Vilnius University Faculty of Law
Department of Private Law

Javahir Rzayeva
II study year, LL.M International and EU Law program

Master's Thesis

Standard Contractual Clauses as a GDPR safeguard: implementation and challenges

Standartinės sutartinės sąlygos kaip BDAR garantas: įgyvendinimas ir iššūkiai

Supervisor: lec.dr.Paulius Jurčys
Reviewer: assist. Justinas Drakšas

Vilnius
2024

ABSTRACT AND KEYWORDS

This work analyzes the challenges and legal intricacies of cross-border personal data transfers in the context of the European Union's General Data Protection Regulation. The study focuses on the GDPR's mechanisms for transferring personal data outside the EU, examining their purpose, effectiveness, and alignment with the EU's data protection standards. It also assesses the influence of key Court of Justice of the European Union decisions, particularly the Schrems I and II cases, on these transfer mechanisms. This analysis delves deeply into the role and impact of Standard Contractual Clauses as a pivotal tool within GDPR.

Keywords: personal data, General Data Protection Regulation, transfer of personal data, Schrems II, adequacy decisions, Standard Contractual Clauses

TABLE OF CONTENTS

INTRODUCTION

As technology rapidly advances, personal data has become both a valuable resource and a product. This shift underscores the growing necessity to balance technological progress with data protection. In our globally connected world, efficient and secure international data transfers are essential for corporate operations, innovation, and collaboration. But these transfers have difficulties, especially when it comes to protecting the privacy of personal data in the face of disparate international data protection regulations. The EU's General Data Protection Regulation (GDPR) plays a key role in ensuring that data transfers meet strict privacy standards. To address these challenges, legal frameworks like adequacy decisions and Standard Contractual Clauses have been established to ensure the safety and privacy of personal data during international transfers.

The *aim* of this research is to examine the difficulties and legal complexities associated with the transfer of personal data across borders, specifically under the framework of the GDPR. The study specifically examines the mechanisms of the GDPR that govern the transfer of personal data beyond the European Union. It analyses the purpose, efficacy, and alignment of these procedures with the data protection standards set by the EU. Focusing on the evolution of Standard Contractual Clauses (SCCs) following the Schrems II decision, the research aims to provide a detailed examination of the changes in implementation strategies adopted by organizations. This involves assessing legal and procedural adjustments made in response to the decision, with a special emphasis on how these changes align with GDPR requirements and address the concerns raised by the Schrems II ruling. The study also aims to fully comprehend and identify the remaining obstacles that organizations face when putting SCCs into practice after Schrems II. This entails exploring obstacles that are both legal and practical, such as particular compliance issues, data privacy concerns, and operational challenges that have arisen or become more intense in the context of the new legal environment. The main aspect of the work is to evaluate the effectiveness of the strategies currently employed by organizations for the implementation of SCCs. This evaluation seeks to determine whether these strategies are adequate and effective in addressing the legal complexities and practical challenges that have arisen post-Schrems II. Moreover, the study aims to contribute to the academic and legal discourse surrounding data protection, privacy laws, and transatlantic data flows. By providing a comprehensive analysis specific to the post-Schrems

II environment, the research seeks to be a valuable resource for scholars, legal experts, and practitioners in the field.

The research aims to achieve the following *objectives*: 1) examining post-Schrems II changes in SCC implementation 2) defining ongoing challenges in SCCs implementation 3) assessing the effectiveness of current implementation strategies 4) contributing to legal and academic discourse.

It would be appropriate to answer the following questions to determine the research *tasks*: 1) what changes can be identified in legal documents and corporate policies concerning SCCs after the Schrems II ruling? 2) what are the current difficulties and obstacles that organizations face in implementing SCCs? 3) do these strategies successfully address the identified challenges and complexities in SCCs implementation? 4) what insights can be provided for stakeholders through this work?

The *relevance* of the research: Personal data exchange is considered a crucial and essential aspect of global commerce in the present era. The rulings made by the Court of Justice of the European Union in cases pertaining to this matter have a significant impact on shaping the future of data transfers. The legislative framework pertaining to data protection and privacy is undergoing rapid evolution. The GDPR, which is considered one of the most stringent data protection legislations worldwide, has a profound influence on the way organizations handle personal data. At a time when data privacy is a major concern globally, this work contributes to understanding how personal data can be protected during international transfers. The GDPR's extraterritorial application adds to the difficulties, particularly for non-EU nations, and raises the possibility of disputes over data protection laws and jurisdiction (Taylor, 2020). The rapid progression of technology, namely cloud computing and big data analytics, has led to an increase in both the quantity and intricacy of cross-border data transmissions. In accordance with the GDPR, Standard Contractual Clauses are a crucial safeguard for international data transfers. Contractual obligations exist between importers and exporters of data, mandating the safeguarding of personal information during its transmission beyond the European Union. In the post-Schrems II decision, which introduced new SCCs to resolve the complexities of global data transfers, the significance of SCCs was emphasized. Importantly, the new SCCs address the deficiencies in its previous version and reflect the GDPR's data transfer requirements as well as some Schrems II related developments. They also provide more legal predictability to EU businesses and offer more flexibility for

complex data processing chains. The purpose of these clauses is to ensure legal certainty and adherence to GDPR principles, particularly in situations involving the transmission of data to countries lacking a European Commission adequacy decision.

Many *research methods* apply to the work: 1) comparative legal analysis: this comparison will highlight the similarities and differences in legal frameworks and how personal data transfers are managed and regulated 2) case law analysis: the method will focus on examining case law, particularly the CJEU's decisions to understand how the concept of 'transfer to third countries' has been interpreted and applied in legal proceedings 3) interpretative legal analysis: this method will be employed to interpret multiple provisions of the GDPR and other related legal texts.

Originality of the research:

The rapid evolution of digital technology, as well as the rising complexity of data privacy legislation, particularly in the context of GDPR, emphasize the importance of a comprehensive understanding of cross-border personal data transfers. The author's research in this arena provides a detailed study that not only exposes the complexities and issues inherent in GDPR compliance for personal data transfers, but also provides strategic insights and solutions to these challenges. Furthermore, the work distinguishes itself by forecasting future technology breakthroughs and their potential impact on data protection and transmission strategies. The combination of these components emphasizes the research's novelty, giving a forward-thinking, in-depth analysis of GDPR implementation in the global digital ecosystem.

Main sources

To achieve the outlined objectives, the author utilizes legal regulations and international guidelines. These guidelines, being exemplary in nature, could potentially serve as a model for future internationally acknowledged documents. These include the following documents: General Data Protection Regulation 2018; EDPB’s Recommendations 2020; Shrems I and II Decisions. Additionally, to deeply research the topic and come to certain conclusions, the author considers the materials of the following primary authors: Christopher Kuner, Philip Gordon, Marcelo Corrales Compagnucci, Philip Lee, Christopher Docksey.

PART I. GENERAL ASPECTS CONCERNING THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

1.1 Chapter I Concept of Transfer to Third Countries

The concept of transferring personal data to third countries is a critical aspect that plays a central role in the global landscape of data privacy and protection laws. The concept of "transfer of personal data to third countries or an international organization" is not defined in the General Data Protection Regulation (Union, 2016) and Directive 95/46 (Council, 1995). Explaining the concept is necessary to determine whether data processing carried out by a data controller or data processor in the European Union constitutes a transfer to a third country or an international organization, and thus whether the data controller and the data processor need to comply with the provisions of Chapter 5 of the GDPR (EDPB, 2021). In addition, the Lindqvist case (Case C-101/01, Bodil Lindqvist, 2003), which is the only case law in which the Court of Justice of the European Union discussed the concept of "transfer to third countries" and the first case law in which it addressed this issue, has a limited scope in defining the concept of transfer to third countries (Bulck, 2017).

In the Lindqvist case, the CJEU analyzed whether uploading personal data to a website, as done by Bodil Lindqvist, constitutes a 'transfer' under Article 25 of Directive 95/46 (EU, 1995), which deals with data protection. The CJEU clarified that sharing data on a website stored on an EU server and accessible worldwide does not amount to a transfer to a non-EU country under this directive. They clarified that simply making data accessible online, including to users in non-EU countries, does not amount to a transfer. A transfer requires actively sending data, and users must take active steps to access this information. The CJEU emphasized that its conclusion was based on the specific circumstances of this case and may not automatically apply to different situations involving international data transfers.

In a 2014 position paper, the European Data Protection Supervisor highlighted key aspects of personal data transfer. The EDPS defined personal data transfer as 'the transmission, disclosure, or other making available of personal data, carried out with the knowledge or intention that recipients will have access to it' (EDPS, 2014). The definition includes intentional transfers and

instances where data access is permitted, such as when recipients access the data. Examples of international personal data transfers, as cited by the EDPS, include:

- Sending data by post or email from an EU data controller to a recipient outside the EU
- Publishing personal data on the internet by the data controller
- Transmitting data from the data controller’s database to a recipient outside the EU
- Granting access to a database by an EU data controller to a recipient outside the EU (EDPS, 2014)

The European Data Protection Board's 2021 recommendation report further clarified that storing personal data in non-EU clouds or allowing remote access from third countries is considered a transfer (EDPB, 2021). These transfers must comply with Chapter 5 of the GDPR (Union, 2018). The GDPR defines transfer as 'dissemination or making available' and 'disclosure by transmission.' Additionally, these transfers, which also constitute processing activities as defined in Article 4(2) of the GDPR (Union, 2018), must adhere to all relevant GDPR provisions. It's important to distinguish between 'transfer' and 'transit transfer' (Office, 2021). The latter, involving data moving from one EU country to another via a third country, is not considered an international transfer. A significant development was the EDPB's Directive of November 18, 2021, which outlined criteria for determining when a processing activity constitutes a transfer. This means that if all the criteria set by the EDPB are not met, there will be no reference to a transfer for the data controller or data processor, and the provisions contained in Chapter 5 of the GDPR (Union, 2018) will not apply.

1.2 Chapter II General Principles on Transfer of Personal Data

EU law facilitates the free movement of personal data among member states. Article 1(3) of the GDPR (Union, 2018) prohibits the restriction or prohibition of this free movement for reasons related to the protection of natural persons in the context of personal data processing. This provision also extends to Iceland, Norway, and Liechtenstein, which are part of the European Economic Area and have adopted EU law, including GDPR, under the EEA Agreement (Europe, 2018, p. 252). This inclusion expands the application area of EU data protection principles to these countries. In July 2018, the EEA Joint Committee amended it to incorporate the GDPR in its

annexes and decided on the implementation of the GDPR (Committe, 2018). It's important to note that the free movement of personal data within the EEA for purposes related to preventing, investigating, detecting, and prosecuting criminal offenses falls not under the GDPR but under Directive 2016/680 (Union, 2016). Chapter 5 of the GDPR specifically covers Articles 44 to 49, which address the transfer of personal data from the EU to third countries or international organizations (Union, 2018).

In Article 44 of the GDPR (Union, 2018), which regulates the general principles regarding transfers, a two-stage approach has been adopted to transfer personal data to third countries where it will be processed or is intended to be processed. According to this approach, to transfer personal data outside the EU without compromising the level of protection provided by the GDPR to natural persons, the transfer must comply with the provisions of both Chapter 5 and all other provisions of the GDPR. GDPR Recital 101 (EU, 2018) further elaborates on the 'General Transfer Principles' of Article 44. As highlighted in Recital 6 (EU, 2018), transferring personal data to countries and international organizations outside the European Union is crucial for developing international trade and cooperation. However, this increase in data transfers also raises concerns about personal data protection. Therefore, Recital 101 stipulates that transferring personal data to data controllers, processors, or other recipients in a third country, including onward transfers, must not diminish the level of protection for individuals within the EU. This stipulation is interpreted to mean that transfers to third countries should not circumvent the protections afforded by the EU Data Protection Law, particularly the GDPR. This requirement aligns with the fundamental right to personal data protection guaranteed by the Charter of Fundamental Rights (Commission, 2000) for individuals in the EU. Because of this, transfers that follow GDPR Chapter 5 but don't provide the necessary level of protection for natural persons as required by other GDPR provisions or the Charter are not allowed.

