decision to establish the DPF and, through it, asserting that the US offers adequate protection, suggests compliance with the GDPR and everything is in place on the US side. However, the Parliament's objections and the continuity of the demand for safeguards when initiating transfers without the use of DPF illustrate a conflict of views on the US. Therefore, it is essential to understand the rationale behind the Commission's decision to grant the US an Adequacy Decision and its endorsement of the DPF, despite the objections from the Parliament.

---

[197] European Parliament "Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework" 2023/2501(RSP) (11 May 2023); Clause 9 < https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html > [accessed 20 March 2024 – "Parliament on DPF"]

[198] European Commission "Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework" (20 September 2023); Section 206 & 208 < https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj> [accessed 20 March 2024 – hereinafter "Commission on DPF"]

[199] ibid, Article 1.

One of the biggest reasons behind the Commission's decision was President Biden's 2022 Executive Order titled "Enhancing Safeguards for US Signals Intelligence Activities"[200], also called "EO 14086", which supposedly addressed the concerns mentioned in the Schrems I and Schrems II regarding the activities of the US intelligence agencies and unauthorised access to the EU Data Subject's personal data, its goal was to limit the scope of these surveillance activities and pull it to a margin that is acceptable by the EU laws.[201] Given that the Commission has reviewed this Executive Order and compared it with the issues raised in the Schrems cases[202], and has still decided in favour of the Adequacy Decision, it is clear that they regard the provisions of the Executive Order as sufficient. Furthermore, as an addition to its position on DPF, the Commission also stated that protections provided by the Executive Order applies to any transfer method used.[203] EDPB is also of the same opinion and affirming that the protections of the Executive Order extend to other methods of transfer provided by the GDPR.[204] However, it is crucial to understand that the scope of the Executive Order's by nature, are limited, and it does not really give any protections against the activities that is mentioned in it because it does not amend any regulations governing intelligence agencies' activities, nor does it resolve the issues identified in the Schrems cases. Meaning that the protections provided are not as effective as it is viewed by the Commission and the EDPB.

To emphasise, the content of the Executive Order explicitly provides instructions to the intelligence agencies to make a distinction between US and non-US persons, stating that surveillance activities targeting these two groups should not be conducted in the same manner[205], however, despite this differentiation, it consistently cites "applicable US law" throughout its sections as a crucial reference point for evaluating the proportionality and necessity of intelligence activities before performed, which directly applies to the justification of these activities when they are carried out on non-US persons. This means that, true to its name, the Executive Order merely introduces measures that postpone the surfacing of actions leading to the concerns outlined in the Schrems cases.

[200] Commission on DPF (n 201), Clause 7
[201] Executive Order (n 16); Section 2 (iii) (A) (1) (a) & (2) (a), (2) (b), (2) (c).
[202] Commission on DPF (n 198), at Clause 5 & 6
[203] European Commission "Questions & Answers: EU – US Data Privacy Framework" (10 July, 2023); Section 7 < https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752> [accessed 20 March 2024]
[204] European Data Protection Board, "Information note on data transfers under the GDPR to the United States after the adoption of the Adequacy Decision on 10 July 2023" (July 2023); p 2 para 3
[205] Executive Order (n 16); Section 4.

This raises doubts on whether there is a substantial impact of the Executive Order on general practice in the US and how far the so-called precautions are reacing, which also leads to suspicions over the longevity of the DPF as this situation is suggesting the possibility of a third Schrems case emerging soon. Scholars concur, arguing that changes are necessary to relevant US Federal laws and that the Executive Order should be supported with these changes in the legislation, as an Executive Order by itself does not diminish or prevent the scope of existing law; it only imposes an extra bureaucratic hurdle to achieve what the law already permits.[206] This means that while the DPF, in conjunction with the Executive Order, appears to be addressing the concerns raised and offers a level of protection on paper, it is not, because its capabilities are limited. Following this, the protections that are mentioned by both the Commission and EDPB to be extending to the BCRs and SCCs are not elevating the concerns over the issues that are observed while the transfers are made with them, because as it will be explained in the upcoming pages, DPF is covering most of the enforcement related requirements to turn the provision of the Executive Order to be effective.

