Stockholms universitet

Privacy Enhancing Technologies

An analysis of implementing encryption and pseudonymization to ensure personal data protection during third-country transfers

Fatima Abdillahi Farah

Faculty of Law
Master Thesis 30 hp.
Subject: Legal Informatics
Spring Semester 2024
Supervisor: Samuel David Carey
Swedish Titel: Integritetsförbättrande teknologier – En analys av implementeringen av kryptering och pseudonymering för att säkerställa skyddet av personuppgifter vid tredjelandsöverföringar

Abstract

The question of third-country transfers reflects a balancing act between two interests: protecting the personal data that is being exported outside the EU and encouraging cross-border transfers. According to Article 45 of the General Data Protection Regulation (GDPR), the European Commission (Commission) can decide that a third country, a territory, a specific sector within a third country, or an international organization provides an adequate level of protection. In that case, a data exporter can transfer the personal data based on the adequacy decision without additional measures. Article 46 of the GDPR further states that a data exporter can rely on providing appropriate safeguards in the absence of an adequacy decision.

In just under five years, the Court of Justice of the European Union (CJEU) invalidated two U.S. adequacy decisions from the Commission. In both the Schrems I and II judgments, the CJEU criticized exemption rules in the adequacy decisions that made it possible for U.S. public authorities to interfere and access the personal data. According to the court, this posed a breach of the fundamental rights of data subjects granted in the Charter of Fundamental Rights of the European Union (Charter).

Furthermore, the CJEU stated in Schrems II that appropriate safeguards alone cannot protect personal data, particularly from the interference of public authorities, since they only provide contractual guarantees between the data exporter and data importer. If a data exporter wishes to transfer personal data to a third country, with domestic laws and practices that pose a risk to the rights of the data subjects, it is therefore required to implement supplementary measures alongside the appropriate safeguards. These supplementary measures can be either organizational or technical.

This thesis, which has examined Privacy Enhancing Technologies, finds that such technologies can form effective supplementary measures to the appropriate safeguards in *some* cases. More specifically, encryption is an effective supplementary measure for data exporters that transfer personal data to a third country for storage purposes. Furthermore, pseudonymization is an effective supplementary measure for third-country transfers for research and analysis purposes. However, there are more possible reasons why personal data is transferred to a third country and in which Privacy Enhancing Technologies are proven non-functional. More specifically, there is, as of yet, no Privacy Enhancing Technology that successfully grants protection for personal data transferred to a third country for support purposes. The reason for this is that such data must be visible to the recipient and Privacy Enhancing Technologies hinders visibility. The visibility of

personal data poses a threat to the rights of the data subjects, as national authorities in third countries have direct access to it if it is seized from the recipient. According to the CJEU, such access constitutes a breach of the rights granted in the Charter.

In the spirit of globalization, there is a wish for data exporters to transfer personal data to all corners of the planet. At the same time, they must ensure the protection of the personal data. It is therefore evident that controllers and processors who are engaged in third-country transfers of this sort need to be given clearer guidance on how to solve this balancing act.

List of abbreviations

BCR	Binding Corporate Rules
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Commission	European Commission
Convention	European Convention of Human Rights
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
DPD	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 (Data Protection Directive)
ECHR	European Court of Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity
E.O 12333	Executive Order 12333 – United States Intelligence Activities
EU	European Union
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Act
GDPR	Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
ICT	Information and Communication Technology
NSA	National Security Agency
OECD	The Organization for Economic Cooperation and Development
PPD-28	Presidential Policy Directive 28
SCC	Standard Contractual Clauses
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Table of content

1 Introduction

1.1 Background

As a result of a large majority of the world's population using the internet today, the amount of data created is almost infinite: around 328,77 million terabytes per day.[1] A big part of this data is personal data, which is defined as any information relating to an identified or identifiable natural person.[2]

The protection of personal data is firmly rooted in the European Union (EU) and can be found in multiple fundamental legal sources of EU law, such as Article 16 in the Treaty on the Functioning of the European Union (TFEU) and Article 8 in the Charter. With the introduction of the GDPR, the protection of personal data has been further strengthened. Among other things, higher demands are now placed on controllers and processors, and data subjects have more in-depth rights regarding how their data is being processed.

As mentioned earlier, high amounts of personal data are created and flowing around constantly. With the increasing use of digital services such as social media, and search engines, large amounts of personal data are transferred from the EU and the European Economic Area (EEA) to third countries. This has created a need for controllers and processors in the union to guarantee that these transfers happen in accordance with EU standards of personal data protection. To ensure that the protection of personal data guaranteed by the GDPR is not undermined during third-country transfers, Article 45 of the GDPR stipulates the requirement of an adequate level of protection. If the Commission believes that a third country, a specific territory or sector within a third country, or an international organization ensures an adequate level of protection, it can decide that such transfers of personal data can proceed without further authorization through an adequacy decision. As of today, there are 11 adequacy decisions from the Commission for various countries and territories such as Argentina, New Zealand, and the Isle of Man.[3] Since the U.S. is one of the most important trading and cooperation

[1] Duarte, Fabio, "*Amount of Data Created Daily (2024)*", Exploding Topics, 13 December 2023, Available at: https://explodingtopics.com/blog/data-generated-per-day, (Accessed 17 February 2024).

[2] Article 4.1 of the GDPR.

[3] European Commission, "*Commission finds that EU personal data flows can continue with 11 third countries and territories*", 15 January 2024, Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161, (Accessed 17 February 2024).

partners of the EU[4], an adequacy decision regarding transfers of personal data to the U.S. has been heavily discussed and processed. That has however turned out to be difficult to achieve.

The first U.S.-EU adequacy decision from the Commission, U.S.-EU Safe Harbour, was set in place in the year 2000 and contained several data protection principles to which companies had to self-certify their compliance.[5] The Safe Harbour framework was however declared invalid by the CJEU in the Schrems I judgment.[6] As a result of this invalidation, the Commission issued a new adequacy decision in 2016. The Privacy Shield Framework provided a legal mechanism that companies, through self-certification, could use for data transfers from the EU to the U.S.[7] However, this framework was also deemed insufficient by the CJEU in Schrems II.[8] In July of 2023, a new adequacy decision, EU-U.S. Data Privacy Framework, was presented.[9]

Regarding the above, it is clear that the U.S., and possibly other third-countries countries, have a hard time reaching an adequate level of protection that the EU requires for third countries. This is not surprising since the GDPR is the strongest framework globally when it comes to the collection and use of personal data.[10]

Recently, the use of different types of Privacy Enhancing Technologies has been discussed as a possible solution to what seems to be a never-ending saga of the CJEU invalidating the Commission's adequacy decisions for the U.S.[11] It is therefore of interest to consider if it is possible that the legal requirements in the GDPR and the Charter can be fulfilled by controllers and processors, who export personal data to third countries, implementing Privacy Enhancing Technologies as supplementary measures.

---

[4] European Commission, *"United States – EU trade relations with the United States. Facts, figure and latest developments",* No date, Available at: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en, (Accessed 25 February 2024).

[5] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

[6] Judgment of the Court (Grand Chamber) of 6 October 2015, Maximilian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 [cit. Schrems I].

[7] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

[8] Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems, C-311/18, ECLI:EU:C:2020:559 [cit. Schrems II].

[9] Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

[10] Council of the European Union, *"The General Data Protection Regulation"*, 11 January 2024, Available at: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/, (Accessed 14 May 2024).

[11] Aslak Juliussen, Bjorn, Kazory, Elisavet, Johansen, Dag & Petter Rui, Jon, *"The third country problem under the GDPR: enhancing protection of personal data transfers with technology"*, Oxford Academic, 19 July 2023, Available at: https://academic.oup.com/idpl/article/13/3/225/7226249, (Accessed 1 March 2024).

Suppose such technologies are successful in protecting the rights of data subjects and maintaining the EU standard for the protection of personal data. In that case, they might be the answer to further facilitating the globalization of today and the future.

1.2 Purpose and Research Question

The purpose of this thesis is to examine if data exporters can ensure compliance with the EU level of protection for personal data by successfully implementing Privacy Enhancing Technologies as supplementary measures during third-country transfers. By examining the legal requirements in the EU regarding personal data protection on one side, and the technological characteristics and abilities of certain Privacy Enhancing Technologies on the other side, the objective of the thesis is to link the two together and examine their compatibility.

The purpose of the thesis will be achieved by answering a number of research questions, which are reflected in each chapter in the main body of the thesis:

- What is the EU standard for the protection of personal data in the Charter and the GDPR?
- What are the legal requirements for third-country transfers of personal data?
- How do encryption and pseudonymization work?
- How can encryption and pseudonymization successfully be adopted as supplementary measures during third-country transfers to ensure an adequate level of protection?

1.3 Delimitations

As mentioned, the focus of the thesis is the use of Privacy Enhancing Technologies during third-country transfers of personal data. Some delimitations follow naturally from this focus, while others have been actively choices due to limited space and time frame.

Firstly, only Articles 5, 45, and 46 of the GDPR will be covered. The very objective of the GDPR is to lay down rules regarding the protection of data subjects concerning the processing of their personal data. Therefore, it would be too comprehensive to analyze all of the relevant articles to understand the standard for personal data protection therein. Since Article 5 contains several fundamental principles that controllers must adhere to, it is the only article in the GDPR that will be covered in the context of the first research question. Although the protection for personal data can be found in multiple legal sources in the EU and

was by no means revolutionary when the GDPR was introduced, it is the most comprehensive herein. The view on the protection of personal data in relevant articles in the Charter will only be assessed briefly to give an understanding of the primary law in the area. Furthermore, the phenomenon of third-country transfers is not dealt with in any other legal source but in Chapter 5 of the GDPR. The focus of the thesis being third-country transfers therefore leads to a natural choice of examining Articles 45 and 46 of the GDPR closely.

Moreover, the U.S. undeniably has had an intricate history with adequacy decisions from the Commission. However, a breakdown of the U.S. data protection laws and rulings will not take place. Since the focus of the thesis is on third-country transfers in general, an assessment of American law in the area would become too redundant. Nevertheless, the topic of an adequate level of protection often refers to the U.S., especially in Schrems I and II, and therefore some brief references to American data protection laws will occur.

Furthermore, Privacy Enhancing Technologies is a broad term that is defined as "a wide range of technologies that help protect personal privacy".[12] Thus, some delimitations regarding what type of technologies used in the thesis are required. Two different technologies will be used to achieve the purpose of the thesis: encryption, and pseudonymization. The reason for this is that these technologies already are mentioned in the GDPR which gives them credibility. Additionally, it should be mentioned that there are some Privacy Enhancing Technologies that do not fall into the scope of the GDPR at all. For example, data that has been anonymized is no longer considered personal data, since it is not relatable to an identified or identifiable natural person.[13] Since encryption and pseudonymization both fall into the scope of the GDPR, the use of them in the thesis is further confirmed.

Lastly, the thesis will only focus on third-country transfers of personal data for three different purposes: storage, research, and support. There are endless hypothetical reasons why a controller would want to transfer data to a third country but due to limited time and space, it is required to delimit the situations. Third-country transfers for storage, research, and support reasons have been specifically examined by the European Data Protection Board (EDPB) in the context of implementing Privacy Enhancing Technologies, making it particularly legitimate to address these in the thesis.