Chapter 5 of the GDPR outlines 'a three-layer structure' for the lawful transfer of personal data to third countries or international organizations, presenting a hierarchical structure: adequacy decisions at the top, appropriate safeguards in the middle, and exceptions at the bottom. Each mechanism in this hierarchy provides a different level of data protection. An adequacy decision, representing the highest level of protection, requires that the legal system of a third country or international organization be 'essentially equivalent' (CJEU, 2015) to EU Data Protection Law standards, which are considered the highest. If an adequacy decision is not available, organizations

can utilize appropriate safeguards. The CJEU's decision in Schrems II (CJEU, 2020) clarified that these safeguards should offer a level of data protection 'substantially equivalent' to that provided by an adequacy decision. Lastly, exceptions are applicable in specific situations where neither an adequacy decision nor appropriate safeguards are feasible.

PART II. Mechanisms for the Transfer of Personal Data

2.1 Chapter I Transfers Based on Adequacy Decisions

The first consideration under the GDPR when transferring personal data to a third country or international organization is whether the European Commission has assessed the data protection level of the third country outside the EU and determined if it provides sufficient protection compared to the European legal regime. Whether there is an adequacy decision depends on whether there will be an adequacy decision means that the Commission has decided that a third country or an international organization provides an “adequate level of data protection”. Article 45 of the GDPR (Union, 2018) provides that, where the European Commission has determined that a third country (including regions or one or more specific sectors within those countries) or an international organization provides an adequate level of protection, personal data may be transferred to that country or international organization (Commission, no date). The Commission can make adequacy decisions for any country that is not a party to the EU. Unlike Directive 95/46, the GDPR grants the Commission exclusive authority to make adequacy decisions for transferring personal data to jurisdictions outside the EU. Adequacy decisions are legally binding for all EU member states and allow the transfer of personal data to a third country or international organization determined by the Commission as "adequate" through this decision, without the need for further approval. Thanks to adequacy decisions, the transfer of personal data to third countries or international organizations without the need for any additional permission or assurance reveals the impact and importance of the decision. With these adequacy decisions taken by the Commission, a "whitelist" has been created in order to transfer personal data without any restrictions or limitations (Dhawan, 2023).

The CJEU, in its Schrems I decision, defined the adequate level of protection as "essentially equivalent" to the level of protection guaranteed by law in the EU, provided by a third country for

fundamental rights and freedoms (CJEU, 2018). The methods used by a third country to ensure an adequate level of protection may differ from those of the EU, but the methods used are not necessarily the same. The concept of adequacy not only requires that the content of data protection rules in third countries or international organizations comply with EU law standards, but also requires that the rules in question be effective in practice (Kuner, 2020). The aim here is to be able to establish the basic requirements of EU legislation regarding data transfers to third countries (Commission, 2017). The adequacy decision can be made in two ways: a full adequacy decision and a partial adequacy decision. A full adequacy decision is the Commission's decision that a third country fully provides adequate protection. Under this decision, transfers to countries deemed fully adequate are treated as transfers to EU countries. A full adequacy decision means that personal data is transferred from the EU to a third country (INSTITUTE, 2020). It ensures that the transfer can be made without the need for any other protection measures, as if it were made within the EU. The Commission recently gave the most recent adequacy decision in this way for the Republic of Korea (Commission, 2021). In the partial adequacy decision, the Commission makes the decision that only a certain sector, region, or international organization in the third country provides adequate protection. For example, the Commission gives a partial adequacy decision to Canada because it applies specifically to commercial organizations (Decision, 2001). In addition, the adequacy decisions taken within the scope of the Safe Harbor and Privacy Shield Agreements, which were prepared for the transfer of personal data from the EU to the US to support transatlantic trade and which the Commission found sufficient to ensure data transfers, are also considered partial adequacy decisions (Kuner, 2020).

GDPR, unlike Directive 95/46, allows the European Commission to make partial adequacy decisions regarding whether a particular region or sector in a third country provides an adequate level of protection, thus expanding the Commission's authority regarding adequacy decisions. However, making such a decision becomes challenging in cases where sectoral boundaries cannot be clearly drawn and the players in the sector are interconnected, such as the health sector. There are 15 (fifteen) adequacy decisions issued by the Commission and currently in force (Commission, 2021). The Commission has so far implemented GDPR Article 45(3) in Andorra, Argentina, the United Kingdom, Canada (commercial organizations), the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan, and most recently, the Republic of Korea. It has been accepted that sufficient protection is provided for personal data transferred

to these countries with the appropriate decisions taken for The CJEU invalidated three previously valid adequacy decisions, rendering them not in force. The adequacy decisions in question were invalidated by the CJEU in its 2006 decision (CJEU, 2006) on the transfer of passenger name record ("PNR") data to the US Customs and Border Protection Bureau and the EU-US Safe Harbor, which it invalidated in its Schrems I decision. The Schrems II decision of 2020 invalidated the adequacy decisions taken within the scope of the EU-US Privacy Shield Agreements (Kuner, 2020). These adequacy decisions do not cover data transfers governed by Directive 2016/680.

The United Kingdom wanted to leave the EU (Brexit) by applying to Article 50 of the Treaty on European Union, and as a result, it left the EU on December 31, 2020. With the departure of the UK from the EU, the UK has become a third country for the EU in personal data transfers from the EU to the United Kingdom. In view of this situation, a Guide has been issued by the EDPB and the UK Information Commissioner's Officer ('ICO') to facilitate the transfer of personal data from the EU to the United Kingdom after Brexit and to address the uncertainties concerning the transfers, and an adequacy decision has been taken for the UK under Article 45 of the GDPR (ICO, 2020). On February 19, 2021, the European Commission published two draft adequacy decisions in accordance with the GDPR and Directive No. 2016/680, stating that personal data transferred to the UK are adequately protected, thereby initiating the procedure for accepting the adequacy decision for the UK (Commission, 2021). The European Commission initiated the procedure for accepting an adequacy decision for the transfer of personal data to the Republic of Korea within the scope of the GDPR with the publication of the draft decision on June 14, 2021. In this context, the adequacy decision regarding personal data transfers from the EU to the Republic of Korea was approved by the Commission on December 17, 2021 (Commission, 2021).

Article 45(2) of the GDPR (EU, 2018) outlines the criteria that the European Commission must consider when assessing the adequacy of data protection in a third country or international organization. However, the evaluation extends beyond these criteria, but they are still highlighted as significant considerations. The criteria include the third country's legislation, respect for human rights and fundamental freedoms, data protection rules, independent supervisory authority, and the existence of a data protection body. The evaluation must also consider the third country's access to personal data by public authorities for law enforcement, public interest, or national security purposes. The Commission must also consider the third country's international commitments and

participation in multilateral or regional systems for data protection. The Commission's assessment will determine if the third country provides a level of protection substantially equivalent to that in the EU. An adequacy decision is binding for all EU countries and allows for the transfer of personal data without additional permissions or security measures. The Commission must consider all conditions that may affect the transfer of personal data when making the adequacy decision. In 1998, Working Party (WP29) (Commission, 1998)established basic principles for third countries to comply with for their protection to be considered adequate. These principles include purpose limitation, data quality and proportionality, security, transparency, right of access, rectification and objection, and restrictions on onward transfers. The Commission considers these principles as a starting point for making an adequacy decision. WP29 has also provided guidance on the qualification criteria in the GDPR, including content-related principles such as basic data protection and fair processing. However, these documents are not legally binding.

2.2 Chapter II Safe Harbor and Schrems I Decision

The EU and the US have different approaches to the protection of personal data. The EU approaches the issue of privacy and personal data protection within the framework of fundamental rights. Although the US Supreme Court has interpreted the Constitution to provide individuals with the right to privacy, this right generally provides protection against government intrusion (Service, 2021). In contrast to the EU, where the Charter guarantees the right to protection of personal data as the primary law, the US lacks comprehensive federal regulation of consumers' personal data processing (Service, 2021). Following the adoption of Directive 95/46 on data protection in the EU in 1995, these differences raised concerns that many businesses and industries would face adverse effects on the transfer of personal data between the EU and the US. As a result of the negotiations held to prevent this negative situation, the United States Department of Commerce (DOC) and the European Commission decided that US companies should comply with the "sufficient data" required for the transfer of personal data from the EU to a third country. agreed on a system that would enable it to meet the “level of protection” requirement. In this context, the European Commission published its Safe Harbor Privacy Principles decision in 2000, which determined that personal data transfers from the EU to the US provide adequate protection in accordance with Article 25 of Directive 95/46. However, the European Commission's decision also

stated that the Safe Harbor Principles could be limited to the extent necessary in cases of public interest, national security, or law enforcement (Commission, 2000). Safe Harbor, which consists of principles based on the EU Data Protection Law, was a self-regulatory mechanism that companies headquartered in the US committed to comply with to ensure the protection of personal data transferred from the EU to the US (Kuner, 2017). The Commission accepted that US companies complying with these principles met the EU's requirements for transferring personal data from the EU. For a company to be included in Safe Harbor, it had to fall under the jurisdiction of the Federal Trade Commission (FTC) and the United States Department of Transportation (DOT). To qualify, companies had to self-certify that they complied with Safe Harbor privacy principles and requirements by submitting a letter to the DOC each year. Additionally, the FTC promised to review notifications of any violations by EU member state authorities. The FTC and DOT regulated Safe Harbor.

After 15 years of use, the Safe Harbor was invalidated by the CJEU's "Schrems I" decision dated October 6, 2015. The CJEU's "Schrems I" decision has been a landmark decision regarding data transfer under the EU Data Protection Law (Kuner, 2017). The case started with the complaint made by Maximillian Schrems, an Austrian citizen, to the Irish national supervisory authority on June 25, 2013. Schrems, a Facebook user, alleged that, based on Snowden's revelations about US surveillance activities, some or all his personal data stored on Facebook was transferred by Facebook from EU-based servers in Ireland to servers in the US and that the US National Security Agency ('NSA') claimed to have access to this data. Schrems claimed that the US did not have adequate protection under data protection law and intelligence surveillance practices and called for the Irish national supervisory authority to review whether the Safe Harbor principles provide adequate protection for personal data transferred to the US and to order Facebook to stop data transfers to the US. He claimed that he should have given instructions. The Irish national supervisory authority stated that Facebook adhered to Safe Harbor and that the supervisory authority could not question whether the adequacy decision taken by the European Commission within the scope of the Safe Harbor Privacy Principles established in accordance with Article 25(6) of Directive 95/46 provided "adequate protection" (COUNCIL, 1995). It refused to act against the case and Facebook on the grounds that it had no basis to consider the complaint. Against the rejection decision of the Irish national supervisory authority, Schrems took the case to the Irish

Supreme Court. The Supreme Court of Ireland referred the case to the CJEU for a preliminary decision on June 18, 2014.

The importance of the CJEU's Schrems I decision, given on October 6, 2015, is based on four main issues it focuses on (Kuner, 2017). In its decision, the CJEU first confirmed that the right to protection of personal data is one of the fundamental rights under EU law, and within the framework of the importance given to fundamental rights in EU law, the European Commission, when evaluating the adequacy of data protection in third countries, fulfils the requirements arising from Article 25 of Directive 95/46 within the scope of the Charter. He emphasized that the qualification evaluation should be "rigid" based on this reading (Schrems I, para 78., 2015).