While the provision and basis of Adquacy Decision was initially one of the main concerns that caused the objection by the Parliament, the other is related to the fact that "the United States still lacks a federal data protection law"[207]. The Parliament is especially concerned with the lack of data protection laws in the US, and it refers to two important aspects of the current US legal landscape on privacy laws which causes issues on its compabilitiy with the GDPR; the inefficacy and imbalance between Federal and State laws. At the State level, only a quarter of the Federal States have laws dedicated to privacy, and only a number of them are in force as of 2024.[208] This means that most of the Federal states do not have comprehensive laws regulating affairs related to the protection of personal data, let alone having regulations that are comparable to the GDPR. This consequently means that they are unable to provide necessary protections for their own Data Subjects from the perspective of the GDPR. This situation is not better at the Federal level as the Federal laws are "sectoral, with different laws regulating different industries and economic sectors."[209]. This sectoral approach creates more problems than a totally unregulated envoirenment as while they are particularly governing

[206] Batlle, Sergi, and Arnaud van Waeyenberge, "EU–US Data Privacy Framework: A First Legal Assessment." European Journal of Risk Regulation 15.1 (2024): p 196-197.
[207] Parliament on DPF (n 197); Clause 12.
[208] See IAPP Tracker supra note 18.
[209] Solove, Daniel J., and Woodrow Hartzog. "The FTC and the new common law of privacy." Colum. L. Rev. 114 (2014): p 587, para 2.

activities related to healthcare, financial, education, marketing and telecommunications, they leave large areas unregulated.[210]

This means that since there is no centralised law in the US like in the EU, places where the State laws exist may have conflicting outcomes when they are not in coherence with the Federal laws and covering areas that are not under the protection of Federal laws. This is important, because, from a general perspective, this also means that the evaluation process for the actions concerning personal data by both private and public entities relies on various differentiating indicators, which also influence the outcome of any possible proceedings. Particularly for the affairs related to the private entities, the outcome may change based on the regulations that exists on the Federal State to which personal data is transferred. Considering the EU provides uniform protection that is applicable in every Member State, to any sector and any personal data, which is also integrated into the national laws of the Member States, this ultimately leads to an undesired arbitrary system that fails to uniformly address practical issues and creates loopholes that could be taken advantage of, and cause issues that would be related to accountability and enforcement.

Therefore, this thesis takes the position that aligns with the objections of the Parliament, because there are major concerns regarding sufficiency of US legal landscape on privacy laws, particularly because they are out of balance and do not provide sufficient protections nationwide, which makes US an unsuitable destination for the transferring EU Data Subjects personal data. It would be unfair to not recognise the advancements that have improved the general standig of the US privacy laws, particularly with the Executive Order is an important step that has been taken for the regulation of the activities which have been a menance for partnership of EU and US for more than 20 years, however, the provisions provided are not effective enough to consider that they provide the required protections. Following this, we also can see that much has not changed for BCRs and SCCs, as there have been no significant changes on the US legal landscape.

3.2 State of Accountability, Cooperation and Enforcement

No matter there are concerns over the US legal landscape, the international data transfers are still happening with the prementioned means of transfer. Which brings us the question what is

[210] See Solove supra note 209.

the state of accountability, cooperation, and enforcement, which as argued in the previous chapters play an important role on the regulation of the data protection and privacy across the borders of the EU. Considering there is a dual system in the US, the most effective way to understand the status of these notions would be comparing them side by side for every transferring mechanism.

As previously mentioned, there are issues regarding accountability and enforcement for BCRs and SCCs as the GDPR, because it is only applicable in the EU's jurisdictional borders and only way to ensure that its provisions are adhered to is based on respecting the rule of law thorough contractual obligations that are established when the involved parties prepare these methods. This is where the BCRs, SCCs, and DPF are divided as while BCRs and SCCs are only executed by the authority of the EU, while DPF is executed by the authority of both the EU and the US, and predominantly governed by the US, which eliminates some of the concerns related to accountability and enforcement. Therefore any concern left regarding to protection of the personal data in the US becomes an issues not related to the tools of transfer but the means of protections provided by the US laws.

The requirements outlined in DPF are the biggest reason why the accountability and enforcement is not in the same state as BCRs and SCCs. Simillar to the GDPR, these requirements are provided as a set of 23 principles that are known as the "DPF Principles", and they are divided into "Main Principles" and "Supplemental Principles".[211] A The main principles include only 7 of 23, which can be seen as a way to adapt the Six Principles in the US soil because they are inspired by the Six Principles of GDPR. They are namely; "principle of notice" and "principle of choice" which corresponds to "principles of lawfulness, fairness, and transparency", "principle of accountability for onward transfer" which corresponds to "principle of accountability", "principle of security" which corresponds to "principle of integrity and confidentiality", "principle of data integrity and purpose limitation" which corresponds to "principle of purpose limitation", "principle of access" which corresponds to "principle of data minimisation" , and "principle of recourse, enforcement and liability".[212] Particularly, the last principle, "the principle of recourse, enforcement and liability" adheres to issues that are related to the accountability, cooperation and enforcement as it provides the

[211] U.S. Department of Commerce and the International Trade Administration "Participation Requirements Data Privacy Framework (DPF) Principles." Data Privacy Framework Program (July 2023); Section II & III < www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles> [accessed 20 March 2024 – hereinafter "DPF Principles"]
[212] ibid.