[12] OECD, *"Emerging Privacy Enhancing Technologies – Current Regulatory and Policy Approaches"*, OECD Digital Economy Papers, March 2023, Available at: https://www.oecd-ilibrary.org/docserver/bf121be4-en.pdf?expires=1715594818&id=id&accname=guest&checksum=DA4D55D5E9D92FAC062BDC7DCFFCAEE1, (Accessed 15 March 2024), p. 11.
[13] See Recital 26 of the GDPR.

1.4 Method and Material

Due to the thesis operating at the intersection of law and technology, it is only reasonable that the method of investigation reflects this dualism and possible tension.

The European legal method will be applied to the parts of the thesis that examine the current law in the area, and the legal informatics method will be used when examining how the technologies in question can be used as a tool to satisfy the current law. The methodology used in a thesis such as this one is vital in achieving its purpose and particularly reflects three topics: the cases used for the study, how the data is gathered, and how this data is analyzed.[14]

1.4.1 European Legal Method

As mentioned above, a European legal method will be used in the thesis. This method will mainly be used in the first part of the thesis, in which the EU standard for the protection of personal data will be examined. Much of the material used throughout the thesis are EU legal sources, and the European legal method will be applied both to describe and interpret the law in the area. In particular, the mutual relationship between different sources of law will be assessed, using this method to systemize the law.

The European legal method is substantially similar to the traditional legal dogmatic method, which is commonly found in academia. But since the legal sources differ in the EU, and EU law should be regarded as its own legal order[15], the European legal method is slightly different from the traditional legal dogmatic method. The differences between the two however do not regard the fundamental view of *how* the method is used in the thesis, but rather *what* selection of material is used. Although there is a lack of a unified definition, at its core legal dogmatics attempts to survey current law through interpreting different legal sources.[16] The legal dogmatic method and its purpose is a contentious topic, which can be explained through its vague description. However, the European legal method will be applied in the thesis in the following way: by having a concrete legal question as a starting point, current law will be used to build an answer to the questions asked. The research questions in the first part of the thesis is what the EU standard for the protection of personal data is and what the legal requirements for third-country transfers are. Arguably, this understanding of the legal dogmatic method will dictate how and what material is used to reach the answer to the asked question.

---

[14] Hjertstedt (2019), p. 167.

[15] This was established in Judgment of the Court of 5 February 1963. – NV Algemene Transporten Expeditie Onderneming van Gend & Loos v Netherklands Inland Revenue Adminstration, ECLI:EU:C:1963:1.

[16] Hjertstedt (2019), p. 167.

The legal system in the EU consists of a hierarchy of norms. This hierarchy can be described as a vertical order that is made up of primary law, secondary law, and supplementary sources.[17] I will proceed to explain what type of legal material falls under each of these three categories and how they will be used in this thesis.

The primary law used in this thesis will be the Charter, particularly Articles 7 and 8. While Article 8 explicitly deals with the protection of personal data, Article 7 does not specifically target this right. However, the CJEU has repeatedly linked the right to a private and family life to personal data protection. Therefore, these articles will grant a holistic perspective and be used as a foundation in the explanation of personal data protection in the EU. Additionally, the hierarchy of norms entails that the secondary law should be read in the light of the primary law. An active choice reflecting this has been made in the disposition of Chapter 2 of the thesis, namely in terms of relevant articles regarding personal data protection in the Charter being assessed before relevant articles in the GDPR. Through this, the Charter further acts as a foundation.

Furthermore, most of the thesis will revolve around secondary law, which in the EU mostly consists of regulations, directives, and decisions.[18] Considering the research questions and purpose of the thesis, articles 5, 45, and 46 of the GDPR will be particularly focused on. It is to be remembered that regulations such as the GDPR are binding legal acts, even though they fall under secondary law.[19] These articles are substantial in understanding the protection of personal data and will provide a further and more detailed understanding of this, compared to the primary law. Moreover, some of the 173 recitals of the GDPR will be used in the thesis to understand the legal framework regarding personal data protection. It is important to note that these recitals are not in themselves legally binding. However, they are useful in understanding the purpose of the articles in the GDPR and the will of the legislator.

Much of the thesis, particularly regarding the implementation of Privacy Enhancing Technologies during third-country transfers, will also be based on supplementary sources. The supplementary sources used are recommendations from the EDPB and the European Union Agency for Cybersecurity (ENISA). The EDPB is an independent organ that aims to achieve a uniform application of data protection laws in the EU. In addition to providing recommendations regarding the interpretation of GDPR, the EDPB advises the Commission on different matters.[20] This highlights their status within the union regarding data protection matters, which stems from their expertise in the area. The ENISA is an organization within the union that aims to increase cybersecurity within the EU. Recommendations from the EDPB and ENISA are not binding and do not have

[17] Hettne & Otken Eriksson (2011), p. 40.
[18] Ibid.
[19] Hettne & Otken Eriksson (2011), p. 42.
[20] Integritetsmyndigheten, *"Europeiska Dataskyddstyrelsen (EDPB)"*, 22 February 2022, Available at: https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-eu-niva/edbp/, (Accesssed 23 April 2024).

legal consequences if they are not followed.[21] However, they will offer guidance on interpreting the primary and secondary law.

Lastly, the position of case law in the EU legal norm must be evaluated since they will make up a part of the material used in the thesis. Decisions from the CJEU are supplementary sources.[22] However, the court has been given a responsibility to make sure that the interpretation and application of the primary law are correct, which gives the judgments a high value.[23] In the thesis, the judgments from the CJEU in Schrems I and II will be used to examine how the previously mentioned articles in the GDPR have been interpreted. Although the court uses different methods of interpretation, the CJEU particularly examines the aim and purpose of the primary and secondary law.[24] This is known as a teleological method of interpretation and simply seeks to achieve the objectives and meaning of the law. The aim of this is to ensure that the law is interpreted in accordance with what was intended at the time of its adoption.

By focusing on a teleological interpretation and the doctrine of *effet utile*, the court also strives for the law to be uniformly and effectively applied among the member states. Since EU treaties often are formulated in a general and policy-oriented way, a teleological approach is best suited for the court. Additionally, the legal multilingualism in the EU is a contributing factor to the above-mentioned. As a result of EU law being equal in authenticity in every language, it is merely impossible for the court to rely on a linguistic interpretation of a specific version. Thus, the court must see the law from a teleological point of view.[25] In the thesis, the doctrine of *effet utile* will be used to understand the interpretation and application of GDPR in Schrems I and II. Hence, the doctrine of *effet utile* will be used as a basic principle throughout the thesis when examining the protection of personal data in the EU, as well as the court's application of it.

Furthermore, it should be mentioned that the legal-dogmatic method, in which the European legal method used in the thesis has its roots, not only consists of charting out the current law. It is mentioned in doctrine that the method also includes an aspect of critical analysis of current law.[26] This critical perspective will mainly be used herein to dissect the advantages and disadvantages of the court's application and interpretation of the GDPR and the Commission's adequacy decisions.

Lastly, the criticism towards the court regarding judicial activism will be mentioned since it can lead to methodological issues in the thesis. This has been mentioned several times in doctrine and has its basis in the opinion that the court in

---

[21] See Article 288 of the TFEU.

[22] EUR-Lex, *"The non-written sources of European law – supplementary law",* 12 March 2018, Available at: https://eur-lex.europa.eu/EN/legal-content/summary/the-non-written-sources-of-european-law-supplementary-law.html, (Accessed 28 April 2024).

[23] Hettne & Otken Eriksson (2011), p. 49.

[24] European Parliament, *"The EU as a community of law – Overview of the role of law in the Union"*, March 2017, Available, at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599364/EPRS_BRI(2017)599364_EN.pdf, (Accessed 5 March 2024), p. 6.

[25] Ibid.

[26] Hjertstedt (2019), p. 167.

some cases engages in law-making, rather than law enforcement.[27] This is particularly relevant in the case of the court invalidating decisions from the Commission in Schrems I & II. In essence, the court invalidated one legal act (the Commission's adequacy decisions) by using another (the Charter and data protection laws). This indicates an inconsistency within the EU law, which can cause issues such as unpredictability when using an European legal method. This will be part of the critical aspects of the method, more specifically as a tool for examining how current law can be burdensome for third-country parties and place high requirements during transfers of personal data.

1.4.2 Legal Informatics Method

Furthermore, the method of legal informatics will be used in the thesis. Since this is a relatively new and unusual methodology in academia[28], a short explanation of legal informatics is required. Legal informatics can be described as a branch of the traditional legal science in which valid law (de lege lata) is analyzed. However, legal informatics goes beyond this by providing perspectives from informatics such as computer sciences, information security theory, and cognitive science.[29]

Legal informatics provides this perspective by studying the relationship between the law and technology, specifically Information and Communication Technology (ICT), in two ways. To start with, the method studies the legal regulation of ICT. Secondly, legal informatics studies how ICT can be used for legal purposes. By this, legal informatics can be explained as a two-way interaction: analyzing how technology affects society and how society affects technology.[30] The terminologies *rules* and *tools* can be used to further understand this two-way relationship between the law and the technology.[31] The legal regulation of technology is the rules, and the legal use of technology is the tools. In order to fully understand matters through the lens of the legal informatics method, the rules and the tools must both be considered and seen as a whole.[32]

The interaction between the law (rules) and technology (tools) is precisely what the thesis will examine. The interaction that will be analyzed is between the law, which will mainly consist of the GDPR but also the Charter, and Privacy Enhancing Technologies. Since the purpose of the thesis is to gain an understanding of how different Privacy Enhancing Technologies can be used to guarantee the protection of personal data during third-country transfers, most of the thesis will examine the effect that the law has on the technology. The EU legal source is the valid law (de lege lata) and the aim of the use of legal informatics as a methodology is to explain how de lege lata can be satisfied using technology. However, since the two perspectives mentioned above must be seen as a dynamic

[27] Reichel (2018), p. 131.
[28] Seipel (2004), p. 32.
[29] Greenstein (2021), p. 167.
[30] Greenstein (2021), p. 168.
[31] Siepel (2004), p. 33.
[32] Siepel (2004), p. 35.

whole in the legal informatics method, there will also be conclusions in the thesis that aim toward the effects that technology has on the law and society. For example, when discussing the possible challenges with the use of Privacy Enhancing Technologies, this second perspective comes into relevance. Therefore, the legal informatic method will be used in the thesis in two ways: to gain an understanding of how GDPR and other legal sources could affect Privacy Enhancing Technologies, and how such technologies can steer the law in a certain direction.

An issue that can arise during the interactions between law and technology is the different speeds at which the two progress. In particular, the ability of the law to keep up with the fast development of IT and its implementation society. According to Siepel, there are different views on the topic. Some may say that the law should lead and provide legal solutions in a prognostic and future-orientated manner. Others might interject with this view and argue that there could be a negative effect if the law and courts are at the forefront and possibly try to shape technology.[33] Since the focus of the thesis is to gain an understanding of how technology can be used as a tool to fulfill legal requirements, the rapid development of technology is seen as an advantage, especially in case it is determined that Privacy Enhancing Technologies can be used to increase the legal protection of personal data. However, the hasty development of IT compared to the slower development of the law can cause some difficulties. An example is the legal interpretation of technological terms. Privacy Enhancing Technologies not having a universal, legal definition is an example of possible methodological difficulties that can arise with the interaction of IT and law.