The second issue addressed by the CJEU in its Schrems I decision is the indirect application of EU law to data processing activities taking place in third countries through data transfer mechanisms. The CJEU stated that EU Law is not directly applicable in third countries, but the transfer of personal data from a member state to a third country based on the provision of Directive 95/46 Art. 2(b) constitutes a data processing activity; therefore, EU Law is valid in terms of data transfers within the scope of Safe Harbor.

The third issue that the CJEU focused on in its decision was the strengthening of the role of national supervisory authorities (Kuner, 2017). According to the decision, the Commission's adequacy decision for the transfer of data to third countries shall not reduce or impede the powers of national supervisory authorities conferred by the Charter and Directive 95/46 (Schrems I, para 53-58., 2015). In this context, even if there is an adequacy decision accepted by the Commission, national supervisory authorities must examine, with full independence (Schrems I, para 40-41., 2015) and "all due diligence", the claims of individuals regarding the adequacy of protection in third countries and the protection of their fundamental rights and freedoms in transfers made based on an adequacy decision (Schrems I, para 63., 2015). It is ultimately up to the CJEU to decide whether a Commission decision is valid or not (Schrems I, para 61, 2015). Within the scope of the study, it is important to discuss the definition of the "adequate level of data protection" required for data transfer to third countries, which was addressed by the CJEU in its decision on the Schrems I case (Kuner, 2017). The protection defined by the CJEU as an adequate level of data protection in the decision in question is a high level of protection determined in the light of the Charter, and this protection is not the same as the protection under EU Law but is a "essentially equivalent" protection (Schrems I, para 73, 2015). The CJEU has also raised the bar on global data protection

by defining the adequate data protection standard that a third country must meet for data transfer outside the EU as a high-level data protection standard (Kuner, 2017).

In its Schrems I decision, the CJEU stated that the Commission should examine the local laws or international commitments of the third country when making an adequacy decision within the scope of the transfer of data in accordance with Directive 95/46 Art. and determined that it was not included. In addition, the CJEU held that US national security, public interest and law enforcement requirements take precedence over the Safe Harbor principles, and that US companies are obliged to disregard the protective principles established by the Safe Harbor, without limitation, in the event of a conflict between these requirements. The CJEU concluded that US authorities can interfere with the fundamental rights of individuals whose personal data has been or may be transferred from the EU to the US under the Safe Harbor principles. Furthermore, the CJEU noted that while the Commission found that the Safe Harbor principles provided adequate data protection, it did not consider whether rules to limit such interference or effective legal protection against interference existed (Schrems I, para 86-87., 2015).

For all these reasons, the CJEU deemed the Safe Harbor Privacy Principles invalid. Although Standard Contractual Clauses and Binding Corporate Rules (BCR) can be used for data transfer between the EU and the US after the decision, the adequacy decision taken under Safe Harbor is no longer a legal basis for transfers. In December 2016, the Commission adopted a decision amending the eleven adequacy decisions then in force to consider the requirements of the Schrems I decision, covering Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay (Commission, 2000-2013). After the CJEU invalidated Safe Harbor with its Schrems I decision, approximately four thousand five hundred) US companies participating in Safe Harbor were concerned that this decision would have negative effects on trade relations between the EU and the US. However, the decision came into effect after a four-month transition period, and the Privacy Shield Agreement came into force in July 2016 because of negotiations between EU and US officials.

2.3 Chapter III Privacy Shield and Schrems II Decision

When Safe Harbor came into force in 2000, the processing of data, including the transfer of personal data, was much more limited than it is today. Negotiations between the EU and the US

to make Safe Harbor more secure started in 2013 with the disclosure of US surveillance practices, and these negotiations gained momentum and importance with the CJEU's Schrems I decision (Commission, 2013). Furthermore, the negotiations for the new agreement considered the changes and innovations envisaged by the GDPR, which had not yet come into force at that time (Service, 2021, p. 8). Following the invalidation of Safe Harbor by the CJEU's Schrems I decision of October 6, 2015, the Commission and DOC agreed on the Privacy Shield system, a valid mechanism for the transfer of personal data from the EU to the US for commercial purposes. It was published by the Commission on July 12, 2016, in a formal decision that the Privacy Shield Agreement provides an adequate level of protection. The Privacy Shield was accepted by all EU members and came into force on August 1, 2016. To transfer data from the EU to the US, the US company had to voluntarily comply with the Privacy Shield principles and obtain certification from DOC.

The Privacy Shield Agreement was invalidated by the CJEU's decision called "Schrems II" on July 16, 2020. Although the Privacy Shield Agreement was designed to provide greater data security after Safe Harbor, to which it was the successor, was invalidated, it remained in force for only a short period of 4 years. While the Privacy Shield Agreement included the seven basic privacy principles included in Safe Harbor, to which it was the successor, it also included the concerns stated by the CJEU in its Schrems I decision. US officials provided written commitments and assurances that they would limit access to personal data, and a compensation mechanism, including the Privacy Shield Ombudsman, addressed complaints about potential access to personal data by US national security authorities. As an indication of this, in February 2016, the US Congress passed the US Judicial Redress Act, which extends certain judicial redress provisions in the US Privacy Act of 1974 to EU citizens. The EU and US sides stated that, compared to Safe Harbor, the Privacy Shield includes significantly stronger privacy protections, oversight mechanisms, compensation rights, and new safeguards regarding US authorities access to personal data (Service, 2021, p. 10). Individuals who believe that their personal data has been seized by the US authorities can file a complaint directly with the US companies or with the EU national supervisory authorities, who will then forward it to the FTC. At the starting point of the Privacy Shield is the provision of new security measures to the relevant persons, including the right to appeal to the US courts in cases where the US authorities believe that the US authorities have unauthorized access to or misuse of their personal data, providing the relevant individuals with more control over how their information is processed, and the US authorities providing sufficient

cause. The aim was to make a commitment that they would not be able to access the data without it. However, the CJEU ultimately invalidated the Privacy Shield Agreement with the Schrems II decision, concluding that it did not achieve these objectives in practice (Gungor, 2020). The CJEU invalidated the Privacy Shield Agreement on the grounds that the US public authorities unauthorized access to and use of personal data transferred from the EU, based on the country's domestic law, did not comply with the EU's high standards of data protection and was not proportionate.

After the Schrems I decision, Maximilian Schrems lodged a further complaint with the Irish national supervisory authority regarding Facebook's use of Standard Contractual Clauses for data transfers from the EU to the US. According to the complaint, Facebook's obligation to make its users' personal data accessible to US government authorities under US surveillance programs rendered Standard Contractual Clauses an invalid legal basis for transferring personal data to the United States. The Irish national supervisory authority referred the case to the Irish Supreme Court after investigating the allegations and finding that the CJEU could not rule on the issue until it had examined whether the Standard Contractual Clauses were valid. The complaint also raised questions about the level of protection offered by the Privacy Shield, which the Commission had deemed to be sufficient, for Facebook's data transfers to the US. The Supreme Court of Ireland stayed the proceedings in 2018 and forwarded several questions to the CJEU regarding the validity of Standard Contractual Clauses (Court, 2018). In his opinion (Kuner, 2021), the Attorney General examined the questions submitted to the CJEU under both the Directive and the GDPR, which had come into full force at that time. The Attorney General approved the Standard Contractual Clauses and found that it was not necessary for the CJEU to examine the validity of the Privacy Shield, although he had doubts that it provided adequate protection (Case C-311/18, "Opinion of Advocate General Saugmandsgaard" para 342, 2021). The questions referred to the CJEU by the Irish Supreme Court are summarized under five headings in the Court's Schrems II decision, and these are whether the GDPR applies to transfers between economic operators (Case C-311/18, Schrems II, para. 80., 2020) in the event that personal data is processed in a third country for the purposes of law enforcement and public security, whether the GDPR applies to transfers between economic operators, the standard what the level of protection is under the contractual clauses; whether national supervisory authorities are required to suspend or prohibit transfers under Standard Contractual Clauses if the relevant clauses are not complied with or an adequate level of protection

cannot be ensured; whether Standard Contractual Clauses apply under the Charter and whether the Privacy Shield Agreement provides an adequate level of protection (Case C-311/18, Schrems II, para. 90, 2020) under the GDPR. According to the CJEU's decision, the Privacy Shield is not an adequate mechanism for the transfer of personal data from the EU to the US. The CJEU overruled the Commission's decision that it provided an adequate level of protection for data transferred under the Privacy Shield, considering the breadth of the US's data collection powers based on US surveillance laws and the lack of a compensation mechanism for data subjects in the EU (Case C-311/18, Schrems II, para. 160, 2020). According to the CJEU, Section 702 of the US Foreign Intelligence Surveillance Act (FISA 702) allows US intelligence agencies to collect more information about non-US citizens than is strictly necessary. The CJEU addressed the independence of the Privacy Shield Ombudsman system and ruled that the system in question could not provide adequate compensation because it was not clear whether the Ombudsman had the authority to make a binding decision on US intelligence agencies. The CJEU invalidated the Privacy Shield Agreement based on four main reasons. These reasons are that US law takes precedence over Privacy Shield requirements, that there are no necessary limitations and safeguards regarding the powers of authorities under US law, especially within the scope of proportionality requirements (Case C-311/18, Schrems II, para. 164, 2020), that there is no effective legal remedy in the US for data subjects in the EU (Case C-311/18, Schrems II, para. 168-185., 2020), and that Privacy Shield does not have the CJEU evaluated these issues within the framework of Articles 7, 8, and 47 of the Charter and, together with these deficiencies, invalidated the Privacy Shield Agreement to enter into force upon the issuance of the decision (Case C-311/18, Schrems II, para. 201-202, 2020).

The primary importance of the Schrems II decision for adequacy decisions under GDPR Art. 45 is that it reinforces the conclusions reached in the Schrems I decision regarding the high standard of protection required for an adequacy decision to be made and the fact that the standard in question must be read considering the Charter (Christhoper K., 2021). The Irish Supreme Court also referred to detailed testimony from US experts on secrecy and intelligence collection (Case C-311/18, “Opinion of Advocate General Saugmandsgaard”, para. 342., 2020). The Irish Supreme Court also considered detailed testimony from US experts on secrecy and intelligence collection, reinforcing the high standard that the CJEU seeks in data transfers to third countries, particularly the US (Christhoper K., 2021). The CJEU ruled in its Schrems II decision that Article 44 should

guarantee the level of protection regardless of Article 5 of the GDPR, which is based on transferring personal data to a third country (Case C-311/18, Schrems II, para. 92 and 105., 2020). This is to prevent violations of EU law and ensure that the level of protection for natural persons, as guaranteed by Article 44 of the GDPR, is not compromised (Case C-362/14, Schrems I, para. 73., 2015).

Following the CJEU's Schrems II decision, the EDPB published recommendations that provide guidance on the use of Standard Contractual Clauses, outlining additional measures that data exporters and data transferees can take to ensure that they meet EU data protection requirements. Additionally, the Commission has published new Standard Contractual Clauses containing the requirements of the GDPR and the Schrems II decision. Despite these developments on the EU side, the US has published a white paper to assist companies in assessing whether their transfers comply with the CJEU decision for data protection. In the document, it is stated that most US companies are not interested in data that concerns US intelligence agencies and that the companies are not engaged in data transfers that concern the CJEU and involve risks to privacy identified in Schrems II. In its decision, the CJEU also found that the United States did not have an adequate compensation mechanism for European citizens whose data could be subject to US surveillance (Service, 2021, p. 14). Under the principle of compensation, European citizens should be able to find out whether US agencies, such as the NSA, collect or process their data in violation of the principles of necessity and proportionality and be able to take legal action in US courts. Schrems II therefore requires significant changes to US surveillance law as well as the establishment of a new compensation mechanism.