basis for the appointed legal authorities the scope for duties and makes these three notions core of the framework.[213]

As an addition to these, the remaining 16 Supplemental Principles reflect other provisions of the GDPR, including concepts like the distinction of sensitive personal data, extension of liability, dispute resolution, and the rights of data subjects.[214] Related to this, following the arguments that have been provided during the Parliament's resolution on objecting to granting Adequacy Decision to the US, we can see that DPF plays an important role in setting a landscape that aligns with the GDPR because the US does not have appropriate laws to establish these principles. One of the reasons why BCRs and SCCs are effective in the US is because it is unable to enforce the Six Principles. This was mainly because, apart from willingly submitting oneself to the EU's authority, which would contradict the US laws, there existed no legal foundation to enforce the Six Principles in the jurisdictional territory of the US. However, the DPF makes its own principles obligatory and only allows free data transfers when they are integrated into their day-to-day business operations.[215] This is what clearly distinguishes DPF from BCRs and SCCs, as well as its predecessors. The DPF Principles are mutually agreed upon by both countries and certified to meet the legal requirements of both sides, which facilitates the necessary cooperation and hypothetically prevents clashes of regulatory requirements. On the other hand, the Six Principles applicable through the use of BCRs and SCCs are still unilaterally decided and enforced only by the EU, which naturally causes issues with their enforcement without cooperation.[216]

However, the enforcement aspect is also supported by the cooperation aspect by appointing the US Department of Commerce, the US Federal Trade Commission, and the US Department of Transportation as regulatory entities.[217] DPF grants them the authority to oversee US entities' activities, requiring compliance with the framework in line with the "principle of recourse, enforcement, and liability", which ensures adherence to DPF principles from both sides.[218] Contrary to the BCRs and SCCs, which are stand-alone and do not have any support from the US side for the matters that are related to to violations of the

[213] See DPF Principles supra note 211, at Section II (7)
[214] ibid.
[215] Commission on DPF (n 198); Clause 45.
[216] Schwartz, Paul M. "The EU-US privacy collision: a turn to institutions and procedures." Harv. L. Rev. 126 (2012): p 1991 para 2.
[217] Commission on DPF (n 198); at Clause 9.
[218] ibid, at Clause 47, 53, 59, 60, 61, 69.

GDPR provisions, there is active supervision for the issues that arise from the US side, which is adding additional protection in case a dispute arises.[219]

DPF does not only appoint regulatory authorities, but it also utilises the newly established Data Protection Review Court for judicial matters[220], as the US grants it the authority to issue binding decisions on cases related to data protection and privacy that are presented before it.[221] This means a comprehensive system is established on paper to facilitate the full cycle of enforcement-related affairs on the US side, which transfers with BCRs and SCCs need but cannot benefit. However, EDPB noted that the jurisdiction of this court is not enforceable against the US authorities[222], this undermines the effectiveness of DPF and serves as a reality-check, as this means that even if a case is brought against an intelligence agency due to the activities impacting EU Data Subjects, there is a significant chance that decisions of this court will not be respected. This could potentially lead to restrictions or invalidation of DPF, as one of the most debated subjects during the provision of the limited Adequacy Decision was related to the activities of state agencies. However, EDPB does not believe that this court is completely powerless. It recognizes that the court's capabilities are strictly limited to how far the US is willing to cooperate.[223]

However, if we disregard this possibility and pretend that the US has fully committed to the DPF and willing to adhere to the provisions of the GDPR, this greatly changes the scale and ensures enforcement of standards compared to the GDPR in the US, as these circumstances are not possible when an international data transfer is realised with the BCRs and SCCs. Because, in both scenarios, the EU is unable to effectively prevent or deter US entities from violating the GDPR through punishment or administrative actions as these entities are beyond its reach. The EU can only impose punishment on a corporate group through the EU subsidiary when BCRs are being used, which is not applicable with the SCCs as it is mainly used for transfers involving non-group entities. Alternatively, the EU can only impose restrictions that could disrupt or prohibit the transfer. Naturally, this collaborative aspect of the DPF effectively facilitates cooperation between the EU and the US in regulatory

[219] Commission on DPF (n 198); Annex I
[220] ibid, at Clause 176.
[221] Executive Order (n 16); Section 3 (ii) (A) & (C)
[222] European Data Protection Board "Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework" 05/2023 (28 February 2023); Clause 167
[223] ibid, at Clause 220

matters[224] and arguably enforces GDPR's provisions across its borders. Because now, there are three US departments that can oversee the activities of the US entities, and a court, which effectively apply the DPF's principles which as previously mentioned, and are inspired by the Six Principles of the GDPR. Even further, if the results are not satisfactory for the persons that has brought a case due to a violation, DPF provides the possibility of pursuing legal action against a US entity on the EU side, with the assistance of the US regulators, which pulls the current landscape to new hights as it guarantees protections from both sides.[225]