1.5 Outline of The Thesis

Since the research question requires two separate subjects, the current law on the area of personal data protection and the technological aspects of Privacy Enhancing Technologies, to be covered and later interconnected, a clear outline throughout the thesis is highly important. The dual characteristics of the thesis result in the chapters being relatively independent of each other, particularly chapters two and three versus chapter four. Therefore, the chapters will each contain an introduction and conclusion that will help the reader understand the chapters and navigate throughout the thesis. Furthermore, the conclusions will leave room for analytical elements.

The *first* chapter, which is now concluded, acts as an introduction. Herein, the topic for the thesis is presented, and the purpose and research question are explained. Following, the two methods used in the essay are presented. The different ways in which the European legal method and the method of legal informatics will be used are explained, as well as some methodological difficulties linked to the two.

[33] Siepel (2004), p. 42.

The *second* chapter will focus on the subject of the protection of personal data in the EU on a broader scale. In this chapter, Articles 7 and 8 in the Charter, which will provide the reader with a fundamental understanding of personal data protection within the EU, as well as the general principles relating to the processing of personal data in Article 5 of the GDPR are established.

The *third* chapter of the thesis acts as a continuation and extension of the second chapter, as it also examines the rules on the subject matter. However, it specifically focuses on the topic of third-country transfers of personal data. The different ways in which the GDPR allows for third-country transfers to occur are presented. The CJEU's decisions in Schrems I and II are also addressed, to help understand how the current law on the area is interpreted and applied by the court.

The third chapter puts an end to the examination of the *rules* in the area the *fourth* chapter proceeds to examine the *tools*: Privacy Enhancing Technologies. This chapter is solely descriptive and will cover encryption and pseudonymization. The purpose of this chapter is to give an understanding of how these different technologies work.

The *fifth* chapter aims to interconnect the law on the area and the characteristics of Privacy Enhancing Technologies by analyzing if and how the above-mentioned technologies can be used to increase the protection of personal data during third-country transfers. More specifically, the different Privacy Enhancing Technologies are applied in three situations in which personal data is transferred from the EU to a third country, examining their functionality.

The thesis will be finalized through a *sixth* chapter, in which the previous chapters will be concluded in final remarks and the research questions will be answered.

2 Personal Data Protection in the EU

2.1 Introduction

In this chapter of the thesis, which will be mapping out current law, the protection of personal data in the EU will be introduced. Since the overall aim of the thesis is to examine different technological solutions in which personal data can be protected during third-country transfers, it is essential to understand the nature of personal data protection as well as the underlying incentives behind it. Firstly, Articles 7 and 8 in the Charter will be explained. Since the Charter is a part of the primary law, it acts as a foundation of the subject. Following this, the secondary law will be presented. More specifically, the general principles of the processing of personal data in Article 5 of the GDPR will be laid out. These principles must be considered by controllers and processors during all processing of personal data and therefore act as a navigator in understanding the rights granted to data subjects during the processing of their data. Lastly, the chapter is summarized.

2.2 Articles 7 and 8 of the Charter

Firstly, it can be established that the rights, freedoms, and principles in the Charter should be recognized by the Union.[34] The rights granted in the Charter are therefore of importance when the EU law is applied and interpreted.

Traditionally, the protection of personal data has fallen under the right to respect for private and family life, which is expressed in Article 7 of the Charter. However, a more specific right to the protection of personal data was introduced through Article 8.[35] Article 7 of the Charter corresponds to Article 8 in the European Convention of Human Rights (Convention) as it has the same meaning and scope. The limitations mentioned in Article 8 of the Convention therefore also apply to Article 7 in the Charter. [36] According to Article 7 of the Charter, everyone has the right to respect for private and family life, home, and communications. The term private life is a broad concept that can not be exhaustively

[34] Article 6 of the Treaty on European Union (TEU).
[35] Frydlinger et al. (2018), p. 26.
[36] See Article 52.3 of the Charter.

defined.[37] However the article is aimed at protecting different private interests that citizens may have. As mentioned above, the right to protection of personal and sensitive data has historically been included in the right to respect for private life and has essentially been viewed as a sub-section of privacy interests.[38] However, the increasing importance of data protection and its economic character, resulted in personal data protection and the right to privacy being separated.[39] Notwithstanding this separation, protection of personal data is still viewed as closely linked to the right to respect for private life, and the two are often invoked together in courts.[40]

There is no corresponding provision to Article 8 of the Charter in the Convention, but the article has its basis in Article 8 of the Convention as well as 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 (DPD).[41]

Article 8 of the Charter grants individuals the right to protection of personal data concerning them. Individuals are also granted the right to have access to data concerning them, as well as having such data rectified. Apart from granting rights to data subjects, responsibilities are also imposed on the processor of the personal data. This includes the requirement for the data to be processed fairly, for specific purposes, and on the basis of the consent of the persons concerned or the law. These requirements have been inserted and developed further in Article 5 of the GDPR. Lastly, Article 8 of the Charter also requires compliance with these rules to be controlled by independent authorities.

2.3 An Overview of the Data Protection Principles in Article 5 of the GDPR

In order to understand the key rulings regarding the processing of personal data in current union law, it is important to mention Article 5 of the GDPR. In it, there are a number of principles that express fundamental requirements of how the processing of personal data should take place. Article 5 applies cumulatively alongside Article 6 of the GDPR, and thus they should be understood in a parallel manner. However, the two articles are slightly different in application – article 6 explains *if* the processing is lawful while Article 5, as mentioned above, explains *how* the processing should happen after it has been established that it is lawful

[37] Costello-Roberts v. the United Kingdom, Judgment of 25 March 1993, *European Court of Human Rights (ECHR)*, 13134/87.
[38] Leenes et al. (2017), p. 2.
[39] Leenes et al. (2017), p. 4.
[40] See for example Amann v. Switzerland, Judgment of 16 February 2000, *ECHR*, 27798/95, and Rotaru v. Romania, Judgment of 4 May 2000, ECHR, 28341/95.
[41] European Union Agency For Fundamental Rights, "EU Charter of Fundamental Rights", Available at: https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data, (Accessed 1 March 2024).

according to Article 6.[42] Furthermore, the principles mentioned in Article 5 are used as guidelines when interpreting other remaining articles of a more detailed kind in the regulation.[43]

Now back to the material content of Article 5, which as mentioned earlier, is vital in understanding the legal requirements put on controllers and processors while processing personal data. The first principle mentioned in the article is regarding *lawfulness*, *fairness*, *and transparency* in relation to the data subject. The term "lawfulness" is further explained in the recital of the GDPR, in which it is stated that processing only is lawful if it is based on the consent of the data subject, or other legitimate basis laid down by the Union or Member State law.[44] In addition to this, article 6.1 of the GDPR further mentions situations that result in lawfulness processing, which indicates the close link between articles 5.1a and 6.1. The term "transparency" in Article 5.1a requires that the data subject easily can access and understand information and communication related to the processing of their personal data. More specifically, the data subject should be aware of the risks, rules, and rights relating to their data.[45]

The next principle mentioned in Article 5 is regarding *purpose limitation*. In essence, this principle emphasizes the importance of the personal data being gathered and processed for specific, explicit, and legitimate purposes.[46] Firstly, this implies that the controller and processor, at an early stage of the collection of personal data
must consider and identify the purpose of the use of the data. The purpose of the collection must not only be identified by the controller but also documented and demonstratable.[47] It is not regulated exactly how precise the purpose should be specified as it depends on the context of a specific collection and its data, but it should be noted that vague descriptions of the purpose often are not deemed sufficient.[48] The specification of the purpose can, for example, be made through information to the data subject or public declarations.[49] Furthermore, the specific purpose must be explicit. This entails that the purpose must be clearly expressed in a comprehensive form, in order to be understood the same way by the data subject, controller, relevant authorities, and other involved actors.[50] In turn, this contributes to transparency and foreseeability. Lastly, the purpose of the collection must be legitimate. This is closely tied to Article 7 in the predecessor of the

---

[42] Michael Holtz (2018), p. 248.
[43] Michael Holtz (2018), p. 249.
[44] Recital 40 of the GDPR.
[45] Recital 39 of the GDPR.
[46] Magnusson Sjöberg (2021), p. 201.
[47] Article 29 Data Protection Working Party, "*Opinion 03/2013 on purpose limitation",* European Commission, 2 April 2013, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (Accessed 2 March 2024), p. 15.
[48] Ibid. p. 16.
[49] OECD, *"The OECD Privacy Framework"*, 2013, Available at: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (Accessed 9 March 2024), p. 57.
[50] Article 29 Data Protection Working Party, "*Opinion 03/2013 on purpose limitation",* European Commission, 2 April 2013, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (Accessed 2 March 2024), p. 17.

GDPR, the DPD. However, the requirement in Article 5.1b of the GDPR is broader than the exhaustive list in the article mentioned above. The current term "legitimate" refers to the purpose being in accordance with any law, both on primary and secondary levels.[51]

The following principle mentioned is *data minimization*. This requires the controller to limit the collection of personal data to what is adequate and relevant to the purpose. Thus, it is prohibited to process personal data that is not needed to reach the purpose. This principle is closely linked to the principle regarding purpose limitation and rarely becomes problematic for controllers since they often want to avoid dealing with personal data that is outside their fields.[52] However, data minimization can become an issue when it comes to big data due to the major risks of unnecessary personal data being collected and processed when large quantities of data are utilized.[53]

Furthermore, Article 5.1d compels the controller and processor to guarantee that personal data is *accurate* and updated. Personal data that is incorrect must be rectified as soon as possible to ensure that the information is accurate. In addition to the principle referring to facts being accurate, it also prohibits the processing of personal data that is subjective.[54] The principle of accuracy is also mirrored in Article 16 of the GDPR, which grants data subjects the right to rectification of personal data regarding him or her that is inaccurate.[55]

Another demand that is placed upon controllers and processors is *storage limitation*. This forbids personal data to be kept and processed for longer than what is necessary in relation to its purpose. In essence, this requires that the personal data is stored during a strictly minimal timeframe and is permanently deleted once the storage no longer fulfills its purpose.[56] The right to be forgotten, which is stated in Article 17 of the GDPR and was first coined in the Google Spain judgment,[57] is relevant in the context of storage limitation. If controllers comply with the principle and delete personal data that is no longer relevant in the eyes of Article 5.1e, the right to be forgotten follows naturally. The principle does however have some exceptions. In the cases of personal data being processed for archiving with public interest, science, or historical research purposes, it may be stored for longer. This is an example of a balance of interests between storage limitation and the right to be forgotten on one hand, and the right to access information on the other hand. By including the exceptions that have been mentioned above, these two interests coexist in the same principle.