The Court of Justice of the European Union's decision in Case C-311/18 (CJEU, 2018), commonly referred to as the "Schrems II" case, revolves around the transfer of personal data from the EU to the United States. Maximillian Schrems, an Austrian privacy activist, lodged a complaint against Facebook Ireland for transferring his personal data to the US, where he believed it was not adequately protected from US government surveillance, giving the case its name. The Court interpreted several EU legal texts as Directive 95/46 on data protection, particularly the clauses related to the transfer of data to third countries, the validity of the Standard Contractual Clauses Decision 2010/87/EU, which many companies use to transfer personal data outside the EU, the EU-US Privacy Shield Decision 2016/1250, which was a mechanism used to facilitate data transfers between the EU and the US,

The Court's decision invalidated the EU-US Privacy Shield on the grounds that it did not provide EU citizens with a level of data protection equivalent to that guaranteed within the EU, especially in light of the potential access to personal data by US authorities. The Court highlighted the lack of adequate legal remedies available to EU citizens to challenge US surveillance programs. Furthermore, the Court emphasized that data exporters and importers must assess whether the data protection provided in the recipient country is adequate on a case-by-case basis. Data exporters and importers must implement additional safeguards or suspend data transfers if the protection is not equivalent to EU standards.

The ruling has significant implications for transatlantic data flows, affecting many businesses that relied on these mechanisms to transfer data legally from the EU to the US. Companies must now reassess their data transfer arrangements and consider alternative mechanisms or additional safeguards to ensure compliance with EU data protection laws.

The decision underscores the EU's commitment to upholding high standards of data protection and the fundamental rights of its citizens, even when facing international data transfer challenges. The decision has prompted discussions on the need for new frameworks and agreements between the EU and third countries, particularly the US, to ensure that personal data receives protection consistent with EU law.

PART III. Assessment and Modification of Standard Contractual Clauses Post-Schrems II

3.1 Chapter I The Effect of the Schrems II Decision on Standard Contractual Clauses

When Directive 95/46 came into force, it was thought that most countries would not benefit from the adequacy decision, which opened the possibility of transfers of personal data outside the EU using what are known as appropriate safeguards. Appropriate safeguards are methods by which companies make legally binding commitments to ensure an adequate level of protection over personal data, supported by legal solutions for both data subjects and national supervisory authorities. The appropriate safeguards contained in the GDPR are based on and extend the provisions of Article 26 of Directive 95/46 (Kuner, 2020). If there isn't an adequacy decision, Article 46(1), and Recital 108 of the GDPR say that the controller and the processor must put in place adequate safeguards to make up for any weaknesses in the protection of personal data in

third countries (EDPB, 2020, p. 8). In this context, provided that appropriate safeguards are provided and other relevant provisions in the GDPR are complied with, personal data can be transferred to third countries and international organizations using the transfer tools specified in GDPR Article 46(2) (EDPB, 2020, p. 7). These appropriate safeguards aim to protect the fundamental rights and freedoms of the data subject regarding personal data held by the data controller and data processor. These transfer methods are often called alternative transfer tools or mechanisms. GDPR Chapter 5 mandates that transfers should be based on adequacy decisions, and in cases where there is no adequacy decision, appropriate safeguards must be used as an alternative. For the appropriate safeguards in GDPR Art. 46(2), unlike the Directive, there is no need to obtain special permission from a supervisory authority, but supervisory authority approval is required for Binding Corporate Rules (BCR), codes of conduct, and certification mechanisms. However, the data exporter can use these methods under their responsibility after obtaining approval. According to Article 46(3) of the GDPR, ad hoc contractual clauses and administrative arrangements between public authorities or bodies require permission from the national supervisory authority. When making an adequacy decision under Article 45(2) of the GDPR, specific data protection risks that must be considered cannot be protected against by appropriate safeguards, which only protect certain types of transmission or transfers (Kuner, 2020). In evaluating the adequacy of the decision, the legal system of the third country or international organization to which the data will be transferred is considered (Kuner, 2020). However, in transfers based on appropriate safeguards, the existence of valid protection for the data transferred in a third country or international organization is required. Appropriate safeguards consist of eight main methods regulated in GDPR Art. 46 and Art. 47. Legally binding and enforceable documents between public authorities or bodies not included in Directive 95/46, approved codes of conduct, approved certification mechanisms, and provisions added to administrative regulations are new transfer mechanisms subject to appropriate safeguards introduced by the GDPR. In its Schrems II Decision, the CJEU stated that the concepts of "enforceable rights," "effective legal remedies," and "appropriate safeguards" within the scope of GDPR Art. 46 are in accordance with the GDPR, which regulates the general principles regarding transfers. It stated that all provisions contained in Part 5 should be interpreted considering Article 44 of the GDPR, which states that they shall apply so as not to undermine the level of protection of natural persons guaranteed by the GDPR (Case C-311/18, Schrems II, para. 104, 2018). Furthermore, GDPR Recital 108 states that any appropriate

safeguards must be compatible with the general principles of personal data processing set out under Art. 5 GDPR.

Another suitable safeguard in GDPR Art. 46 is Standard Contractual Clauses (Union, 2018). Standard Contractual Clauses, like other appropriate safeguards, provide the legal basis for transfers of personal data to third countries or international organizations in the absence of an adequacy decision pursuant to Article 45(3) of the GDPR. They are regulated in GDPR Art. 46(2)(c) and Art. 46(2)(d). The Standard Contractual Clauses included in GDPR Art. 46(2)(c) are the clauses accepted and declared by the Commission. The Standard Contractual Clauses included in GDPR Art. 46(2)(d) are new contractual clauses introduced by the GDPR that are not included in Directive 95/46. The Standard Contractual Clauses included in GDPR Art. 46(2)(d) are accepted by the national supervisory authority and approved by the Commission (Union, 2018). However, the opinion of the EDPB is required to accept the Standard Contractual Clauses in Article 46(2)(d) prepared by the national supervisory authority. National supervisory authorities are granted the authority to accept Standard Contractual Clauses under the GDPR, which expands their overall authority. Both clauses are subject to the review procedure referred to in the Standard Contractual Clauses referred to in GDPR Art. 93(2) (Council, 2011). In addition, in accordance with Article 46(2), there is no need to obtain special permission from national supervisory authorities for transfers within the scope of Standard Contractual Clauses. Thus, the GDPR has simplified procedures and reduced bureaucracy for international data transfers by overriding the notification and authorization obligations contained in the Directive, which are valid in some EU countries.

Personal data transfers across the EU commonly rely on Standard Contractual Clauses, also known as model contract clauses, as the most effective method of ensuring appropriate assurance. Article 28(6) of the GDPR states that the contract between the data controller and data processors regarding the processing activity may be "wholly or partially" based on Standard Contractual Clauses accepted by the Commission or the local supervisory authority, making Standard Contractual Clauses a model for data transfer. This provision in Article 28(6) of the GDPR demonstrates the essential nature of Standard Contractual Clauses as a tool for data transfer. The Standard Contractual Clauses method involves signing a contract between the person transferring personal data from the EU and the person receiving the data outside the EU. The contract in question should include the obligations of the parties arising from the contract and the rights of the relevant person. Relevant parties can request these rights from the data transferor and the data

transferee. Additionally, in transfers made using Standard Contractual Clauses, the data transferee must agree to comply with the courts and local supervisory authority to which the data transferor is subject in the event of a dispute (Europe, 2018).

In line with Directive 95/46, adopted by the Commission, there were two sets of Standard Contractual Clauses for transfers from data controllers to data controllers and one set of Standard Contractual Clauses for transfers from data controllers to data processors (Commission, 2010). In 2016, based on the CJEU's Schrems I decision, the Commission decided to amend the contractual clauses from data controller to data controller, approved in 2001, and from data controller to data processor, approved in 2010 (Decision, 2016). After the GDPR comes into force, the Commission, on June 4, 2021, in accordance with GDPR Art. 46(2)(c), for data transfers from data controllers or data processors located in the EU to data controllers or data processors located outside the EU, published two modernized sets of Standard Contractual Clauses to replace these three Standard Contractual Clauses (Commission, 2021). GDPR Recital 106 requires regular review of Standard Contractual Clauses approved by the Commission, as well as adequacy decisions. In Article 46(5) of the GDPR, powers granted by a Member State or supervisory authority based on Article 26(2) of Directive 95/46 shall remain valid until modified, renewed, or repealed, if necessary, by that supervisory authority. The same article further states that the decisions adopted by the Commission within the scope of Article 26(4) of Directive 95/46 are valid until they are changed, renewed, or repealed by a Commission decision. As a matter of fact, with the decision taken on June 4, 2021, the Commission published two new sets of Standard Contractual Clauses to replace the three sets of Standard Contractual Clauses accepted within the scope of the Directive. Users must use Commission-approved Standard Contractual Clauses exactly as they are, without making any changes other than filling in the annexes. However, in practice, if a change is made to the Standard Contractual Clauses, this means that the Standard Contractual Clauses in question will be considered *ad hoc* clauses requiring the approval of the national supervisory authority (Kuner, 2020). GDPR Recital 109 regulates that the relevant parties can add additional clauses or measures to the contractual clauses in line with their needs if they do not conflict with the main clauses and do not hinder the fundamental rights and freedoms of the data subjects. Data controllers and data processors can be supported in this direction. In practice, it is seen that these additional measures are unlikely to be incompatible with these conditions; on the contrary, they create a practice that protects the freedoms of individuals more and does not conflict with Standard Contractual Clauses.

Additional clauses are especially important in cases where there is a high risk of sensitivity to data and detailed data security requirements (EDPB, 2020). Because in this case, additional clauses allow a more effective and appropriate assurance to be provided.

The CJEU's Schrems II decision was the first to confirm that Standard Contractual Clauses, which are a data transfer mechanism, provide sufficient protection (Christhoper K., 2021). In paragraph 148 of the decision, the CJEU states that Standard Contractual Clauses effectively suspend or prohibit the transfer of personal data to a third country when the receiving party fails to comply with these clauses as outlined in the annex of the decision. In addition, according to the determination of the CJEU in the Schrems II decision, since the applicability of EU law requires the applicability of the Charter, data transfers made based on the appropriate safeguards in Article 46 of the GDPR must be interpreted considering the Charter, and the standards regarding the level of protection must be determined based on the Charter (Case C-311/18, Schrems II, para. 105, 2018). In these circumstances, the CJEU has approved the use of Standard Contractual Clauses alone as a data transfer mechanism (Case C-311/18, Schrems II, para. 136, 2018). The Court underlined that the Standard Contractual Clauses adopted by the Commission aim to provide data controllers or processors established in the EU with guarantees that apply in the same way in all third countries, regardless of the level of protection contractually guaranteed in each third country.

Appropriate safeguards, which are data transfer mechanism adapted only to certain types of transfers, are narrower in scope than adequacy decisions, which are another data transfer mechanism. However, in its Schrems II decision, the CJEU ruled that a level of protection essentially equivalent to that guaranteed under EU law, which applies to adequacy decisions, also applies to transfers made based on Standard Contractual Clauses (Case C-311/18, Schrems II, para. 96., 2018). The CJEU ruled in the decision in question that the criteria for appropriate safeguards under Article 46 are the same as those for determining the adequacy decision under Article 45(2) (Case C-311/18, Schrems II, para. 104, 2020). This decision is one of the most important results of Schrems II regarding international data transfers under the GDPR.