Of course, even in cases where it is not permitted, EU authorities can take action against the Data Controller at any time, similar to their approach with BCRs and SCCs.[226] This is because the EU entity becomes responsible for the protection of personal data the moment it crosses the virtual borders of the EU and reaches the destination country.[227] However, this approach would have a limited effect, as personal data would have already been exposed to risks, and the damage could not be reversed. Although this is not a long-term solution, it is particularly harmful because if the jurisdiction of one country permits a specific action while another actively opposes it, this could lead to numerous violations. Ultimately, the latter country might resort to completely banning any interaction with the former. This is what we have observed with the Schrems cases, as the issue of accountability was not directed to the private sector practice but the public sector practice, the violating parties were known, and no action could be taken against it and only solution was invalidation of frameworks.

In the context of data protection, if incidents of data breaches continue to happen, it could lead to a situation like Balkanization, which would be more than just a simple restriction and could negatively affect the relationships between all the partner countries involved and consequently impact the global economy.[228] Therefore, it is crucial to identify the party responsible for the breach and hold them accountable to prevent any harm to the existing legal structure and partnerships. Nevertheless, this issue only remains for BCRs and SCCs, but it does not exist with the DPF, as the DPF principles establishes accountability[229] and cooperation aspect of the framework enforces it because it is a key part of overseeing the

[224] Commission on DPF (n 198); at Clause 70-78.
[225] ibid, at Clause 73.
[226] European Data Protection Board, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" 01/2022 (18 June 2021); Clause 60, 65 & 130
[227] GDPR (n 14); Article 24.
[228] Nicola, Fernanda G., and Oreste Pollicino. "The balkanization of data privacy regulation." W. Va. L. Rev. 123 (2020): p 115 para 2
[229] DPF Principles (n 212); Section II (4)

activities of US entities and links them to their obligations. The Commission also affirms this and states that accountability is an integral part of the DPF.[230] While this arrangement ensures that there are no hurdles when claims are made against US entities violating the rights of EU Data Subjects, which also extends to third parties involved in processing activities.[231]

At the time of writing, the DPF has not yet completed its first year. Since it is a recent development, there is not enough data to determine its effectiveness in the coming years. There are concerns regarding its longevity, similar to its predecessors. However, one thing that is clear is that it does not face the same issues that BCRs and SCCs are experiencing. While we are still grappling with questions about effective enforcement and accountability, the DPF has already solved these issues, and the questions directed towards it are about the effectiveness of legislation. Although its support is limited, the DPF is backed by US laws that echo the requirements of GDPR. Additionally, there are US governmental institutions responsible for supervision, enforcement, and judicial matters. Which shows us the steps to an effective regime to regulate the privacy related matters between two countries.

[230] Commission on DPF (n 198); Clause 44.
[231] Commission on DPF (n 198); at Clause 38, 40, 45, 46.

CONCLUSION

Navigating the complexities of international data transfers involves dealing with issues unique to both the physical and virtual realms. The challenge lies in the physical realm's inability to accurately reflect the virtual realm, making it difficult for scholars and lawmakers to fully understand the nature of international data transfers. This often leads to regulations that are either insufficient or excessively stringent. Since the physical borders do not exist in the virtual realm, managing interactions involving international data transfers presents challenges, complicating enforcement efforts by regulatory authorities. Despite these obstacles, we still possess certain tools that allow us to comprehend the virtual realm's nature. However, our attempts to apply rules based on the physical realm's characteristics, without considering the rapid technological advancements, render the legal frameworks for the virtual domain either outdated or incapable of providing comprehensive coverage.

While problems with international data transfers are common, there are specific issues that arise from the interactions between countries due to significant differences in how they approach data protection and privacy. These differences exacerbate the already existing challenges, making international data transfers even more difficult than necessary. In particular, the EU and the US have been working together to find ways to facilitate data transfers between them. However, their legal frameworks are so different that disputes arise at the first sign of conflict. This illustrates that, in addition to the technical and general legal issues surrounding international data transfers, there are also complications caused by incompatible legal frameworks.

The main issue within the EU is the Six Principles of GDPR, which protect an EU Data Subject's personal data from the moment it is created until it is destroyed. Exiting the jurisdictional borders of the EU does not diminish the protections afforded by the Six Principles, as they are tied to the personal data and follow it wherever it goes. This situation creates challenges, especially in terms of accountability and enforcement. These aspects play a crucial role in the regulation and execution of privacy regulations, as they are instrumental in identifying and attributing responsibility for actions taken with the personal data during its processing activities.