The last principle mentioned in Article 5.1 is regarding *integrity* and *confidentiality*. This gives the controller and processor a responsibility to ensure that the

---

[51] Ibid, p. 20.
[52] Frydlinger et al. (2018), p. 39.
[53] Ibid.
[54] Ibid.
[55] Magnusson Sjöberg (2021), p. 202.
[56] Recital 30 of the GDPR.
[57] Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, ECLI:EU:C:2014:317.

personal data is protected against unauthorized or unlawful processing. The controller and processor also must protect the data from being subject to accidental loss, destruction, or damage. According to the article, different technical and organizational measures should be used to protect the integrity and confidentiality of personal data. The amount and characteristics of personal data are vital when determining the appropriate measures.[58]

2.4 Summary

Individuals' right to protection of their personal data is found in both primary and secondary law. Although Article 7 in the Charter is aimed at protecting the overall right to respect for private and family life, this often includes the protection of personal data. Furthermore, Article 8 specifies individuals' right to the protection of personal data concerning them. This confirms that personal data is viewed as a fundamental right within the Union and thus remaining EU law must be viewed, interpreted, and applied accordingly. Since the rulings in the primary law are not at a level of detail, the secondary law sets out requirements on exactly how personal data should be protected. Article 5 of the GDPR therefore sets the frame for how controllers and processors lawfully must handle personal data for the rights of the data subjects to be observed.

[58] Frydlinger et al. (2018), p. 41.

3 Third-country Transfers of Personal Data

3.1 Introduction

In the previous chapter, the overall regulatory framework regarding personal data protection in the EU was described. As the focus of the thesis lies in the protection of personal data specifically in the context of third-country transfers of personal data, this chapter will examine the regulatory framework that is applicable when personal data is exported outside the EU/EEA. Third-country transfers can take place in different ways. In the following chapter, the two main transfer tools will be covered: transfers based on an adequacy decision from the Commission and transfers that have been subject to appropriate safeguards taken by a controller or processor. In other words, Articles 45 and 46 of the GDPR will be explained. Following this, the questions presented in front of the CJEU and the assessment of them in Schrems I&II will be presented, to understand the interpretation and application of the subject matter.

The recitals of the GDPR state that two interests coexist in the legislation behind third-country transfers. On one hand, increasing globalization has led to a need for personal data to flow to and from the EU. This has been particularly necessary for the expansion of international trade and cooperation. On the other hand, there is a demand that the increase of such flow of personal data does not result in the protection ensured by the GDPR being undermined.[59] The rulings regarding third-country transfers are therefore to be described as a balance between encouraging cross-border transmissions and maintaining the EU standard of protection for data subjects.[60]

3.2 Transfers Based on Adequacy Decisions - Article 45 of the GDPR

Article 45 of the GDPR concerns third-country transfers based on adequacy decisions. Such decisions can be given to a third country, a territory, a specific sector within that third country, or an international organization. That can only take place after the Commission makes an overall assessment of the third country or

[59] Recital 101 of the GDPR.
[60] Frydlinger et al. (2018), p. 234.

organization in question. The adequacy decision is binding for all member states, which provides legal uniformity within the Union.[61] Article 45.2 of the GDPR mentions several elements that the Commission particularly takes into consideration when assessing if a third country has an adequate level of protection. This assessment is meant to mirror the fundamental values of the EU, especially the protection of human rights.[62]

The first topic in this assessment aims at the national laws of the third country.[63] For example, the legislation regarding national and public security, public authorities' access to personal data, and data protection laws are particularly relevant. Moreover, demands are placed on national authorities.[64] In addition to the third country being required to have one or several effectively and independently functioning supervisory authorities, they must also ensure compliance with data protection laws. According to the recitals of the GDPR, there are two major reasons for these requirements put on third-country authorities: to help data subjects exercise their rights and to cooperate with equivalent authorities in member states.[65] Lastly, the international commitments that the third country in question has entered are relevant in assessing the adequacy of the level of protection.[66] In particular, the Commission considers if the third country is part of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

If the Commission, after an overall assessment, decides an adequate level is ensured, transfers to the third country in question can take place without further measures taken by the controller or processor.[67] The adequacy decision must contain a mechanism for a periodic review of their functioning, which should take place every 4 years at a minimum.[68] The GDPR states that the review should consult with the third country in question for the EU to understand the ongoing relevant progress there.[69] If the Commission considers that a third country no longer provides the appropriate protection for personal data, the adequacy decision can be amended, revoked, or suspended. It should be noted that the general principles relating to the processing of personal data in Article 5.1 of the GDPR must still be complied with by the data exporter for such transfers to be lawful.

[61] Recital 103 of the GDPR.
[62] Recital 104 of the GDPR.
[63] Article 45.2a of the GDPR.
[64] Article 45.3b of the GDPR.
[65] Recital 104 of the GDPR.
[66] Article 45.3c of the GDPR
[67] Frydlinger et al. (2018), p. 236.
[68] Article 45.3 of the GDPR.
[69] Frydlinger et al. (2018), p. 237.

3.2.1 The CJEU´s invalidation of U.S. adequacy decisions – Schrems I & II

The topic of adequate level of protection in third countries was brought in front of the CJEU in 2015 and 2020. Although the court dealt with slightly different questions in the respective judgments, both Schrems I and II play a vital role in understanding how the relevant legal requirements for third-country transfers of personal data have been interpreted.

Schrems I

The judgment in Schrems I arose after Maximilian Schrems, an Austrian resident, made a complaint to the Irish Data Protection Commissioner. In the complaint, Schrems asked the Commissioner to prohibit Facebook Irland from transferring his personal data to Facebook Inc., located in the United States.[70] According to him, the law in the United States was insufficient in protecting personal data against surveillance by U.S. public authorities. Schrems used the revelations made by the whistleblower Edward Snowden regarding the activities of the American intelligence services as grounds for his claim.[71] The Commissioner took the opinion that he was not required to examine the matter and rejected the complaint. The CJEU however held that transfers of personal data from the EU to the United States serve necessary objectives in the public interest and therefore proceeded with the complaint.

Initially, the referring court asked if an adequacy decision issued by the Commission prevented a supervisory authority of a member state from examining a person's claim concerning the protection of their rights and freedoms during the processing of personal data relating to him in that third country.[72] The CJEU prohibited member states and their authorities from adopting measures that conflicted with such decisions.[73] However, the CJEU held that national supervisory authorities must be able to examine whether third-country transfers have complied with the requirements in the then-applicable DPD.[74]

The court further examined whether the U.S. adequacy decision at the time, *Safe-Harbor*, complied with the legal requirements in the DPD and Charter. At first, it was established that the DPD did not require a third country to ensure the level of protection guaranteed in the EU. The term "adequate level of protection" implied that it was sufficient for the country to ensure a level of protection of fundamental rights and freedoms that was equivalent to that guaranteed in the DPD and Charter.[75] When the Safe-Harbor principle was further examined, the CJEU made several conclusions. The court held that the system of

[70] Schrems I, para. 27.
[71] Schrems I, para. 28.
[72] Schrems I, para. 37.
[73] Schrems I, para. 52.
[74] Schrems I, para. 57.
[75] Schrems I, para. 73.

organizations self-certifying their adherence to the Safe-Harbor principles did not contravene the DPD. However, it was highlighted that third countries were required to establish effective detection and supervision mechanisms for infringements of the rules by the self-certifying companies.[76]

Moreover, the limitation of the applicability of the Safe-Harbor principles was criticized by the CJEU. According to the adequacy decision, the principles could be left without regard if it "was necessary to meet national security, public interest, or law requirements".[77] The court stated that the scope and application of such interferences with the fundamental rights in Article 7 and Article 8 of the Charter must be clear and precise. Above all, such restrictions must only be applied when strictly necessary.[78] Since the U.S. legislation authorized the storage of all personal data that had been transferred from the EU to the U.S. without making any differentiations, limitations, or exceptions, the CJEU held that it was not limited to what was strictly necessary. In particular, the limitation granted public authorities access to personal data information in election communications, which was regarded as a violation of the respect for private life granted in Article 7 of the Charter.[79]

In addition to this, the legislation did not provide any possibilities for individuals to pursue legal remedies to maintain their rights granted by EU legislation. Thus, the decision was deemed as not observing Article 47 of the Charter.[80] It should also be noted that the CJEU mentioned the fact that the Commission never stated that the United States ensured an adequate level of protection in the decision.

All these factors weighed together resulted in the CJEU ruling Article 1 of the adequacy decision, and therefore the whole of it, as invalid. Essentially, the CJEU held that the principles stated in Safe-Harbor did not comply with the DPD, read in the light of the Charter.

Schrems II

As a result of the invalidation of the first U.S. adequacy decision in Schrem I, a new decision was adopted. The new decision was named *Privacy Shield* and in it, the Commission addressed some of the remarks presented by the CJEU in Schrems I. Particilurarly the limitations and safeguards available in U.S. law were highlighted.

Simultaneously, Maximilian Schrems's original complaint was referred back to the Irish Commissioner. Since Facebook Ireland declared that the personal data that was transferred to the U.S. was based on a Standard Contractual Clauses (SCC) decision from the Commission, Schrems was asked to reformulate his claim. The main argument in his new complaint was that U.S. law required

[76] Schrems I, para. 81.
[77] Schrems I, para. 84.
[78] Schrems I, para. 92.
[79] Schrems I, para. 94.
[80] Schrems I, para. 95.

Facebook Inc. to share personal data with national authorities such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). According to Schrems, the manner in which these authorities used the data was incompatible with Articles 7, 8, and 47 of the Charter.[81] Schrems therefore argued that neither the SCC decision nor the Privacy Shield decision could be lawful grounds for transfers of personal data to the U.S.

The CJEU initially stated that the GDPR, and not the DPD, should be used for interpretation since a final decision had not been reached by the Commissioner before the directive was replaced by the regulation. Regarding the question of the level of protection required by Articles 46.1 and 46.2c of the GDPR during transfers of personal data to a third country, the CJEU made similar statements to the ones made in Schrems I. Although the third country in question could not be expected to offer the same protection guaranteed by the GDPR and Charter, the CJEU held that the rights, and legal remedies in a third country had to ensure that the data subjects were given an essentially equivalent level of protection.[82]

The CJEU went ahead and confirmed that the SCC decision in this case did offer adequate safeguards by fundamental rights and freedoms provided in the Charter.[83] However, it was held that such SCCs are only binding for the European controller and the recipient in the third country as they are parties to the contract, while authorities in the third country are not. Thus, the content of SCCs could be insufficient in ensuring protection from the interference of public authorities.[84] For these reasons, the CJEU stated that it may be necessary to add supplementary guarantees to SCCs to not undermine the level of protection granted by the GDPR, interpreted in the light of relevant articles in the Charter.[85] As for this specific SCC decision, the CJEU found that it provided effective mechanisms that ensured the suspension or prohibition of transfers that did not comply with clauses. Thus, the decision did not stand in conflict with Articles 7, 8, and 47 in the Charter.[86]

The last question that the CJEU had to answer was whether personal data transfers to the U.S. based on the Privacy Shield decision corresponded with Articles 7, 8, and 47 in the Charter or not. Identical to the Safe-Habor decision, this adequacy decision allowed its principles to be disregarded if it was deemed "necessary to meet national security, public interest, or law enforcement requirements".[87] The CJEU argued that the general character of this paragraph enabled U.S. public authorities to access and use personal data transferred from the EU, especially regarding surveillance programs.[88] According to the court, the

[81] Schrems II, para. 55.
[82] Schrems II, para. 105.
[83] Schrems II, para. 124.
[84] Schrems II, para. 126.
[85] Schrems II, para. 132.
[86] Schrems II, para. 148.
[87] Schrems II, para. 164.
[88] Schrems II, para. 165.

communication of personal data to a public authority or other third party was a breach of Articles 7 and 8 of the Charter, irrespective of the use of that information.[89]

The court proceeded to mention that the rights granted by Articles 7 and 8 in the Charter are not absolute. However, limitations may only be made if they are necessary and meet the objectives of the general interests recognized by the EU.[90] Any interference with the articles must be clear and precise in its application and scope. The CJEU found that multiple U.S. legal acts, on which many different surveillance- and monitoring programs were based, inferred the rights of the Charter. Neither Section 702 of the Foreign Intelligence Act (FISA), Executive Order 12333 (E.O 12333) nor Presidential Policy Directive 28 (PPD-28) were found to observe the minimum safeguards under Articles 7 and 8 of the Charter since they failed to limit interference to what was strictly necessary.[91] In addition to this, the CJEU found that the U.S. acts did not grant data subjects sufficient rights to bring proceedings against U.S. authorities in courts.[92] The court therefore ruled the U.S. as incapable of ensuring an essentially equivalent right to that guaranteed in Article 47 of the Charter.