Despite the letter of the GDPR and the long-standing practice of national supervisory authorities, the interpretation of the Schrems II decision ignores the hierarchy between these two data transfer mechanisms (Kuner, 2020). It is also stated in the EDPB's guide that the CJEU's Schrems II decision applies not only to Standard Contractual Clauses but also to all appropriate safeguards included in GDPR Art. 46(2) (EDPB, 2020). In the Schrems II decision, the CJEU

confirmed the validity of Standard Contractual Clauses as a means of data transfer (Case C-311/18, Schrems II, para. 136., 2018). In this context, the CJEU underlined that for Standard Contractual Clauses to remain a valid data transfer mechanism, data exporters must provide appropriate safeguards and apply "additional measures" when necessary, to eliminate the gaps in ensuring a level of data protection at a standard essentially equivalent to EU Law in third countries (Case C-311/18, Schrems II, para. 103, 133, 134., 2018). The CJEU determined in the Schrems II case that Standard Contractual Clauses do not bind public authorities in third countries that are not parties to the contract. This is because these clauses are contractual, and as a result, public authorities of third countries cannot be prevented from accessing personal data in transfers made through Standard Contractual Clauses. In this context, the CJEU decided that the parties must provide "additional safeguards" in addition to the safeguards provided under Standard Contractual Clauses to protect against third countries' access to personal data by competent authorities and referred to GDPR Recital 109 at this point (Case C-311/18, Schrems II, para. 134;, 2018) (EDPB, 2020). Furthermore, the CJEU did not define additional guarantees or provide detailed information on how to obtain these guarantees in either the GDPR or the Schrems II decision. The EDPB's guidance includes details on additional safeguards that data controllers and data processors acting as data exporters can follow to determine the safeguards they should obtain. According to the aforementioned document, the main additional assurances set by EDPB as examples are: technical measures such as encryption, pseudonymization, and data processing at multiple locations or parties; commitments to implement technical measures; contractual measures such as publishing transparency reports and documents on public authorities' access to data and prohibiting onward transfers; and organizational measures such as the adoption of internal policies and documentation of data access requests (EDPB, 2020, p. 28). Additionally, EDPS has published a document aimed at ensuring and monitoring compliance of EU institutions, bodies, offices, and agencies with the Schrems II decision (EDPS, 2020).

In the Schrems II case, the CJEU charged the data controller and processors, who are the data transferors, with the primary responsibility to provide a standard of protection essentially equivalent to EU law in third countries for personal data transfers made under Standard Contractual Clauses. At this point, the CJEU has also applied the principle of accountability in GDPR Article 5(2) to data transfers to third countries, which is a form of data processing (EDPB, 2020, p. 10). According to the Court, as a requirement of the principle of accountability, the data

transferor with Standard Contractual Clauses, in cooperation with the data transferee, takes additional measures to those provided by these clauses when necessary to check whether the relevant third country laws provide sufficient protection compared to EU laws and to determine the level of protection provided by EU laws before the transfer (Case C-311/18, Schrems II, para. 134., 2018). The third country must verify on a case-by-case basis whether it complies with the requirements (Case C-311/18, Schrems II, para. 142., 2018). The CJEU has stated that if a controller or processor established in the EU cannot take sufficient additional measures to guarantee such protection, the relevant controller or processor, or, failing this, the national supervisory authority, must suspend or terminate the transfer of data to third countries (Case C-311/18, Schrems II, para. 135., 2018). The CJEU stated that a national supervisory authority can suspend and prohibit data transfers if it determines that EU and domestic law have been infringed, as the approval of Standard Contractual Clauses by the Commission does not give the Commission the power to limit the powers of national supervisory authorities under Article 58(2) of the GDPR. In its Schrems II decision, the CJEU confirmed the principles regarding the application of appropriate safeguards set out in the Schrems I decision (Case C-311/18, Schrems II, para. 133, 2018) (Christhoper K., 2021). Unless an adequacy decision is available, the national supervisory authority is unable to comply with these articles in the third country in question, where the protection of the transferred data required by EU law, in particular Article 45, Article 46 of the GDPR, and the Charter, cannot be provided by any other means and the transfer of the data controller or data processor. If the transfer does not suspend or terminate, the national supervisory authority must, in its own opinion and considering all the conditions of the transfer, suspend or terminate the data transfer made within the scope of Standard Contractual Clauses (Case C-311/18, Schrems II, para. 121., 2018). In addition, even if there is an existing adequacy decision, if a person lodges a complaint, the national supervisory authority should be able to examine whether the transfer complies with the requirements of the GDPR and, if they have doubts about the validity of the adequacy decision, apply to the national courts for a preliminary ruling on it (Case C-311/18, Schrems II, para. 120., 2018).

3.2 Chapter II Modernized Standard Contractual Clauses After the Schrems II Decision

On June 4, 2021, the Commission published two new updated sets of Standard Contractual Clauses that incorporate the requirements of the GDPR and consider the legal assessment in the CJEU's Schrems II decision (Commission, 2021). The first of these sets is regulated within the scope of GDPR art. 28(7) and art. 29(7), which do not cover international transfers and are for use between data controllers and data processors within the EU (Commission, 2017). The second set of Standard Contractual Clauses are Standard Contractual Clauses created to provide appropriate assurance in the transfer of personal data to third countries within the scope of GDPR Art. 46 (Commission, 2021). These new modernized Standard Contractual Clauses replace the three existing Standard Contractual Clauses. The existing Standard Contractual Clauses, created in the early 2000s in accordance with the provisions of Directive No. 95/46, did not incorporate the innovations and changes introduced by the GDPR, which replaced the Directive in 2018. In its Schrems II decision, the CJEU stated that third country laws may weaken the level of protection of transferred data and that public authorities may have unauthorized access to transferred personal data. Therefore, the CJEU also stated that Standard Contractual Clauses should include additional measures to provide a level of protection equivalent to the protection provided by the GDPR. This situation has created the need to update existing Standard Contractual Clauses with the innovations brought by GDPR. The new Standard Contractual Clauses require significantly enhanced security measures, notification, reporting, and recording obligations over existing ones.

On September 27, 2021, the abolition of the current Standard Contractual Clauses requires that contracts regarding data transfer signed after this date be regulated in accordance with the new Standard Contractual Clauses. Contracts signed using existing Standard Contractual Clauses before September 27, 2021, are considered to provide appropriate assurance for 15 months (until December 27, 2022), provided that the processing activities subject to the contract do not change (Commission, 2021). The new Standard Contractual Clauses continue to contain some of the same issues as the existing Standard Contractual Clauses. The new Standard Contractual Clauses include requirements for GDPR compliance to ensure an adequate level of data protection, prohibit parties from changing the standard clauses, and mandate updating of annexes for specific data transfers. Additionally, additional clauses can be added to new Standard Contractual Clauses, as well as existing ones, if they do not conflict with the standard clauses. In addition to existing requirements,

principles such as transparency, data subject rights, and data breaches are important innovations brought by new Standard Contractual Clauses to comply with GDPR principles. Although existing Standard Contractual Clauses offer limited data transfer, new Standard Contractual Clauses provide more flexibility thanks to their new modular structure (Gordon, 2021). Thanks to this structure, data transferors and data transferees can choose the option that best suits their needs under the same contract (Compagnucci, 2021). These modules are four: transfers from data controller to data controller or data processor and from data processor to data processor or data controller. Current Standard Contractual Clauses only cover transfers from the data controller to the data controller or data processor. An example of a data processor-to-data processor transfer is that a cloud service provider located in the EU, which is a data processor, transfers data to another data processor in a third country that provides infrastructure services to this service provider. In the case of a transfer from the data processor to the data controller, the data is transferred back to the data controller (return to the original), and this is called reverse transfer (Compagnucci, 2021, p. 8). According to the new Standard Contractual Clauses, the data exporter may also be established outside the EU, expanding the requirement beyond just the data transferor established within the EU being a party to the contract. This application, with its modular structure, allows the transfer of all kinds of data between the data transferor and the data transferee, regardless of its location and data processing role (Lee, 2021).

In the new Standard Contractual Clauses, it is possible for more than one data-transferring party within company groups or collaboration to enter a contract and to add new parties to the contract over time based on the "docking clause" (Decision, 2021). This optional clause allows third parties transferring data to join the existing contract without entering a separate contract. Third parties can also become involved in the contract by signing the relevant annexes, which contain the details of the transfer, the technical and organizational measures applied, and the list of sub-processors. It is thought that this new system will provide greater flexibility and convenience for existing data processing practices, especially in the context of acquisitions, sub-processors, and additional corporate entities (Braun, 2021). The new Standard Contractual Clauses include two provisions that address the concerns stated in the CJEU's Schrems II decision. The data transferee must ensure that local laws do not undermine the level of protection provided by Standard Contractual Clauses and must document the local law assessment to support this guarantee. Upon request, the party receiving the data must forward these documents to the relevant

EU data protection authorities and declare that they have implemented additional measures. The second provision is that Standard Contractual Clauses require the data transferee to sue for government access requests regarding the personal data in question. Additionally, if the data transfer is legally permitted, the data exporter must inform the data subject of the access request in question, if possible. As another consequence of the Schrems II decision, new Standard Contractual Clauses require companies to carry out a "Data Protection Impact Assessment", which includes a data transfer impact assessment, and to document this assessment and submit it to the national supervisory authority upon request. Companies should include in the data transfer impact assessment an evaluation of whether the laws of the third country to which data are transferred conflict with the GDPR and Standard Contractual Clauses, as well as whether additional measures for data protection are necessary. For example, this assessment should determine whether the transferred data is subject to FISA 702 (Compagnucci, 2021, p. 9). This evaluation should be constantly monitored and revised in case there is a change in third-country laws (Compagnucci, 2021, p. 9). The annexes of the new Standard Contractual Clauses also contain more detail than the annexes of the existing ones. Personal data retention periods, the definition of additional protections for special personal data, and a detailed explanation of the technical and administrative measures taken by the data transferee can be given as examples of these details. Because of the abundance of these details, it is evident that preparing the standard contract clause annexes will require more time.

The new Standard Contractual Clauses include several security measures. Annex II of the new Standard Contractual Clauses details the technical and organizational measures required for an appropriate level of protection, including measures to ensure the security of data. According to Annex II, these measures should be defined in specific rather than general terms. These measures are aimed at ensuring an appropriate level of security, considering the scope, nature, context, and purpose of the processing and the risks to the rights and freedoms of natural persons. The most notable and important measures are pseudonymization and encryption measures (Decision, 2021, p. 31). The new Standard Contractual Clauses clearly state that the data transferee can demonstrate its compliance with its obligations under these articles and oblige the data transferee to provide such compliance documents upon request of the national supervisory authority. Contrary to the current Standard Contractual Clauses, according to the new Standard Contractual Clauses, those to whom data is transferred are subject to the EU supervisory authorities, and the relevant persons

will be able to complain about the data transferred to the EU supervisory authorities and courts. In addition, data transferees are required to report data breaches directly to the EU supervisory authorities.

The new Standard Contractual Clauses impose more obligations and requirements for data transferees, and especially for data transferees who are data controllers, in line with the requirements of the GDPR. These obligations include meeting the requests of relevant persons to exercise their GDPR rights, deleting personal data that is no longer needed within the scope of the purposes for which they are transferred, filing a lawsuit regarding the third country authorities' request for access to personal data, the obligation to notify the relevant persons and notify the EU authorities of data breaches, and providing technical and technical information for the transferred data. Recipients of the data transfer will likely need to modify their personal data protection policies to meet these obligations (Gordon, 2021).