The GDPR's tools are designed to facilitate data transfer by preparing the environment in advance. However, most of the time, these tools struggle to secure cooperation from regulatory authorities in the receiving state, causing their effectiveness to diminish quickly.

Even the specialized frameworks developed between the EU and the US, such as voluntary self-certification systems like the DPF, face challenges. Despite being crafted through detailed negotiations to meet the specific needs of both regions, they cannot bridge the regulatory gaps, ultimately impacting accountability and enforceability.

Currently, the DPF has not completed its first year, and its future remains uncertain. When examining the specifics of the DPF, it becomes apparent that there are no significant differences from its predecessors, despite the involvement of more instruments and entities within the framework. The main reason their existence has not made a significant impact is that all developments up to this point are merely bureaucratic schemes that do not lead to any real change. What is permitted by US law is still accessible to the entities that were previously eligible to exercise their rights as granted by the law. The only change is that legitimizing actions may now require more time. However, the blame does not solely lie with the US, as the characteristics of the GDPR make it a difficult instrument to work with. Especially due to the Six Principles, it is almost certain that the GDPR is unable to interact effectively with any jurisdiction that is identical or significantly similar to its structure.

Currently, the mechanisms for transfers are operating correctly, enabling the legitimation of transfers between the EU and the US for entities wishing to participate in DPF. However, it is almost certain that Schrems III is on the horizon, and the transfer tools provided by the GDPR will continue to be inefficient. This will result in the cycle we've been observing since the early 2010s: a new specialized tool will be introduced, EU authorities will either revoke or suspend this tool, and entities will revert to traditional transfer mechanisms until another specialized tool is introduced.

BIBLIOGRAPHY

BOOKS

1. Briner, Russell F., and Sid R. Ewer. "Financial information flow and transborder restrictions." Journal of Systems Management 38.8 [1987]
2. Clark, David D., Kenneth T. Pogran, and David P. Reed. "An introduction to local area networks." Proceedings of the IEEE 66.11 [1978]
3. Galbreath, Jeremy. "Compressed digital videoconferencing: An overview." Educational Technology 35.1 [1995]
4. Gupta, B. M., and S. P. Gupta. "Transborder data flow debate." [1982]
5. IEEE Computer Society. LAN/MAN Standards Committee, International Electrotechnical Commission, and IEEE Standards Board. “Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Overview and Architecture” No. 802. IEEE, [2015]
6. Kelley, Sam. "Global Network System" Bibliotex Digital Library [2022]
7. Li, Jun, et al. "Managing data retention policies at scale." IEEE Transactions on Network and Service Management 9.4 [2012]
8. Naef, Tobias. "The Restrictive Effect of the Legal Mechanisms for Data Transfers in the European Union." Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law. Cham: Springer International Publishing [2022]
9. Nurse, Jason RC, et al. "Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy." HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part III 23. Springer International Publishing, [2021]

JOURNALS

10. Aaronson, Susan. "Why trade agreements are not setting information free: The lost history and reinvigorated debate over cross-border data flows, human rights, and national security." World Trade Review 14.4 [2015]
11. Andregg, Michael. "Ethical implications of the Snowden revelations." The International Journal of Intelligence, Security, and Public Affairs 18.2 [2016]

12. Batlle, Sergi, and Arnaud van Waeyenberge, "EU–US Data Privacy Framework: A First Legal Assessment." European Journal of Risk Regulation 15.1 [2024]
13. Bauer, Matthias 'The Economic Importance of Getting Data Protection Right' ECIPE [2013]
14. Berger, Eric. "Individual Rights, Judicial Deference, and Administrative Law Norms in Constitutional Decision Making." BUL Rev. 91 [2011]
15. Boland, Joshua, et al. "A COVID-19-era rapid review: using Zoom and Skype for qualitative group research." Public Health Research & Practice 32.2 [2022]
16. Bradford, Laura, Mateo Aboy, and Kathleen Liddell. "Standard contractual clauses for cross-border transfers of health data after Schrems II." Journal of Law and the Biosciences 8.1 [2021]
17. Cate, Fred H. "Government data mining: The need for a legal framework." Harv. CR-CLL Rev. 43 [2008]
18. Chang, Younghoon, et al. "The role of privacy policy on consumers' perceived privacy." Government Information Quarterly 35.3 [2018]
19. Christakis, Theodore. "'European Digital Sovereignty': Successfully Navigating Between the'Brussels Effect'and Europe's Quest for Strategic Autonomy." [2020]
20. Christopher Kuner, "Data Nationalism and Its Discontents," Emory Law Journal 64 [2015]
21. Crutzen, Rik, Gjalt-Jorn Ygram Peters, and Christopher Mondschein. "Why and how we should care about the General Data Protection Regulation." Psychology & Health 34.11 [2019]
22. Dhont, Jan Xavier. "Schrems II. The EU adequacy regime in existential crisis?" Maastricht Journal of European and Comparative Law 26.5, [2019]
23. Doverspike, Robert D., K. K. Ramakrishnan, and Chris Chase. "Structural overview of ISP networks." Guide to Reliable Internet Services and Applications [2010]
24. Drechsler, Laura. "Comparing LED and GDPR adequacy: One standard two systems." Global Privacy Law Review 1.2 [2020]
25. Eger, John M. "Emerging restrictions on transnational data flows: privacy protection or non-tariff trade barriers." Law & Pol'y Int'l Bus. 10 [1978]
26. Fishman, William L. "Introduction to transborder data flows." Stan. J. Int'l L. 16 [1980]
27. Fraser, Erica. "Data Localisation and the Balkanisation of the Internet." SCRIPTed 13 [2016]