The above-mentioned led the CJEU to rule that the Privacy Shield decision was incompatible with Article 45.1 of the GDPR, read in the light of Articles 7,8 and 46 of the Charter. With that, transfers of personal data from the EU to the U.S. could no longer be based on Privacy Shield.

3.3 Transfers subject to appropriate safeguards - Article 46 of the GDPR

In case of the absence of an adequacy decision, a controller or processor can transfer personal data to a third country by using another transfer tool: establishing appropriate safeguards in accordance with Article 46 of the GDPR. The purpose of such safeguards is to compensate for the lack of protection for data subjects in a third country. By establishing appropriate safeguards, controllers or processors can grant the data subjects rights that are comparable to those that are granted within the EU.[93] A control or processer must comply with the responsibilities stated in the GDPR when using appropriate safeguards.[94] In particular, the safeguards should relate to compliance with the general data protection principles mentioned in Article 5 of the GDPR and the principles of data

[89] Schrems II, para. 171.
[90] Schrems II, para. 174.
[91] Schrems II, para. 184.
[92] Schrems II, para. 192.
[93] Recital 108 of the GDPR.
[94] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, para. 4.

protection by design and by default. Moreover, the safeguards should ensure the right to effective legal remedies for the data subjects.[95]

One of the appropriate safeguards mentioned in Article 46 is Binding Corporate Rules (BCR).[96] These are defined as personal data protection policies used by a controller or processer in the union to a controller or processer in a third country within a group of undertakings or enterprises.[97] BCRs are mostly used by companies that are active both in and outside the EU/EES to ensure that the personal data that they process can flow lawfully and are approved by specific data protection authorities.[98]

Appropriate safeguards can also be incorporated by controllers and processors into contractual arrangements with parties in third countries through SCCs, which were discussed in both Schrems I&II. These clauses are approved by the Commission and are used by controllers and processors to demonstrate their compliance with the requirements for third-country transfers laid down by the GDPR. SCCs impose obligations on both the data importer and exporter. For instance, the data importer is required to keep documentation of the processing and inform the data exporter if they are unable to comply with the SCCs. On the other hand, the data exporter is required to suspend the transfer, or even terminate the contract, if the importer in the third country is unable to comply with or in breach of the clauses.[99] Furthermore, the SCCs also provide rules on liability and indemnification between the parties in case the data subject suffers material or non-material damage as a consequence of violations of their rights.

However, it is important to note that transfer tools that fall under Article 46, such as SCCs and BCR, do not function in a vacuum. As mentioned in Schrems II, SCCs are solely intended to grant the parties contractual guarantees during third-country transfer.[100] Since SCCs are uniformly applied, they do not consider the level of protection guaranteed in each third country separately. Therefore, the use of appropriate safeguards under Article 46 of the GDPR requires the controller or processor to verify if the law and practice of the third country ensure adequate protection on a case-by-case basis. Suppose an assessment reveals that the legislation and practice of the third country in question impinges on the effectiveness of the appropriate safeguards. In that case, the data exporter is required to use additional measures on top of the transfer tools in Article 46.[101]

When assessing if the transfer tools under Artice 46 are valid and function as effective mechanisms to ensure an adequate level of protection in practice, the EU data exporter must investigate both the specific circumstances of a transfer and different aspects of the legal system in the third country. Assessing the

---

[95] Ibid.

[96] See Article 47 of the GDPR.

[97] Article 4.20 of the GDPR.

[98] Frydlinger et al. (2018), p. 240.

[99] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, para. 17.

[100] Schrems II, para. 133.

[101] Recommendations 01/2020.

specific circumstances of the transfer includes looking into the purpose for which the data is being transferred, the sector in which the transfer occurs, the category of personal data that is being transferred, and the possibility that the personal data may be subject to further transfers to another third country. [102] Depending on the characteristics of each transfer, the SCCs and BCRs become either more or less valid and functioning. The assessment of the legal system of the third country includes the existence of comprehensive data protection laws and independent data protection authorities. Furthermore, if the laws and practices in the third country enable unnecessary and disproportional governmental interference and disregard of fundamental rights and freedoms granted in the Charter, they can not be viewed as compatible with transfer tools under Article 46.[103] In that case, the exporter of the personal data must either suspend the transfer or implement supplementary measures to avoid the risk of the protection granted in the union being undermined.[104]

3.4 Summary

The EU is faced with a constant balancing act between encouraging cross-border exchanges with third countries and ensuring that the protection of EU citizens' data is not undermined during this process. Over the past decade, this has become a conflict of interest which has led to different bodies within the union, namely the Commission and the CJEU, making different assessments.

It is clarified that the GDPR enables processors and controllers to transfer personal data to a third country based on two main procedures. Firstly, based on an adequacy decision adopted by the Commission, and secondly, through providing certain appropriate safeguards. The general principles in Article 5 of the GDPR must also be observed during third-country transfers, without exceptions.

The Schrems I&II cases manifested how the CJEU viewed the EU standard of protection of personal data in relation to third countries, particularly the regulatory frameworks in the U.S. Although Schrems I and II had slight differences, the CJEU invalidated both of the EU – U.S. adequacy decisions on essentially the same grounds: they stood in conflict with the fundamental rights granted in the Charter. This shows that is not enough that data protection principles and rules in secondary law are satisfied. Such principles and rules must be seen in a larger context of the primary union law. In other words, the GDPR must be seen as an extension of the fundamental values that are provided in the Charter. This is not a surprise since the hierarchy of norms in the EU leads to secondary law usually being viewed in light of primary law.

It can be questioned if the CJEU set the threshold too high in the Schrems cases. The right to respect of private and family life, an effective remedy, and a

[102] Recommendations 01/2020, para. 33.
[103] Recommendations 01/2020, para. 16.
[104] Recommendations 01/2020, para. 17.

fair trial were explicitly considered by the CJEU when the level of protection in the U.S. was being evaluated. Since national legislation was seen as an obstacle to this, the level of protection was regarded as deficient. In those same judgments, the CJEU expressed that it is not required by third countries to provide an identical level of protection of personal data as the EU and that it is sufficient that the protection is comparable. This statement by the court is reasonable considering that the EU has the strictest privacy and security laws regarding personal data globally, any other assessment would simply be unsustainable and make third-country transfers impossible. The question this raises is if the CJEU, in Schrems I & II, has not done exactly this.

All too strict judgments of the rules, both in primary and secondary law, regarding third-country transfers from the CJEU can have negative consequences for cross-border transfers as third countries would struggle to meet the requirements. On one hand, the court's strict interpretation of the union law gives the fundamental values of the EU a great impact. This is also in accordance with the aim and objective of the GDPR, which is to protect the fundamental rights and freedoms of natural persons. On the other hand, a strict interpretation leaves little room for considering discrepancies in different legislations.

However, there are additional possibilities to facilitate third-country transfers. In case of an absence of an adequacy decision, the data exporter in the EU can use transfer tools such as SCCs and BCRs as stated in Article 46 of the GDPR. Nonetheless, it is important to note that they do not function in a vacuum. The validity of such tools is based on both the circumstances of the transfer, and the domestic laws and practices in the third country. In case there are deficiencies, data exporters are required to set supplementary measures in combination with the transfer tools.

4 Privacy Enhancing Technologies

4.1 Introduction

The focus so far has been on relevant regulatory frameworks, both regarding the protection of personal data and the legal mechanisms of third-country transfers of personal data. In the chapters above, it has been concluded that the right to protection of personal data is deeply rooted in the EU and is stipulated in both primary and secondary law. Furthermore, Articles 45 and 46 of the GDPR provide the framework for the specific ways in which personal data can be transferred to third countries. The articles act as a balance between the legislator encouraging cross-border transfers and still maintaining the protection of the personal data that is transferred.

This chapter will present Privacy Enhancing Technologies. Understanding the technical aspects of Privacy Enhancing Technologies is essential to determine if and how they can be effective in ensuring the legal requirements and act as supplementary measures to the transfer tools mentioned under Article 46. Furthermore, this chapter will act as a descriptive supplement to chapter five.

Firstly, the somewhat broad definitions of Privacy Enhancing Technologies will be presented. Following this, the broadness of the term will be concretized by explaining a selection of two technologies: encryption and pseudonymization.

4.2 The definition of Privacy Enhancing Technologies

Although the concept of Privacy Enhancing Technologies is not new, there is a lack of a uniform definition.[105] The term is not defined at all in the GDPR. However, several definitions have been made over time to help increase the understanding and categorization of such technologies. In a report from the Organization for Economic Cooperation and Development (OECD), Privacy Enhancing Technologies was defined as follows:

[105] OECD, *"Emerging Privacy Enhancing Technologies – Current Regulatory and Policy Approaches"*, OECD Digital Economy Papers, March 2023, Available at: https://www.oecd-ilibrary.org/docserver/bf121be4-en.pdf?expires=1715594818&id=id&accname=guest&checksum=DA4D55D5E9D92FAC062BDC7DCFFCAEE1, (Accessed 15 March 2024), p. 10.

> *Privacy-enhancing technologies (PETs) commonly refer to a wide range of technologies that help protect personal privacy. Ranging from tools that provide anonymity to those that allow a user to choose if, when and under what circumstances personal information is disclosed, the use of privacy-enhancing technologies helps users make informed choices about privacy protection.*[106]

The ENISA has described Privacy Enhancing Technologies as technologies that *"can support privacy integration in systems and services"*.[107] Furthermore, the White House has defined Privacy Enhancing Technologies as: "… *a set of techniques and approaches that enable data sharing and analysis among participating parties while maintaining disassociability and confidentiality"*.[108]

Although these definitions are slightly different, they indicate that Privacy Enhancing Technologies is a category of technologies with certain characteristics. The are multiple explanations for the different definitions of the term Privacy Enhancing Technology. On one hand, the differences reflect the state of technological development at a given time and on the other hand, the context in which they are used.[109] Essentially, a "one size fits all" definition of the term is difficult to achieve as it must be tailored to the specific context.