The effectiveness of the new Standard Contractual Clauses largely depends on the context in which they are used and the specific requirements they must meet. From this point of view, it appears that, the overall structure of this new model raises some challenges. Indeed, the possibility of interfacing different contractual forms within the same general model is likely to generate some uncertainties in its practical application (Bertoldi, 2021). The new Commission Decision on Standard Contractual Clauses represents a significant change in how these clauses are applied for international data transfers. According to Art.1 of the Decision, the new SCCs are designed to provide appropriate safeguards as per Art. 46 of the GDPR for data transfers from an EU entity (data exporter) to a non-EU entity (data importer) when the GDPR is not directly applicable to the importer. This implies that the new SCCs are primarily intended for situations where the GDPR does not apply to the data recipient. The decision indicates that these mechanisms for data transfer outside the EU may not be necessary when the data is transferred to entities covered under Article 3(2) of the GDPR, which extends the regulation's scope to certain entities outside the EU based on their data processing activities. The European Data Protection Board plans to assess the interaction between the territorial scope of the GDPR and the provisions on international data transfers. Chapter V of the GDPR emphasizes that the goal of data transfer mechanisms is to ensure an adequate level of data protection, suggesting that such mechanisms might not be needed when EU data protection law can be directly applied. While the new SCCs aim to modernize EU law in light

of evolving trade practices, it remains to be seen if they will effectively address the issues posed by the previous model clauses in practical scenarios (Bertoldi, 2021).

3.3 Chapter III EDPB's Recommendations After the Schrems II Decision

Following the CJEU's Schrems II decision, the EDPB published recommendations on additional measures that complement the transfer mechanisms to ensure the protection of transferred personal data at the EU level, within the scope of the requirements in the Schrems II decision, with the draft version on November 10, 2020 (EDPB, 2020), and the final version on June 18, 2021 (EDPB, 2021). According to the EDPB recommendations, the preferred transfer mechanism should include some additional measures to provide an equivalent level of protection to the fundamental rights and freedoms of individuals under the GDPR and the Charter. The recommendations also provide considerable guidance for safeguarding against access to personal data by public authorities in third countries. The EDPB recommends that both the data transferor and the recipients of the data ensure the level of protection determined by EU law in data transfer. As data transferors, data controllers or data processors must cooperate with data transferees to ensure the protection of data and monitor the impact of the measures taken for this purpose. In these recommendations, EDPB recommends that, within the scope of transferring personal data to third countries that do not have an adequacy decision, the data transferor and the data transferee should follow a six-step system to evaluate the transfers. The EDPB's final recommendations determined whether additional measures were required for a particular data transfer. The six-step road map to be followed by the data exporter will be summarized below:

Step 1: “Know your data transfers”: Data exporters must be aware of personal data transfers to third countries, including onward transfers. In this context, as a requirement of the principle of accountability, all processing activities should be recorded by those transferring data; data should be mapped; relevant persons should be informed; and the data minimization principle should be observed (EDPB, 2020, pp. 8-9). Recording and mapping data transfers is necessary to ensure a substantially equivalent level of protection wherever data is processed, despite the difficulty it may pose (Compagnucci, 2021, p. 6).

Step 2: “Determine the transfer mechanism you trust”: In this step, it is necessary to determine the appropriate transfer mechanism in GDPR Part 5 for the transfer. The next steps do

not need to be taken if there is an adequacy decision for a third country. However, the existence of an adequacy decision does not prevent the relevant person from having the right to complain or the supervisory authorities from filing a lawsuit before the court and applying to the CJEU (EDPB, 2020, p. 12). In addition, the transfer of personal data can continue by considering the conditions contained in the provision through the exceptions in Article 49 of the GDPR. If the transfer does not fall within the scope of an adequacy decision or exceptions, continue with step 3 for the transfer using appropriate safeguards in Article 46 of the GDPR (EDPB, 2020, p. 13).

Step 3: "Assess whether the appropriate safeguards under Art. 46 of the GDPR on which you are relying are effective in the light of all the circumstances of the transfer": Data transferors must be aware of the publicly available laws, regulations, and/or practices of the third country, including in onward transfers, within the scope of Art. 46. Data transferors must carry out a data transfer impact assessment to determine if the transfer affects the effectiveness of appropriate safeguards (Case C-311/18, Schrems II, para. 104, 2018) (EDPB, 2020, p. 15). This assessment includes the legislation and practices in the third country regarding the protection of transferred data, whether third country public authorities can access personal data and surveillance laws, the criteria used to assess adequacy in Article 45(2) of the GDPR, and different aspects of the third country legal system. Considerations such as the rule of law and individuals' right to judicial compensation against illegal access to personal data should be considered. In addition, the sources and information to be used in the evaluation must be impartial, reliable, verifiable, and publicly available, and they must be documented to be presented to the supervisory authority or judicial authorities upon request (EDPB, 2020, pp. 18-19). The assessment result determines that the transfer mechanism is effective, indicating an equivalent level of protection to that provided in the EU (Case C-311/18, Schrems II, para. 105, 2018). (EDPB, 2020, p. 20)

Step 4: "Adoption of additional measures": If, according to the data transfer impact assessment, it is determined that the transfer mechanism of GDPR Art. 46 is not effective, the data exporter must evaluate, in cooperation with the data transferee, whether additional measures are needed (EDPB, 2020, p. 21). The purpose of additional measures is to enhance the existing safeguards provided by the transfer mechanism (Case C-311/18, Schrems II, para. 133, 2018). Additional measures may be of a contractual, technical, or organizational nature. Adding these measures to the safeguards contained in Article 46 can provide a level of protection essentially equivalent to the EU standard for transferred data in the third country (EDPB, 2020, p. 28).

Determining which additional measures may be effective should be done on a case-by-case basis, considering the assessment in the first three steps (EDPB, 2020, p. 21). In addition, the EDPB has determined a non-exhaustive list that will influence the data exporter, in cooperation with the data transferee, to determine what additional measures are to be taken to protect the transferred data to which public authorities request access based on the problematic legislation of the third country (EDPB, 2020, p. 22).

Step 5: "Formal procedural steps": Formal procedures need to be followed when additional measures to be taken are identified. If the additional measures for Standard Contractual Clauses do not conflict with the Standard Contractual Clauses and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined, approval from the national supervisory authority is not required. (EDPB, 2020, pp. 23-24)

Step 6: "Reassessment at appropriate intervals": The data exporter, in cooperation with the data exporter, conducts an initial assessment of the level of protection of the third country in the third country to which data is transferred, as well as a data transfer impact assessment and a continuous assessment of whether there are new developments that may affect additional measures taken based on the transfer. The data exporter must monitor and review the situation (EDPB, 2020, p. 25). This situation also demonstrates compliance with the principle of accountability in Article 5(2) of the GDPR. Data transferors must establish adequate systems so that a transfer based on Standard Contractual Clauses can be suspended or prohibited if the additional measures taken are no longer effective in the third country, the rules are violated, or they are no longer possible to comply with (EDPB, 2020, p. 25).

On the other hand, there are some important points that attract attention in EDPB's recommendations. The recommendations state that appropriately applied technical measures are the only way to prevent or neutralize the access of public authorities in third countries to personal data, especially for surveillance practices. Additionally, it is mentioned that technical measures, in conjunction with contractual and organizational measures, will enhance data protection by preventing access to personal data (EDPB, 2020, p. 22). Furthermore, it has been stated that the effectiveness of these measures is enhanced when they are applied collectively rather than individually (EDPB, 2020, p. 22). If the laws and practices of the third country have problematic legislation, the data exporter may suspend the transfer, take additional measures, or continue the transfer without taking additional measures. However, to continue data transfer without taking

additional measures, there is a condition that the problematic legislation does not apply to the relevant data transfer or to the data transferee. In this case, it must be documented that the problematic legislation will not apply to the data transferor or the data transferee and that it will not prevent the data transferee from fulfilling its obligations under Article 46 by preparing a detailed report in cooperation with the data transferor and the data transferee. This certification is a requirement of the principle of accountability. The EDPB does not consider these recommendations as an opinion or decision, and they are not legally binding. EDPB recommendations are an important guide to consider for transfers. In addition to the recommendations of the EDPB, there may also be guidelines published by national supervisory authorities (EDPB, 2020, pp. 17-18).

These recommendations are not an opinion or decision made by the EDPB and are not legally binding. EDPB recommendations are an important guide to consider for transfers. In addition to the recommendations of the EDPB, there may also be guidelines published by national supervisory authorities. As a matter of fact, there is a guide published by the French national supervisory authority (CNIL) regarding data transfer outside the EU (CNIL, 2021). The French supervisory authority, CNIL, would allow no transfers of personal data to entities outside the EEA or subject to non-EEA law. According to CNIL, EU personal data must be processed by entities subject to EU law alone. Therefore, none of the three types of health transfers are permissible. Once an entity subject to foreign law accesses the personal data, the full protections of the GDPR have been compromised. This interpretation of Schrems II would lead to siloed research efforts and would undercut collaborative responses to public health challenges such as COVID-19. EU/EEA organizations (eg universities, pharma, medical device companies, technology providers) would be prevented from processing personal data from third countries, as once the data are processed in the EU/EEA and subject to GDPR, it would not be possible to transfer it back to the third country where the personal data were originally collected (e.g. an African country). Accordingly, these international research collaborations would need to exclude EU/EEA organizations in favor of controllers and processors established in other jurisdictions such as the USA or other Asia Pacific Economic Cooperation member countries (Laura Bradford, 2021).

3.4 Chapter IV Implementation of Standard Contractual Clauses from the Perspective of Stakeholders

Legal professionals, including attorneys, lawyers, and in-house counsels, face significant challenges when dealing with Standard Contractual Clauses (SCCs), crucial for ensuring GDPR compliance in international data transfers. The complexity and constant evolution of data protection laws necessitate a thorough understanding of these changes, including new SCC versions, and varying data protection laws globally. In this regard, lawyers, attorneys, and in-house counsels need to be aware of these changes, including new versions of the SCCs and changes to data protection laws both within and outside the EU (Horvath, 2022). SCCs ensure that personal data transferred to third countries receives a level of protection essentially equivalent to that guaranteed within the EU. They must assess whether the legal framework in the recipient country might impede the effectiveness of SCCs, especially considering the Schrems II decision. Another point to note is that SCCs are not one-size-fits-all solutions. They often require customization to fit the specific conditions of data transfer. Tailoring them to specific transactions requires attorneys to have a deep understanding of the nature of the data being transferred, the purposes of the transfer, and the capabilities of the data importer. In-house counsels must ensure compliance of the SSCs with both internal legal obligations (such as corporate policies) and external legal requirements, including the laws of the country where the data is transferred. Also, in-house counsels often face the challenge of negotiating GDPR with business partners who have different priorities or levels of understanding of their data protection requirements. An organization's broader data protection and privacy strategy should integrate SCCs (Cory, 2020). This requires a holistic approach to compliance, privacy policies, and data management. Ensuring that data-subject rights are enforced in a third country is a significant challenge. Lawyers should develop a strategy for how to handle data subject complaints and potential litigation, particularly in jurisdictions with different legal systems. They should assess and mitigate the risks associated with data transfers, particularly considering the potential for significant fines under the GDPR. These challenges require lawyers, attorneys, and in-house counsels not only to have a deep understanding of data protection laws but also to be adept at navigating international legal landscapes, negotiating contracts, and implementing comprehensive data governance frameworks.