28. Greze, Benjamin. "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives." International Data Privacy Law 9.2 [2019]
29. Gruschka, Nils, et al. "Privacy issues and data protection in big data: a case study analysis under GDPR." 2018 IEEE International Conference on Big Data [Big Data]. IEEE, [2018]
30. Hahn, Isabel. "Purpose Limitation in the Time of Data Power: Is There a Way Forward?." Eur. Data Prot. L. Rev. 7 [2021]
31. Heck, Zachary S. "A Litigator's Primer on European Union and American Privacy Laws and Regulations", 44 LITIG.59, 59 [2018]
32. Herrera, Geoffrey L. "Cyberspace and sovereignty: thoughts on physical space and digital space." Power and security in the information age. Routledge, [2016]
33. Hill, Jonah Force "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," Lawfare Research Paper Series 2, no. 3 [2014]
34. Iqbal, Zafar, and Aasim Munir Dad. "Outsourcing: A review of trends, winners & losers and future directions." International Journal of Business and Social Science 4.8 [2013]
35. Jensen, Eric Talbot. "Cyber sovereignty: The way ahead." Tex. Int'l LJ 50 [2015]
36. Jiang, Chengze. "Research on Applying the WTO Security Exception Clause to the Security Dispute Caused by Cross-border Data Flows." 2021 International Conference on Social Development and Media Communication [SDMC 2021]. Atlantis Press, [2022]
37. Kalmanek, Charles R., Sudip Misra, and Yang Richard Yang, eds. "Guide to reliable internet services and applications". Springer Science & Business Media [2010]
38. Kuner, Christopher. "Reality and illusion in EU data transfer regulation post Schrems." German Law Journal 18.4 [2017]
39. Kunii, Tosiyasu L., "The 3rd industrial revolution through integrated intelligent processing systems" IEEE International Conference on Intelligent Processing Systems Vol.1, Cat. No. 97TH8335 [1997]
40. Malgieri, Gianclaudio. "The concept of fairness in the GDPR: a linguistic and contextual interpretation." Proceedings of the 2020 Conference on fairness, accountability, and transparency, [2020]
41. Kuner, Christopher. "Regulation of Transborder Data Flows Under Data Protection and Privacy Law." [2011]

42. Mattoo, Aaditya, and Joshua P. Meltzer. "International data flows and privacy: The conflict and its resolution." Journal of International Economic Law 21.4 [2018]
43. Mueller, Milton L. "Against sovereignty in cyberspace." International studies review 22.4 [2020]
44. Nicola, Fernanda G., and Oreste Pollicino. "The balkanization of data privacy regulation." W. Va. L. Rev. 123 [2020]
45. Novotny, Eric J. "Transborder Data Flow Regulation: Technical Issues of Legal Concern, 3 Computer LJ 105 [1981]." UIC John Marshall Journal of Information Technology & Privacy Law 3.1 [1981]
46. Osula, Anna-Maria. "Transborder access and territorial sovereignty." Computer law & Security review 31.6 [2015]
47. Panday, Jyoti, and Jeremy Malcolm. "The political economy of data localization." Partecipazione e conflitto 11.2 [2018]
48. Paull, Burness. "International Data Transfers: European Commission publishes final version of New Standard Contractual Clauses." [2021]
49. Pavlidis, George. "Financial information in the context of anti-money laundering: Broadening the access of law enforcement and facilitating information exchanges." Journal of Money Laundering Control 23.2 [2020]
50. Phillips, Mark. "International data-sharing norms: from the OECD to the General Data Protection Regulation [GDPR]." Human genetics 137 [2018]
51. Pine, John C. “Technology and Emergency Management”. John Wiley & Sons, [2017]
52. Popek, Gerald J., and Charles S. Kline. "Encryption and secure computer networks." ACM Computing Surveys [CSUR] 11.4 [1979]
53. Posner, Richard A. "Privacy, surveillance, and law." U. Chi. L. Rev. 75 [2008]
54. Reidenberg, Joel R. "The simplification of international data privacy rules." Fordham Int'l LJ 29 [2005]
55. Rotenberg, Marc. "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection." European Law Journal 26.1-2 [2020]
56. Schwartz, Paul M. "Global data privacy: The EU way." NYUL Rev. 94 [2019]
57. Schwartz, Paul M. "The EU-US privacy collision: a turn to institutions and procedures." Harv. L. Rev. 126 [2012]
58. Shanmugam, Divya, et al. "Learning to limit data collection via scaling laws: A computational interpretation for the legal principle of data minimization."

Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency. [2022]

59. Sharma, Ashlesh, et al. "On the rise and fall of ISPs." Proceedings of Netecon 9 [2009]
60. Shavitt, Yuval, and Udi Weinsberg. "Topological trends of Internet content providers." Proceedings of the Fourth Annual Workshop on Simplifying Complex Networks for Practitioners. [2012]
61. Shekhar, Raj, and Aman Yuvraj Choudhary. "Data Localisation and Cross-Border Flow of Data: Balancing the Incongruent Dimension of Barriers, Safeguards and" Free Flow of Data"." RGNUL Fin. & Mercantile L. Rev. [2022]
62. Solove, Daniel J., and Woodrow Hartzog. "The FTC and the new common law of privacy." Colum. L. Rev. 114 [2014]
63. Streinz, Thomas. "The evolution of European data law." The Evolution of EU Law,OUP, 3rd edn 2021 [2021]
64. Su, Yongtao, et al. "Broadband LEO satellite communications: Architectures and key technologies." IEEE Wireless Communications 26.2 [2019]
65. Tehrani, Pardis Moslemzadeh, Johan Shamsuddin Bin Hj Sabaruddin, and Dhiviya AP Ramanathan. "Cross border data transfer: Complexity of adequate protection and its exceptions." Computer law & security review 34.3 [2018]
66. Terpan, Fabien. "EU-US data transfer from safe harbour to privacy shield: back to square one?." European Papers-A Journal on Law and Integration 2018.3 [2019]
67. Terzis, Andreas, et al. "A two-tier resource management model for the Internet." Seamless Interconnection for Universal Services. Global Telecommunications Conference. GLOBECOM'99.[Cat. No. 99CH37042]. Vol. 3. IEEE, [1999]
68. Thobani, Shaira. "Processing personal data and the role of consent." Eur. J. Privacy L. & Tech. [2020]
69. Tracol, Xavier. "“Schrems II”: The return of the privacy shield." Computer Law & Security Review 39 [2020]
70. Tsaugourias, Nicholas. "Law, borders and the territorialisation of cyberspace." Indonesian J. Int'l L. 15 [2017]
71. Tzanou, Maria. "Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights." Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, Hart Publishing, Forthcoming [2020]

72. Ursic, Helena, et al. "Data localisation measures and their impacts on data science." Research Handbook in Data Science and Law. Edward Elgar Publishing [2018]
73. Vaida, Mircea-F., Ovidiu Buza, and Kalman Pusztai. "Streaming Audio-Video Content Over Internet with a Multimedia Presentation Generator." Web-Based Education: Proceedings of the Fourth IASTED International Conference, WBE-2005, [2005]
74. Valancius, Vytautas, et al. "How many tiers? pricing in the internet transit market." Proceedings of the ACM SIGCOMM 2011 Conference [2011];
75. von Solms, Suné, and Renier Van Heerden. "The consequences of Edward Snowden NSA related information disclosures." ICCWS 2015—The Proceedings of the 10th International Conference on Cyber Warfare and Security: ICCWS2015. [2015]
76. Walker, Stuart D., et al. "Data transmission." The Cable and Telecommunications Professionals' Reference. Routledge [2012]
77. Wang, Feng, and Lixin Gao. "Interdomain Routing and Reliability." Guide to Reliable Internet Services and Applications [2010]
78. Weber, Rolf H. "Transborder data transfers: concepts, regulatory approaches and new legislative initiatives." International Data Privacy Law 3.2 [2013]
79. Whalen v. Roe, 429 U.S. 589 [SCOTUS, 22 February 1977].
80. Winther, Mark. "Tier 1 isps: What they are and why they are important." IDC White Paper [2006]
81. Xiao, Yineng, and Yi Li. "On the importance of coordinated international rules in cross-border circulation of data." International Journal of Frontiers in Sociology 5.2 [2023]
82. Xu, Kuai, et al. "On properties of internet exchange points and their impact on as topology and relationship." International Conference on Research in Networking. Berlin, Heidelberg: Springer Berlin Heidelberg, [2004]
83. Zhang, Yan, et al. "On wide area network optimization." IEEE Communications surveys & tutorials 14.4 [2011]