Although there are many different understandings of what Privacy Enhancing Technologies are, they are all surrounded by the concept of information privacy. Therefore, it is of use to explain what information privacy is. Similar to Privacy Enhancing Technologies, information privacy can be defined in many different ways. At its core, the term can be described as a person's ability to control information regarding oneself.[110] Regarding information privacy of personal data, it can therefore be understood that the term emphasizes the right to control information that relates to oneself as an identified or identifiable living individual, such as name, home- or email address, and personal identity number.

The definition of Privacy Enhancing Technologies can thus be described as technological solutions that aim to grant natural persons privacy and control over their information. When personal data is being processed, the aim of using Privacy Enhancing Technologies is mainly for controllers and processors to have control over the rights of the data subjects not being violated, as they are responsible for complying with GDPR.

---

106 Ibid, p. 4.
107 Enisa, *"Promoting Data Protection by Design: Exploring Techniques"*, 27 January 2022, Available at: https://www.enisa.europa.eu/news/enisa-news/promoting-data-protection-by-design-exploring-techniques, (Accessed 1 April 2024).
108 Federal Register – The Daily Journal of the United States Government, *"Request for Information on Advancing Privacy-Enhancing Technologies",* 6 September 2022, Available at: https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, (Accessed 23 April 2024).
109 OECD, *"Emerging Privacy Enhancing Technologies – Current Regulatory and Policy Approaches"*, OECD Digital Economy Papers, March 2023, Available at: https://www.oecd-ilibrary.org/science-and-technology/emerging-privacy-enhancing-technologies_bf121be4-en, (Accessed 15 March 2024), p. 10.
110 Belanger & Crossler (2011), p. 1018.

4.3 The technology behind two different types of Privacy Enhancing Technologies

4.3.1 Encryption

The first documentation of cryptography dates to 1900 BC in Egypt, in which messages were hidden using a substitution cipher. This was done simply by replacing each letter in plain text with another letter of the alphabet. Since only the sender and recipient had knowledge of which letters replaced each other, the recipient could later convert the ciphertext to the original plain text and therefore reveal the information.[111] Another famous ancient method of encryption is the so-called Caesar cipher, named after the Roman general and statesman Julius Caesar. In Ceasar cipher, every letter in the plain text was moved a specific number of steps in the alphabet in order to hide the original message, and similarly to the Egyptian substitution cipher, only the sender and recipient knew the number of steps every letter needed to be moved in order to reveal the original message.[112]

Over time, cryptography has changed form, from being based on traditional pen-and-paper encryption techniques to modern encryption techniques using computers. Regardless of the different techniques in history, encryption still works the same. Modern-day encryption refers to a mathematical procedure in which clear information, usually text, is converted into a code using a key. The correct key must be used for the information to become clear and readable again.[113] Thus, encrypting data protects the information against unauthorized third parties intercepting and having access to it.

Encryption is mentioned in the GDPR as one of the appropriate technical measures that should be used by controllers and processors to ensure the security of personal data. According to Article 32 of the GDPR, the use of encryption is dependent on the context of specific processing and its risk. This requires the controller and processor to, among other things, assess the art of the processing and the cost of the implementation of encryption. Processing personal data that has a high risk of threatening the rights and freedoms of natural persons is an example of a factor that indicates that the controller and processor are required to implement appropriate technical measures such as encryption.

Modern-day encryption is usually divided into two different types: symmetric encryption and asymmetric encryption. Although the two serve the same purpose, which is to protect information from the interception of unauthorized parties, the two methods differ in their approach.

---

[111] Morkel, T & Eloff, JHP *"Encryption techniques: A Timeline Approach"*, Available at: https://digifors.cs.up.ac.za/issa/2004/Proceedings/Research/062.pdf, No date, (Accessed 15 March 2024), p. 4.

[112] Magnusson Sjöberg (2021), p. 84.

[113] Intersoft Consulting, *"Encryption"*, Available at: https://gdpr-info.eu/issues/encryption/ (Accessed 12 March 2024).

Symmetric encryption

Symmetric encryption is the version of encryption in which the key used to encrypt the original plain text to the cyphertext is the same as the one used to decrypt the cipher text to the plain text.[114] The term "key" is a collective name for the information that is used to encrypt and decrypt the message. In the example mentioned above with the Egyptian substitution cipher and the Ceaser cipher, the key is simply the information of which letter substitutes which or how many steps each letter should be moved to reveal the plain text. Such keys are relatively easy to break since it only takes statistical analysis to understand the system. The symmetric encryptions used today are far more advanced and difficult to break since the key usually represents a random sequence of digits based on mathematical algorithms.[115] There are several different algorithms for symmetric encryption that are used today and the longer the string of digits is, the harder it is to break the encryption.

There are both advantages and disadvantages of using symmetric encryption to protect information from being accessed by unauthorized parties. The advantages include the fact that the symmetric keys are often short, which facilitates and quickens the process of encrypting the plain text. Furthermore, there are possibilities for compiling different keys on top of each other to gain stronger ciphers and therefore better protection. One major disadvantage of symmetric encryption is that the key must be kept secret by both the sender and the recipient, which leads to an increased responsibility on both ends and an increased risk of disclosure of the key.[116]

Asymmetric encryption

Asymmetric encryption, also known as public key encryption, is the second type of encryption and can be described as a more intricate version of symmetric encryption. Instead of using only one key, two different keys are used. The key used to encrypt the plain text into cipher text is public and usually found on the internet, which means anyone who wants to send cipher text to a recipient can encrypt it using the key. However, the key used to decrypt the cipher text into plain text again is secret and once the information is encrypted by the sender, only the recipient can decrypt it into the original plain text.[117] Similar to symmetric encryption, several different algorithms can be used with the secret key. The method is

---

[114] Ubaidullah Bokhari, Mohammed & Makki Shallal, Qahtan, "*A Review on Symmetric Key Encryption Techniques in Cryptography",* ResearchGate*,* August 2016, Available at: https://www.researchgate.net/publication/333118027_A_Review_on_Symmetric_Key_Encryption_Techniques_in_Cryptography, (Accessed 2 April 2024), p. 44.

[115] Ibid.

[116] Ibid, p. 47.

[117] Humadi, Ahmed, "*Encryption*", ResearchGate, 8 December 2020, Available at: https://www.researchgate.net/publication/347301480_enycryption, (Accessed: 4 April), p. 4.

often used for communication on the internet, for example between one of many clients and a server model belonging to a company.[118]

As mentioned above, symmetrical encryption carries a high risk of disclosure since both the sender and the recipient must keep the key secret. This is not an issue regarding asymmetric encryption, as only the recipient has access to the secret key. It can thus be argued that asymmetric encryption provides better security. On the other hand, asymmetric encryption is a longer and more complicated process since two corresponding keys must be created and used.[119] This also leads to higher costs and knowledge requirements for a party that wishes to implement asymmetric encryption.

4.3.2 Pseudonymization

Unlike encryption, pseudonymization is explicitly defined in the GDPR. In it, the procedure is described as:

> *The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*[120]

During the process of pseudonymization, the original data is used as the input in a system. The system then converts the original data into two different outputs: pseudonymized data and additional information. The two data sets do not function separately and must be added together to reveal the original data.[121]

This process can be further explained to facilitate the understanding of it. Let us say that a company that provides music streaming services implements pseudonymization to protect the personal data of the users. This will result in the company having two different databases. Database 1 contains pseudonyms, which consist of something that is not directly assignable to the individual, such as a series of numbers or letters. Alongside the pseudonyms, database 1 contains the services that each person behind the pseudonyms is subscribed to. Database 2 on the other hand consists of the full names of the subscribers alongside the pseudonym that is attributed to each individual. The personal data can only be attributed to a specific person if one has access to Database 2, In other words, both database 1 and 2 must be available to a third party for the pseudonymization

---

[118] Ibid.

[119] Keyfactor, *"When to use symmetric encryption vs. asymmetric encryption"*, 17 June 2020, Available at: https://www.keyfactor.com/blog/symmetric-vs-asymmetric-encryption/. (Accessed 1 April 2023).

[120] Article 4.5 of the GDPR.

[121] Information Commissioners Office, *"Chapter 3: Pseudonymisation – Draft anonymization, pseudonymization and privacy enhancing technologies guidance"*, February 2022, Available at: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. (Accessed 2 April 2024), p. 3.

to break and the personal data to be attributed to a specific person, making the personal data more protected.

Database 1:

Account holder	**Account type**
Person 1222	Free trial
Person 1223	Silver package
Person 1224	Golden package

Database 2:

Account holder	**Pseudonym**
Emma Smith, 1978-08-03	Person 1222
Jacob Lee, 1994-12-23	Person 1223
Sam Davis, 1985-06-15	Person 1224

Database 1 and 2 combined reveal that:

Person 1222 is named Emma Smith, was born August 3rd 1978, and has a free trial subscription.
Person 1223 is named Jacob Lee, was born on December 23rd 1994 and has a silver package subscription.
Person 1224 is named Sam Davis, was born on June 15th 1985, and has a golden package subscription.

It is important to note that According to Article 4.5 of the GDPR, the additional information, which in this case is Database 2, is required to be kept separate and protected. If not, there is a risk that a third party gets hold of the additional information and attribute the personal data to a specific person. The company must therefore implement technical and organizational measures to guarantee that the additional information is kept hidden, as well as keep it separate.

Lastly, it is important to note that pseudonymization should be separated from anonymization. Since the process of anonymization results in the information not being identified or identifiable to a natural person, it is no longer defined as personal data and consequently falls outside of the scope of the GDPR.[122] However, pseudonymization still keeps the information as personal data and thus falls under the scope of the GDPR.

4.3.3 Encryption vs Pseudonymization – Key Differences

It can be established that encryption and pseudonymization, although both fall under the definition of Privacy Enhancing Technologies, have differences.

After assessing the characteristics of encryption and pseudonymization, it is clear that the two technologies operate differently. While pseudonymization

[122] See the definition of "personal data" in Article 4.1 of the GDPR and Recital 26 of the GDPR.

anonymizes data by replacing its original form with pseudonyms, encryption makes the data confidential by making it physically difficult for unauthorized parties to access it. In other words, the process of pseudonymization aims to convert personal data into a form in which it cannot be linked to a specific person whereas encryption locks the personal data up and prevents any kind of access by an unauthorized party.

These characteristics result in different possibilities for data accessibility. Since pseudonymization does not hide all of the information but rather converts the parts that are considered personal data into pseudonyms, it allows for the data to still be used by a broader audience for different purposes, such as analytical or operational ones.[123] It is however difficult, if not impossible, for encrypted data to be used for analytical, statistical, or operational since such data must be decrypted first to be available to anyone other than the sender and recipient. Furthermore, the two technologies can be combined for further protection. As mentioned above, the GDPR requires that the additional information in the case of pseudonymization is subject to technical and organizational measures. Accordingly, the additional information be encrypted and therefore further strengthen the prevention of unauthorized access.[124]

4.4 Summary

The term Privacy Enhancing Technologies does not have one single definition but is rather a collective term for different technologies that aim to protect the privacy of information. Encryption and Pseudonomyzation are mentioned in the GDPR as ways of protecting personal data. Given the fact that they both fall under the term Privacy Enhancing Technology, it is evident that they aim to grant security and confidentiality to personal data. However, the two technologies operate in a completely different manner and provide different types of possibilities.