Companies that engage in data transfers using Standard Contractual Clauses (SCCs) have several concerns, mainly due to the strict requirements of the EU General Data Protection Regulation (GDPR) and the complexity of international data transfer laws. For example, ensuring compliance with the specific requirements of the GDPR and SCCs is an important concern. Non-compliance can result in fines and reputational damage. As the legal landscape for data protection and privacy related to international data transfers is constantly evolving, companies are anxious to keep up with these changes and adapt their practices accordingly. After the Schrems II decision, monitoring of the adequacy of data protection in third countries has increased. Companies are concerned that the legal and regulatory frameworks in these countries may undermine the protection provided by SCCs (Overstraeten, 2021). The risk of data breaches and the associated liabilities is a significant concern, especially when data is transferred internationally. Companies are concerned about the potential financial and reputational impact of such breaches. Implementing SCCs and ensuring ongoing compliance can be costly. This includes costs related to legal advice, technological measures for data protection, and administrative efforts. Companies often must negotiate GDPR with their business partners, which can be difficult, especially when partners have different views on data protection or are in jurisdictions with different legal standards. There is concern, particularly in non-EU jurisdictions, about how the implementation of the SCCs will take place. Companies are also concerned about their potential liability in the event of non-compliance by their partners. The interpretation and application of SCCs can sometimes be ambiguous, leading to uncertainty about how best to implement them in specific business contexts. Another question for companies is how information transfer mechanisms like SCCs can affect their business continuity and scale, especially in a globally and digitally interconnected business environment.

Regulators and Non-Governmental Organizations such as Max Schrems' organization European Center for Digital Rights (NOYB) have different concerns about Standard Contractual Clauses and international data transfers. The role of regulators in data transmission is undeniable. Regulators focus on ensuring that SCCs effectively enforce data protection laws, particularly the GDPR. They are concerned about the adequacy of the protection offered by SCCs. Furthermore, ensuring a consistent approach to data protection in different EU member states is a challenge for regulators. They aim for the harmonized implementation of data protection laws. Regulators must provide organizations with clear guidance on effectively implementing SCCs. Like companies, they are concerned about ambiguities and the need for clarity in legal requirements. Regulators are

responsible for handling complaints about data transfers and remedying any breach of the GDPR. They are concerned about how effective the mechanisms are in place to address these issues.

NGOs like NOYB are deeply concerned about protecting basic privacy rights. They focus on ensuring that SCCs and other data transfer mechanisms do not violate individual privacy rights. There is serious concern about how the laws and practices of third countries, particularly those with extensive surveillance programs, will affect the privacy of EU citizens. NGOs seek greater transparency and accountability in international data transfers. They cite the lack of transparency in data processing activities and the lack of accountability, particularly at large tech companies, as problems. The goal of NGOs like NOYB is to raise public awareness of data protection rights and empower individuals to act against privacy violations. They are concerned about the understanding and enforcement of the rights of the public under the GDPR. Regulators are primarily concerned with the enforcement, compliance, and harmonization of data protection standards, while NGOs focus on the protection of fundamental rights, transparency, and the fight against inadequate data protection practices. Both play an important role in shaping the international data transfer landscape and the effectiveness of mechanisms such as SCCs.

The effective implementation of Standard Contractual Clauses (SCCs) depends on the cooperation and knowledgeable efforts of all parties involved. Each stakeholder has a crucial role to play in shaping the international data transfer framework and ensuring that personal data transfers meet the strict protection standards set by the EU. As the digital environment continues to evolve, tools and methods must constantly adapt to protect international personal data. It provides a harmonious combination of unlimited information

CONCLUSION

1. Organizations should research, thoroughly analyse, and understand the data protection and privacy laws of the recipient country. Organizations should focus on the supervisory laws and practices of the country of significant concern in the Schrems II decision. Also, the transfer of data to third countries raises the issue of taking into account and assessing the existence of potential risks for the rights and freedoms of data subjects. Factors such as government access to data, the lack of an independent oversight body, and the lack of legal remedies for data subjects in the receiving country should be considered. Organizations should explore alternative data transfer mechanisms where the legal framework of the recipient country does not offer adequate protection. This may include the use of Binding Corporate Rules (BCR) for intra-group transfers or the adoption of specific technical measures such as encryption and pseudonymisation to protect data. Given that laws and interpretations are subject to change, it is important that organizations continuously monitor data protection legal developments both within the EU and in host countries. Organizations should regularly update the due diligence process in response to these changes.

2. After the Schrems II decision, the European Commission developed updated versions of the Standard Contractual Clauses that better comply with GDPR requirements and address the issues raised in the Schrems II decision. Organizations should utilize these updated Standard Contractual Clauses and ensure their full integration into their contracts. Although Standard Contractual Clauses provide a standard framework, they may need to be adapted to specific relocation scenarios. Organizations should ensure that provisions accurately reflect the realities of data transfer, including the type of data transferred, the purposes of the transfer, and processing activities. Keeping detailed records of the assessment process, decisions made, and actions taken is essential to demonstrating compliance with data protection authorities.

3. Organizations should establish clear internal policies on international data transfers and train their employees accordingly. These policies should be detailed and tailored to the organization's specific data transfer needs. In particular, policies should incorporate the concepts and requirements arising from the Schrems II decision. This involves understanding the implications of transferring data to countries outside the EU, particularly the US, and the additional protection requirements where necessary. It is critical to implement robust training programs for all employees involved in data processing and transmission. These training sessions should cover

the basics of data protection laws, the specifics of the GDPR, the Schrems II ruling, and the organization's internal data transfer policies. Training programs can incorporate scenario-based learning to help employees understand the practical applications of policies and how to respond in different situations involving international data transfers. Training programs may involve external data protection experts or legal experts to benefit from their expertise and cover areas that may be overlooked internally. In addition to formal training, it is crucial to develop a culture of data protection awareness within the organization. This can be achieved through regular communications, updates, and an open-door policy for employees to discuss data protection issues.

4. In addition to the Standard Contractual Clauses, additional technical, organizational and contractual guarantees should be implemented. These measures may include encryption, pseudonymisation and regular audits to ensure compliance with EU data protection standards. Segmentation can be used to apply the principles of data minimization and limit access and exposure to data within the organization, ensuring that only necessary data is transferred. Implementing strict role-based access controls ensures that only authorized personnel have access to personal information based on their role and necessity, mitigating risks. It is possible to carry out regular internal audits of data processing activities to ensure compliance with data protection policies and legal requirements. Based on rapidly developing technology, it will be useful in this regard to regularly update and improve technological solutions to prevent possible threats and ensure reliable data protection.

5. Continuous assessment of data transfer mechanisms and the legal landscape of the recipient country is important. Legal experts specializing in international data protection laws should conduct a periodic review of the legal landscape in recipient countries, focusing on changes in data protection laws, supervisory practices, and court decisions that may affect the adequacy of data protection. To ensure an accurate and up-to-date analysis, it is advisable to engage legal experts who specialize in international data protection laws. Furthermore, it is essential to maintain detailed documentation of all assessments, including justifying the selection of specific reporting mechanisms and determining recipient country adequacy. It may be a reasonable step to periodically inform data subjects of the assessments and safeguards available for international data transfers in order to ensure transparency.

6. Given the complexity and evolution of data protection laws, particularly in the context of Standard Contractual Clauses, it is critical to provide continuing education and training for legal

professionals. This includes attorneys, paralegals, and in-house counsels. As one stakeholder, regulators play a key role in the effective implementation of data protection laws. To increase the effectiveness of the implementation of Standard Contractual Clauses, it is important that regulatory bodies provide comprehensive and clear guidance that evolves with the changing legal landscape. Regulatory bodies can ensure regular updates to the guidance, reflecting the latest legal developments and best practices. Keeping organizations informed of available resources, including case studies, can be an effective way to help organizations resolve issues related to Standard Contractual Clauses. Progress can be made by streamlining active dialogue and feedback mechanisms with various stakeholders, including businesses, legal professionals, and data protection officers. Organizations should engage with NGOs and advocacy groups, such as the European Center for Digital Rights (NOYB) to increase transparency and accountability in data transfers. These groups focus on protecting privacy rights and ensuring that data transfer mechanisms, including Standard Contractual Clauses, comply with the fundamental rights of individuals. Partnering with NGOs in public awareness campaigns on data protection rights can be useful, as campaigns can educate the public about their rights under the GDPR, the importance of data privacy, and how to redress for privacy breaches. Such efforts will not only inform the public but also increase confidence in organizations' commitment to protecting user data.

LIST OF REFERANCES

I. LEGAL ACTS

1. EU legal acts

1. European Data Protection Board (2021) Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.
   Available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en
   [Accessed 12 September 2023].

2. European Data Protection Supervisor (2014) '*Transfer of personal data to third countries'*
   Available at: https://edps.europa.eu/data-protection/our-work/publications/papers/transfer-personal-data-third-countries_en

3. European Data Protection Board (2020) Recommendations *01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.* Available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

4. European Parliament and the Council of the European Union (1995) *Directive 95/46/EC of the European Parliament and of the Council, On the protection of individuals with regard to the processing of personal data and on the free movement of such data.*
   Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

5. European Commission, the European Parliament, and the Council of the European Union (2018) Available at: https://gdpr-info.eu

6. European Parliament and the Council of the European Union (1995)
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046
7. European Commission, the European Parliament, and the Council of the European Union (2018)
Available at: https://gdpr-info.eu/chapter-5/
[Accessed 14 September 2023].
8. European Commission, the European Parliament, and the Council of the European Union (2018)
Available at: https://gdpr-info.eu/art-4-gdpr/

9. Decision of the EEA Joint Committee (2018) No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]
Available at: https://op.europa.eu/en/publication-detail/-/publication/03c28303-8b25-11e8-8a53-01aa75ed71a1/language-en

10. European Parliament and of the Council (2016) Directive (EU) 2016/680 The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

11. European Commission, the European Parliament, and the Council of the European Union (2018) Article 44 of GDPR.
Available at: https://gdpr-info.eu/art-44-gdpr/

12. European Commission, the European Parliament, and the Council of the European

Union (2018) Recital No 101.
Available at: https://gdpr-info.eu/recitals/no-101/

13. European Commission, the European Parliament, and the Council of the European Union (2018) Recital No 6.
Available at: https://gdpr-info.eu/recitals/no-6/
14. European Union (2000) The Charter of Fundamental Rights.
Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf
15. European Commission, the European Parliament, and the Council of the European Union (2018) Article 45 of GDPR.
Available at: https://gdpr-info.eu/art-45-gdpr/#:~:text=A%20transfer%%2020of%20personal%20data,an%20adequate%20level%20of%20protection.

16. Data Protection Commission (no date) *Transfers of Personal Data to Third Countries or International Organisations.* Available at: https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations
[Accessed 18 September 2023].
17. European Commission (2021) Adequacy Decisions.
Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

18. European Commission (2021) Implementing Decision (EU) 2021/1772.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D1772

19. European Commission (2021) Implementing Decision (EU) 2021/1772.
Available at: https://commission.europa.eu/documents_en

20. European Commission, the European Parliament, and the Council of the European

Union (2018) Article 45 of GDPR.
Available at: https://gdpr-info.eu/art-45-gdpr/#:~:text=A%20transfer%20of%20personal%20data,a%20n%20adequate%20level%20of%20protection.

21. European Commission (1998).
Available at: https://ec.europa.eu/newsroom/article29/items

22. European Commission (2000).
Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520

23. European Parliament and the Council of the European Union (1995).
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5

24. EDPB (2020) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
Available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

25. European Commission, the European Parliament, and the Council of the European Union (2018) Article 46 of GDPR.
Available at: https://gdpr-info.eu/art-46-gdpr/

26. European Commission, the European Parliament, and the Council of the European Union (2018) Article 64 of GDPR.
Available at: https://gdpr-info.eu/art-64-gdpr/

27. European Parliament and of the Council, Regulation (2011)
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R0182

28. EDPS (2020) Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling.
Available at: https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf

29. EDPB (2020) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
Available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en

30. European Commission, the European Parliament, and the Council of the European Union (2018)
Available at: https://gdpr-info.eu

31. European Commission, the European Parliament, and the Council of the European Union (2018) Chapter V.
Available at: https://gdpr-info.eu/chapter-5/
[Accessed 14 September 2023].