TREATIES

84. Consolidated Version of the Treaty on European Union, OJ C115/13 [2008]
85. European Convention on Human Rights, 213 UNTS 222 [3 September 1953]

LEGAL ACTS

EU Regulations and Directives

86. General Data Protection Regulation, Regulation 2016/679, OJ L 119/1 [25 May 2018]
87. Law Enforcement Data Protection Directive, Directive [EU] 2016/680, OJ L 119/89 [27 April 2016]

Council of the European Union

88. Council Regulation [EC] No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data OJ L 8 [12 January 2001]

European Commission

89. European Commission "Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation [EU] 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework" [20 September 2023]
90. European Commission “Questions & Answers: EU – US Data Privacy Framework” [10 July, 2023]
91. European Commission, “Commission Implementing Decision [EU] 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation [EU] 2016/679 of the European Parliament and of the Council” [4 June 2021]
92. European Commission, “Commission Implementing Regulation [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” [28 June 2021]
93. European Commission, “Data Protection: European Commission adopts new Adequacy Decision for safe and trusted EU-US data flows” [10 July 2023]

European Parliament

94. European Parliament “Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework” 2023/2501[RSP] [11 May 2023]
95. European Parliament “Resolution of 3 February 2016 containing the European Parliament’s recommendations to the Commission on the negotiations for the Trade in Services Agreement [TiSA] [2015/2233[INI]]” Official Journal of the European Union, C 35/21 [31 January 2018]

European Data Protection Board

96. European Data Protection Board “Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework” 05/2023 [28 February 2023]
97. European Data Protection Board, "Information note on data transfers under the GDPR to the United States after the adoption of the Adequacy Decision on 10 July 2023" [July 2023]
98. European Data Protection Board, "Recommendations on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules [Art. 47 GDPR]" 1/2022 [20 June 2023]
99. European Data Protection Board, “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data” 01/2022 [18 June 2021]
100. European Data Protection Board. "Guidelines on the concepts of controller and processor in the GDPR - version for public consultation." 07/2020 [7 July 2021]
101. European Data Protection Board. "Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR" 05/2021 [14 February 2023]
102. European Data Protection Board. "Guidelines on the territorial scope of the GDPR [Article 3] - version for public consultation." 03/2018 [12 November 2019]

European Data Protection Supervisor

103. European Data Protection Supervisor, "EDPS investigation: European Commission's use of Microsoft 365." Case 2021-0518 [8 March 2024]

104. European Data Protection Supervisor, "European Commission's use of M365 infringes data protection rules for EU institutions and bodies." Press Release, EDPS/2024/05 [11 March 2024]

US Federal Regulations and Executive Orders

105. The Code of Federal Regulations, "Notice of Privacy Practices for Protected Health Information." [1938]

106. Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities, Order no. 14086, Federal Register [7 October 2022]

CASES

107. Comissão Nacional de Proteção de Dados, Deliberação 2021/533 [CJEU, 28 April 2021]

108. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18 [CJEU, 16 July 2020]

109. Jehovantodistajat v. Finland, Case C-25/17, [CJEU, 10 July 2018]

110. Lindqvist v. Åklagarkammaren i Jönköping Case C-101/01 [CJEU, 6 November 2003]

111. Maximillian Schrems v Data Protection Commissioner, Case C-362/14 [CJEU, 6 October 2015]

OTHER

112. Business Insider "PayPal is Shutting Down in Turkey", Insider Intelligence [1 June 2016], available at: https://www.businessinsider.com/paypal-is-shutting-down-in-turkey-2016-6

113. Cloudflare. "What is a WAN? Understanding Wide Area Networks." [2023], available at: www.cloudflare.com/en-gb/learning/network-layer/what-is-a-wan/

114. European Commission. "Adequacy Decisions.", available at : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

115. Hamm, Andrew, et al. “Data Protection Laws and Regulations USA 2023-2024” [7 July 2023], available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

116. International Association of Privacy Professionals, “US State Privacy Legislation Tracker”, [1 March 2024] available at; https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

117. U.S. Department of Commerce and the International Trade Administration “Participation Requirements Data Privacy Framework [DPF] Principles.” Data Privacy Framework Program [July 2023], available at: www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-[DPF]-Principles

118. Vurkır, Namık Berk. "Concerns over the new trends of censorship in Türkiye." Estonian Human Rights Centre [25 October 2022] available at: https://humanrights.ee/en/2022/10/censorshipturkey/

Non-exclusive licence to reproduce thesis and make thesis public

I, Namık Berk Vurkır,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

"Viability of Existing Methods for International Data Transfers between the EU and US"

supervised by Anna-Maria Osula,

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Namık Berk Vurkır
29.04.2024