Both symmetrical and asymmetrical encryption utilize a key, which usually consists of mathematical algorithms, to encrypt and decrypt the data. In comparison to asymmetrical encryption, symmetrical encryption provides slightly less protection. The reason for this is that the protection is dependent on two, often independent, parties being responsible for the same key. Logically, a system that requires two parties to keep a secret is more likely to fail than one that is dependent on only one party making sure of confidentiality. Asymmetrical encryption provides stronger protection since two different keys are used to encrypt and decrypt the data. Moreover, as a result of the data being locked in, encryption does not facilitate data accessibility to a high extent.

---

[123] Richman, Amitai, "*Pseudonymization vs Encryption: Understanding the differences"*, k2view, 7 June 2023, Available at: https://www.k2view.com/blog/pseudonymization-vs-encryption/#How-Pseudonymization-Works-Preserving-Privacy-Through-Data-Anonymization. (Accessed 8 April 2024).

[124] Cloudflare, *"What is pseudonymization",* No date, Available at: https://www.cloudflare.com/learning/privacy/what-is-pseudonymization/. (Accessed 3 April 2024).

Pseudonomyzation does not work in the same way as encryption since it is not based on locking the personal data but rather altering the form of some parts of it. For personal data to be sufficiently protected, pseudonymization is also dependent on the additional information that enables the personal data to be attributed to a specific person to be kept secret and separate. If the additional information is not properly guarded, unauthorized parties can break the pseudonymization and access the personal data.

Encryption and Pseudonomyzation have different strengths and weaknesses when it comes to their ability to protect personal data. It is however important to note that these technologies do not exclude one another and that the two can be used in combination to grant the best possible protection. For example, the additional information to pseudonymized data can be encrypted.

5 Adopting Privacy Enhancing Technologies as supplementary measure during third country transfers

5.1 Introduction

In the previous chapter, the technical characteristics and mechanisms of Privacy Enhancing Technologies were described. This chapter will still move in the area of Privacy Enhancing Technologies but apply them in practice rather than only describing them. By establishing the functionality of encryption and pseudonymization, this chapter aims to answer the main question of the thesis: if and how controllers based in the EU can implement different Privacy Enhancing Technologies to ensure that the rights of data subjects are not undermined. Firstly, two principles in the GDPR that suggest that controllers implement Privacy Enhancing Technologies will be presented. Secondly, three situations where personal data from the EU is exported to a third country will be illustrated: storage, research, and support. These different scenarios are then used to conclude whether, and if so which, Privacy Enhancing Technology is able to achieve the objective of protecting the rights of the data subjects. Lastly, some of the risks and challenges of using Privacy Enhancing Technologies will be assessed.

5.2 Reasons for adopting Privacy Enhancing Technologies

The implementation of Privacy Enhancing Technologies is linked to multiple concepts in current data protection regulation. In other words, there are already existing incentives in the GDPR for data controllers and processors to implement Privacy Enhancing Technologies as proactive methods of compliance.[125]

5.2.1 Data Privacy by Design

The principle of data protection by design is mentioned in Article 25.1 of the GDPR and describes the implementation of technical and organizational

[125] Magnusson Sjöberg (2021), p. 213.

measures as a way of complying with data protection principles such as data minimization. The principle specifically refers to processors and controllers implementing measures at an early stage of the design of IT systems and applications to encourage the protection of personal data.[126] The requirement of "building" in the implementation of data protection in systems and applications differs from case to case. Before implementing appropriate technical and organizational measures the controller should take several factors into account, such as the implementation costs and the nature of the processing.[127]

It is important to note that the principle of data privacy by design is not only directed at controllers implementing certain measures but also at the producers of the applications, services, and products that are used to process personal data.[128] That way, producers are encouraged to ensure that controllers and processors can comply with data protection laws and policies. The implementation of Privacy Enhancing Technologies is a way to adhere to the requirement of data protection by design.[129] As mentioned, the principle of data protection by design is focused on technical and organizational measures being implemented at an early stage. In the context of third-country transfers, this implies that Privacy Enhancing Technologies should be implemented in the systems even before the personal data leaves the EU.

5.2.2 The Principle of Accountability

Furthermore, implementing Privacy Enhancing Technologies is a means for controllers and processors to comply with the principle of accountability.[130] The principle of accountability is established in Article 5.2 of the GDPR. It is directly linked to the general principles of processing personal data in Article 5.1 of the GDPR, as it states that controllers are responsible for complying with the general principles relating to the processing of personal data. Furthermore, the principle of accountability requires controllers to be able to demonstrate compliance.[131] In essence, the principle of accountability acts as a burden of proof of controllers. In case of a dispute between a data subject and a controller, it is not the responsibility of the data subject to show that there has been a breach of the GDPR. Rather, the responsibility is placed on the controller to prove that they have complied with the regulation.[132]

---

126 Magnusson Sjöberg (2021), p. 213.
127 See Article 25.1 of the GDPR.
128 Recital 78 of the GDPR.
129 Enisa, *"Promoting Data Protection by Design: Exploring Techniques"*, 27 January 2022, Available at: https://www.enisa.europa.eu/news/enisa-news/promoting-data-protection-by-design-exploring-techniques, (Accessed 1 April 2024).
130 Wiewiórowski, Wojciech, *"Accountability needs technology"*, European Data Protection Supervisor, 8 September 2016, Available at: https://www-edps-europa-eu.translate.goog/press-publications/press-news/blog/accountability-needs-technology_en?_x_tr_sl=en&_x_tr_tl=sv&_x_tr_hl=sv&_x_tr_pto=sc, (Accessed 17 April).
131 Article 5.2 of the GDPR.
132 Frydliger et al. (2018), p. 42.

The principle of accountability is particularly relevant when it comes to the right to protection of personal data since it is an "active" right.[133] This means that the very nature of the right to protection of personal data entails that controllers are constantly obligated to ensure that it is complied with. Controllers also have a constant obligation to demonstrate their methods of approach, which is a clear example of the objectives of the principle of accountability.

As mentioned above, the principle of accountability establishes that controllers must ensure and demonstrate compliance with the general principles relating to the processing of personal data, but it does not mention *how* controllers could or should show accountability. Therefore, the principle can be satisfied in several ways. Among other things, accountability is connected to documentation.[134] If a controller implements extensive documentation around their processing of personal data, it is easier to establish compliance with the principles in Article 5.1 of the GDPR. Similarly, controllers can ensure compliance with the principle of accountability by implementing technical measures, such as encryption and pseudonymization, since it facilitates an active maintenance of the protection of personal data.[135]

5.3 Implementing Privacy Enhancing Technologies

It has been established that the EU has a legitimate interest in the protection of personal data not being undermined during third-country transfers.[136] As the CJEU mentioned in Schrems II, there is an evident risk of authorities in third countries accessing personal data. According to the CJEU, the risk of public authorities in third countries identifying data subjects and gaining information about them imposes a significant risk on the rights of union members.[137]

Moreover, it has been established that supplementary measures, such as different Privacy Enhancing Technologies, must be implemented when a controller uses appropriate safeguards under Article 46 of the GDPR and the domestic laws and practices in the third country reduce the efficiency of those transfer tools.[138]

In order to understand if the implementation of Privacy Enhancing Technologies is successful in ensuring personal data protection, and if so, which specific ones are the most suitable under certain circumstances, the different reasons why a data exporter based in the EU would transfer personal data to a third country must be assessed. The reason for this is that different purposes for third-country transfers require the data to be handled differently, and consequently, different risks are actualized.

---

133 Recommendations 01/2020, para. 9.
134 Frydliger et al. (2018), p. 42.
135 Recommendations 01/2020, para. 9.
136 See under Chapter 3.4.
137 Schrems II, para. 171.
138 See under Chapter 3.3.

5.3.1 Third-country transfers for storage purposes

Data exporters that are based in the EU could wish to transfer personal data to a third country for storage purposes. This situation is relevant for example when controllers use a web hosting service provider that is based in a third country to back up data and not lose it.[139] Web hosting service providers are companies that offer a range of different services to clients, such as connectivity to the World Wide Web, the design of websites, and storage space. [140] When a controller uses the storage space service of a web hosting provider based in a third country, there is a risk of the public authorities of that country accessing the personal data. This can happen either by the authorities directly confiscating the data or by requiring the web hosting service provider to give them access to it.[141] Either way, this situation imposes a possible threat against the rights of the data subjects.

A recipient that only stores personal data, such as a web hosting service provider, does not need the personal data in clear. This means that the recipient can fulfill its responsibility towards the exporter without actually seeing the personal data. Since it is possible to store data that has not been disclosed or is visible to the recipient, the data can be encrypted.[142] For that reason, the EDPB has stated that is suitable for the controller to encrypt the personal data before transferring it to the recipient in the third country that will store it.[143] To ensure that the personal data is not accessible to unauthorized parties such as public authorities in the third country, it can be understood that it should be encrypted into cipher text during the transmission outside of the EU as well as stay encrypted while it is stored.

Furthermore, the controller must ensure that the encryption used is strong before it is exported to a third country for storage purposes. This is done by, for example, using algorithms with long key lengths and properly storing and managing the keys. The controllers should also consider how long the personal data is being stored in the third country.[144]

5.3.2 Third-country transfers for research purposes

A controller based in the EU may also need to transfer data, which contains personal data, to a third country for research purposes. For example, this may be the case in clinical trials, if a clinical research company based in the EU/EEA

[139] Recommendations 01/2020, para. 30.
[140] See the definition in Google Domains Help, *"About hosting providers"*, available at: https://support.google.com/domains/answer/3288265?hl=en, (Accessed 17 April 2024).
[141] Recommendations 01/2020, para. 29.
[142] OECD, *"Emerging Privacy Enhancing Technologies – Current Regulatory and Policy Approaches"*, OECD Digital Economy Papers, March 2023, Available at: https://www.oecd-ilibrary.org/docserver/bf121be4-en.pdf?expires=1715594818&id=id&accname=guest&checksum=DA4D55D5E9D92FAC062BDC7DCFFCAEE1, (Accessed 15 March 2024), p. 19.
[143] Recommendations 01/2020, para. 30.
[144] Ibid.

needs the expert knowledge or tools of a similar company in a third country.[145] Similar to the case of personal data that is transferred to a third country for storage purposes, this sort of transmission to third countries can pose threats to the rights of the data subjects. Namely by the personal data being accessed by authorities there. This can be done either by the authorities in the third country acquiring the personal data directly or commanding the recipient to hand over it.[146] Therefore, it is the responsibility of the controller to ensure that the protection of personal data, for example in the context of a clinical trial, is not undermined.[147]

Since the recipient in this case does not need the personal data in clear to achieve the objectives of the transfer, which is to conduct research and analyze the data, the EDPB has considered pseudonymization as an effective technical measure that the exporter can utilize to protect the personal data.[148] Encrypting personal data would not work in this case since encrypted data is locked up in that format until it is decrypted. Therefore, pseudonymization is the most optimal Privacy Enhancing Technology for analytical, statistical, or operational purposes unless it is decrypted first.[149]

However, it must be noted that pseudonymization only can provide effective protection if the exporter can ensure that the additional information is kept separate from the pseudonymized data and only is accessible to reliable parties.[150] If not, there is a risk that the pseudonymized data is traceable to an identified or identifiable party, thus violating the rights of the data subject.[151] Furthermore, the data exporter must in this case implement suitable organizational and technical measures for the additional information. This is an additional step that is not required in the case of encrypting personal data that is transferred to a third country for storage reasons, which makes this case more intricate.