32. European Commission, the European Parliament, and the Council of the European Union (2018) Article 4 of GDPR.
Available at: https://gdpr-info.eu/art-4-gdpr/

33. EEA Joint Committee (2018) Decision No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement[2018/1022]
Available at: https://op.europa.eu/en/publication-detail/-/publication/03c28303-8b25-11e8-8a53-01aa75ed71a1/language-en

34. European Commission (2000).
Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pd

35. European Commission (1998).
Available at: https://ec.europa.eu/newsroom/article29/items

36. European Commission (2000) Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441).
Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520

37. European Parliament and of the Council (2011) Regulation No 282
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R0182

II. SCIENTIFIC LITERATURE

1. Books

1. Christhoper, K., Lee, A. B., and Christhoper, D. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

2. Articles in scientific journals

1. Van den Bulck, P. (2017) 'Transfers of personal data to third countries', ERA Forum, 18, pp. 229–247. Available at: https://link.springer.com/article/10.1007/s12027-017-0482-3.
2. Cedric, R. and Mistale, T. (2020) 'The GDPR as Global Data Protection Regulation?'. Available at: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688 [Accessed 14 Sep. 2023].
3. Christhoper, K. (2017) 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', German Law Journal.
4. Christhoper, K., Lee, A.B. and Christhoper, D. (2021) Update of Selected Articles. Oxford University Press. Available at: https://web.archive.org/web/20210509231556id_/https://fdslive.oup.com/www.oup.com/academic/pdf/law/GDPRCommentary_ArticleUpdates.pdf.

5. Chiara, B. (2021) 'The New European Commission Decision on Standard Contractual Clauses: A System Reform?', European Papers. Available at: https://www.europeanpapers.eu/en/europeanforum/new-european-commission-decision-standard-contractual-clauses-system-reform.
6. Laura, B., Mateo, A. and Kathleen, L. (2021) 'Standard contractual clauses for cross-border transfers of health data after Schrems II', Journal of Law and the Biosciences, 8. Available at: https://academic.oup.com/jlb/article/8/1/lsab007/6306998#265323735.

III. CASE LAW

1. Criminal proceedings against Bodil Lindqvist. European Court of Justice (2003) Case C-101/01.
2. Maximillian Schrems v Data Protection Commissioner. European Court of Justice (2015) *Case C-362/14, Schrems I, para 78.*
3. Maximillian Schrems v Data Protection Commissioner. European Court of Justice (2015) *Case C-362/14, Schrems I, para 53-58.*
4. Maximillian Schrems v Data Protection Commissioner. European Court of Justice (2015) *Case C-362/14, Schrems I, para 40-41.*
5. Maximillian Schrems v Data Protection Commissioner. European Court of Justice (2015) *Case C-362/14, Schrems I, para 63.*
6. Maximillian Schrems v Data Protection Commissioner. European Court of Justice (2015) *Case C-362/14, Schrems I, para 61.*
7. Maximillian Schrems v Data Protection Commissioner. European Court of Justice (2015) *Case C-362/14, Schrems I, para 73.*
8. Maximillian Schrems v Data Protection Commissioner. European Court of Justice (2015) *Case C-362/14, Schrems I, para 86-87.*
9. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) Case C-311/18, Schrems II, para. 80.
10. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 90.*

11. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 160.*
12. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 164.*
13. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 168-185.*
14. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 201-202.*
15. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, "Opinion of Advocate General Saugmandsgaard", para. 342.*
16. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 92 and 105.*
17. Maximillian Schrems v Data Protection Commissioner. European Court of Justice (2015) *Case C-362/14, Schrems I, para. 73.*
18. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 136.*
19. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 96.*
20. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 104.*
21. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 136.*

22. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 103, 133, 134.*
23. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 134.*
24. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 134.*
25. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 142.*
26. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 135.*
27. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 121.*
28. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 120.*
29. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 104.*
30. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 105.*
31. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II, para. 133.*

32. Maximillian Schrems v Data Protection Commissioner. Court of Justice of the European Union (2015) Judgment of the Court.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362
33. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. Court of Justice of the European Union (2020) Judgment of the Court.
Available at: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN
34. Joined Cases C-317/04 and C-318/04. Court of Justice of the European Union (2006) Judgment of the Court.
Available at: https://curia.europa.eu/juris/document/document.jsf?docid=57549&doclang=en
35. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. European Court of Justice (2020) *Case C-311/18, Schrems II,*
Available at: https://www.europeansources.info/record/cjeu-case-c-311-18-data-protection-commissioner-v-facebook-ireland-and-maximillian-schrems/

IV. OTHER DOCUMENTS

1. CJEU (2015) *Research and documentation directorate.*
Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf
[Accessed September 2023].

2. Information Commissioner's Office (2021) *International Transfers.*
Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

3. European Union Agency for Fundamental Rights and Council of Europe (2018) *Handbook on European data protection law.*
Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

4. CJEU (2018) *Adequacy Referential.*
Available at: https://ec.europa.eu/newsroom/article29/items/614108

5. BİLGİ Information Technology Law Institute (2020) Report of Data Flow.
Available at:
https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf

6. European Commission (2001) Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002D0002

7. European Commission (2021) *Adequacy decisions.*
Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

8. Information Commissioner's Office (2022) *Guide to the General Data Protection Regulation (GDPR)*
Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

9. Congressional Research Service (2021) U.S.-EU Privacy Shield and Transatlantic Data Flows.
Available at: https://crsreports.congress.gov/product/pdf/R/R46917

10. European Commission (2000-2013).
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D2295

11. European Commission (2013) *Press Release.*
Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_13_1166

12. Congressional Research Service (2021) U.S.-EU Privacy Shield and Transatlantic Data Flows.
Available at: https://crsreports.congress.gov/product/pdf/R/R46917

13. European Union Agency for Fundamental Rights and Council of Europe (*2018) Handbook on European data protection law.*
Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

14. European Commission (2010).
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087

15. European Commission (2016) Implementing Decision.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D2297

16. European Commission (2021) Standard Contractual Clause.
Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

17. European Commission (2017)*"Standard Contractual Clause".*
Available at: https://commission.europa.eu/funding-tenders/procedures-guidelines-tenders/data-protection-public-procurement-procedures_en#:~:text=A%20standard%20contractual%20clause%20guarantees,(EU)%202018%2F1725.

18. European Commission (2021) Standard Contractual Clause for international transfers.

Available at: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

19. European Parliament and of the Council (2021) Regulation on standard contractual clauses for the transfer of personal data to third countries. Available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en
20. Braun, M. et al. (2021) 'European Commission adopts and publishes new Standard Contractual Clauses for international transfers of personal data'. Available at: https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data
21. Horvath, Z. (2022) 'The New GDPR SCC Framework: What In-house Lawyers Must Do Today to Be Prepared' Available at: https://www.law.com/corpcounsel/2022/06/24/the-new-gdpr-scc-framework-what-in-house-lawyers-must-do-today-to-be-prepared/?slreturn=20231125140635
22. Cory, N., Dick, E. and Castro, D. (2020) 'The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade' Available at: https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade/
23. Overstraeten, T. and Church, P. (2021) 'EU: New Standard Contractual Clauses – From theory to practice' Available at: https://www.linklaters.com/nl-nl/insights/blogs/digilinks/2021/june/eu-new-standard-contractual-clauses-from-theory-to-practice

24. Prasad, V. and Dhawan A. (2023) '*Taking Personal Data Across Borders With Adequacy Decisions'*
Available at: https://www.mondaq.com/shareholders/1378700/taking-personal-data-across-borders-with-adequacy-decisions

25. Gungor, D. (2020) Cancellation of the "Privacy Shield" Agreement Regarding Data Transfers from the European Union to the USA.
Available at: https://www.mondaq.com/turkey/privacy-protection/989728/avrupa-birli287i39nden-abd39ye-yapilacak-veri-aktarimlarina-304li351kin-gizlilik-kalkani-anla351masinin-304ptali

26. Christhoper K.,Lee A B., and Christhoper D. (2021) Updated of Selected Articles, *Oxford University Press.*
Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839645

27. Kuner, C. (2020)'*Schrems II Re-Examined'*
Available at: https://verfassungsblog.de/schrems-ii-re-examined/

28. Gordon, P. Argento, Z., and Appenteng, K. (2021) 'The European Union's New Standardized Data Transfer Agreement: Implications for Multinational Employers'
Available at: https://www.littler.com/publication-press/publication/european-unions-new-standardized-data-transfer-agreement-implications

29. Compagnucci, M.C., Aboy, M., and Minssen, T. (2021)*'Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses'*
Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3951085

30. Lee, P. (2021) 'The updated standard contractual clauses — A new hope?'
Available at: https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/

31. CNIL (2021) ‘Data controllers: how to identify and process data transfers outside the EU?’
Available at: https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue

32. European Commission (2017) *Exchanging and Protection Personal Data in a Globalised World*.

33. CJEU (2015) *Research and documentation directorate.*
Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf
[Accessed September 2023].

34. Information Commissioner’s Office (2021) *International Transfers.*
Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

35. European Union Agency for Fundamental Rights and Council of Europe (2018) *Handbook on European data protection law.*
Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

36. CJEU (2018) *Adequacy Referential.*
Available at: https://ec.europa.eu/newsroom/article29/items/614108

37. BİLGİ Information Technology Law Institute (2020) Report of Data Flow.
Available at: https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf

38. European Commission (2016) Implementing Decision.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D2297

39. *European Commission (2017) "Standard Contractual Clause"*
Available at: https://commission.europa.eu/funding-tenders/procedures-guidelines-tenders/data-protection-public-procurement-procedures_en#:~:text=A%20standard%20contractual%20clause%20guarantees,(EU)%202018%2F1725

40. EPIC (2018) The High Court Commercial.
Available at: https://epic.org/documents/data-protection-commissioner-v-facebook-and-max-schrems-standard-contractual-clauses/

SUMMARY

This work ensures a comprehensive examination of the intricacies involved in cross-border transfers of personal data within the framework of the European Union's General Data Protection Regulation. The objective of the thesis is to examine the effectiveness of Standard Contractual Clauses as safeguard under the GDPR for transferring data across borders after the Schrems decisions.

The work evaluates the effectiveness of SCCs in ensuring GDPR compliance and identifies the legal and practical challenges organizations face in their implementation. The thesis contributes to academic and legal discourse on data protection and privacy laws, particularly in the context of transatlantic data flows. Employing analytical and comparative methods, it dissects the challenges and implementations of SCCs. Findings reveal complexities in SCCs' application, underscoring a need for clearer guidelines. Conclusively, it posits that despite hurdles, SCCs remain vital for GDPR compliance in international data transfers but require continuous adaptation to evolving legal landscapes.

Following the Schrems II ruling, it's crucial for companies to understand the data protection laws of the countries where they transfer data, focusing on areas highlighted by the decision like government data access and data subjects' legal rights. The European Commission's updated SCCs should be integrated into contracts and adapted to specific transfer situations. Companies should also implement additional measures like encryption and regular audits to meet EU standards. Ongoing assessment of the legal environment in recipient countries and maintaining transparency about data safeguards are essential. Legal professionals require continual education as data privacy rules evolve, and regulatory authorities should give updated guidance. Collaboration with non-governmental organizations can raise public awareness and transparency about data privacy.