5.3.3 Third-country transfers for support purposes

Lastly, there may be cases where controllers that are based in the EU/EEA transfer data to third countries for technical support. There has been an increase in companies in different sectors outsourcing or wanting to outsource their IT services, such as technical assistance for customers, to developing countries in

---

[145] Liss, Joseph, Peloquin, David, Bernes, Mark & Bierer E Barbara, *"Demystifying Schrems II for the cross-border transfer of clinical research data*, Oxford Academic, 23 October 2021, Available at: https://academic.oup.com/jlb/article/8/2/lsab032/6407729?itm_medium=sidebar&itm_source=trendmd-widget&itm_campaign=Journal_of_Law_and_the_Biosciences&itm_content=Journal_of_Law_and_the_Biosciences_0, (Accessed 20 April 2024).

[146] Recommendations 01/2020, para. 29.

[147] European Commission , "*Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation",* No date, Available at: https://health.ec.europa.eu/document/download/c3042973-b36d-4094-a1fb-a6fc980f065e_en, (Accessed 19 April 2024).

[148] Recommendations 01/2020, para. 31.

[149] See under Chapter 4.3.3.

[150] Ibid.

[151] See under Chapter 4.3.2.

recent years.[152] For example, studies have shown that a majority, over 60%, of French companies are planning on outsourcing IT services to French-speaking countries in Africa. The main driving force for this is cost efficiency, improving the quality of the service, and focusing on the core of the business.[153] Another example is Germany, where studies have shown that as much as 72% of German organizations plan to outsource parts of their operations.[154] The increase in outsourcing of IT services such as technical support and assistance will undoubtedly result in personal data leaving the EU/EEA to third countries without an adequate decision from the Commission. For example, there are no countries in Africa, as of yet, that have been granted an adequacy decision. This means that exporters in these cases must take supplementary measures, in combination with providing appropriate safeguards as mentioned in Article 46 of the GDPR, to ensure that the rights of the data subjects are not undermined as a result of the transfers.

However, there is an obvious difference between the cases of third-country transfers for storage and research purposes, where it has been found that encryption and pseudonymization provide effective protection, and third-country transfers for support purposes: giving support requires that the personal data is accessible in clear for the recipient. In other words, the person sitting in for example India and giving technical assistance to customers in France most likely will need the personal data belonging to the data subject visible to perform their task.

In cases where the processing requires the data to be visible, the EDPB has established that there is currently no technical measure that can prevent the rights of the data subject from being violated, for example by public authorities in third countries accessing their data.[155] In conclusion, it is the responsibility of the data exporter to find out if there are organizational measures that could be effective in ensuring the protection of personal data.

5.4 Risks and challenges with using Privacy Enhancing Technologies

It is noted that encryption and pseudonymization at the least are successful in protecting personal data rights in the case of third-country transfers for storage and research purposes. However, there are challenges and potential risks with using Privacy Enhancing Technologies.

---

[152] The Center for the Promotion of Imports from Developing Countries - Netherlands Ministry of Foreign Affairs, *"What is the demand for IT Outsourcing Services on the European Market?"*, 27 March 2024, Available at: https://www.cbi.eu/market-information/outsourcing/trade-statistics, (Accessed 17 April 2024).

[153] See Whitelane Research, *"France 2022"*, Available at: https://whitelane.com/france-2022/, (Accessed 5 April 2024).

[154] See Whitelane Research, *"Germany 2022",* Available at: https://whitelane.com/germany-2022/, (Accessed 5 April 2024).

[155] Recommendations 01/2020, para. 35.

Firstly, a lack of expertise regarding Privacy Enhancing Technologies can impose risks.[156] Technologies such as encryption and pseudonymization are complex solutions that require thorough understanding and correct implementation. If the implementation is incorrect, there is a risk the utility of the Privacy Enhancing Technology is weakened, thus compromising the safety of the exported personal data. The optimum for ensuring that the Privacy Enhancing Technology is correctly implemented would be to have one or multiple people within the company who are particularly skilled in technology and privacy. It is important to note that correct and sufficient expertise in the implementation of Privacy Enhancing Technologies can be costly for the controller and its company. To reduce the cost and resources involved which it claims, controllers can however outsource that part of the business to other companies.[157]

Another risk with the use of Privacy-Enhancing Technologies is the lack of maturity in some cases.[158] The maturity of a Privacy Enhancing Technology is dependent on the phase within its lifecycle. Broadly speaking, technologies can be described as having 7 different phases in their lifecycle: birth, childhood, adolescence, adulthood, seniority, senility, and death.[159] Furthermore, the maturity of a Privacy Enhancing Technology is measured by combining the scale of readiness and the scale of quality of that particular technology.[160] A Privacy Enhancing Technology, such as encryption, must be mature enough during the time of implementation to withstand threats such as cyberattacks and provide robust protection. On the one hand, "young" technologies might be underdeveloped and lack experience. On the other hand, a technology that is in the late stages of its lifecycle might be obsolete, making it particularly vulnerable, or outperformed by newer technologies. Moreover, the risk of lack of maturity can be mitigated through controllers correctly assessing the maturity of the technology and the most ideal phase for implementation.[161] This assessment is dependent on which Privacy Enhancing Technology is concerned, as well as the context of use.

---

156 Information Commissioners Office, *"Chapter 3: Pseudonymisation – Draft anonymization, pseudonymization and privacy enhancing technologies guidance",* February 2022, Available at: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. (Accessed 2 April 2024), p. 5.

157 Ibid.

158 Ibid.

159 Hansen, Marit, Hoepman, Jaap-Henk & Jensen, Meiko, *"Towards Measuring Matutiry of Privacy-Enhancing Technologies"*, No date, Available at: https://www.cs.ru.nl/~jhh/publications/pet-maturity.pdf, (Accessed 21 April 2024), p. 3.

160 Ibid, p. 5.

161 Information Commissioners Office, *"Chapter 3: Pseudonymisation – Draft anonymization, pseudonymization and privacy enhancing technologies guidance",* February 2022, Available at: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. (Accessed 2 April 2024), p. 9.

5.5 Summary

By incorporating technological measures such as Privacy Enhancing Technologies in the systems at an early stage, preferably even before the personal data is transmitted, controllers comply with the requirement of privacy by design stated in the GDPR. Privacy Enhancing Technologies also facilitate proving accountability. However, not every Privacy Enhancing Technology is suitable for every situation, which is not surprising considering the broadness of the term.

The first question that must be asked is *if* a Privacy Enhancing Technology can be successfully implemented at all. The answer to this question lies in whether the purpose of the third-country transfer requires the personal data to be accessible in clear for the recipient to be able to fulfill its task. In the case of storage and research, this is not an issue. However, a recipient that provides support on behalf of a controller in the EU must see the data in clear to the job. In that case, it is impossible to implement a Privacy Enhancing Technology functionally. Since the data subjects cannot be guaranteed protection against violations of their rights if the personal data is visible to the recipient, the case of third-country transfers for support reasons is a dead-end, at least in the context of technological solutions. If the processing requires the data to be visible in clear, the controller simply must find other additional measures, or cease the transfers.

If it is established that the purpose of the transfer does not require the personal data to be visible to the recipient, the second question that must be asked is *what* form the personal data must be in order for the task and purpose to be fulfilled. In the case of storage, the data can stay in a locked format since nothing is being done to it. Therefore, it is sufficient for it to be encrypted and just "left alone". However, recipients who are conducting research on the data must have something concrete to work with and analyze. In that case, it is suitable for the exporter to pseudonymize the part of the data that is personal data before it is transmitted to the third country. That way, the data subjects are protected from their personal data being disclosed and the recipient can fulfill their task of performing statistical, analytical, or operational research on the data.

In conclusion, the question of whether a Privacy Enhancing Technology effectively can be adopted as a supplementary measure during third-country transfers depends entirely on the context and purpose of the transfer as well as the characteristics of the specific Privacy Enhancing Technology.

6 Concluding remarks

This thesis has aimed to examine if the implementation of different Privacy Enhancing Technologies, more specifically encryption and pseudonymization, during third-country transfers of personal data could effectively protect the rights of the data subject. This is a complex question that has far from one simple answer.

Firstly, it must be understood that personal data protection is well-established in the EU. This is most evident in the fact that the EU has the strongest regulatory framework for personal data worldwide. Individuals´ right to the protection of their personal data was not groundbreaking when the GDPR came into force in 2018. Rather, the right has been seen as a part of the fundamental right to respect for private and family life and was later explicitly incorporated in a separate article in the Charter. In other words, it can quickly be established that there are regulatory frameworks in the EU, both in primary and secondary law, that aim to guarantee the protection of personal data.

In the context of third-country transfers, the judgments of the CJEU, Schrems I and II, mention a key problem that is considered a threat to the rights of data subjects: public authorities in third countries accessing and using their personal data. According to the CJEU, public authorities and other third parties in a third country accessing the personal data of EU citizens signifies a breach of Articles 7 and 8, regardless of the context. This is particularly relevant for third countries that lack respect for human rights and effective supervisory authorities since this puts the data subjects in a particularly vulnerable situation. One of the main aims of the EU is to protect its citizens, and public authorities in third countries accessing and using the personal data of these citizens would be going against this very aim.

It is practically impossible for a third country to provide the same level of protection for personal data as the EU does, given the level of protection granted by the EU. Because of this, the CJEU has concluded that "an essentially equivalent" level of protection is sufficient when assessing if a third-country transfer can proceed without additional measures. Nevertheless, it can be established that this standard is still difficult to achieve for third countries, not least for the U.S granted the reoccurring invalidation of U.S. adequacy decisions. In addition, there seems to be an internal conflict within the EU as the CJEU continues to interpret "essentially equivalent" more strictly than the Commission does in their assessments of the requirements of "adequate level of protection" in Article 45 of the GDPR.

Nonetheless, there are ways other than through adequacy decisions in which data exporters can carry out third-country transfers and thereby encourage cross-

border exchanges. In some ways, the existence of alternative solutions argues for the high requirements for adequacy decisions. In other words, it is difficult to argue that the high requirements of adequacy decisions, particularly the strict interpretations of the CJEU, pose an obstacle to cross-border exchanges since there are other possibilities in the GDPR for data exporters who wish to transfer personal data to a third country. As stated in Article 46 of the GDPR, a controller or a processor can transfer personal data to a third country by providing appropriate safeguards, such as BCRs or SCCs. However, the use of appropriate safeguards is in some cases easier said than done. In Schrems II, the CJEU emphasized that SCCs do not function in a vacuum, as they only are intended to grant contractual guarantees to the parties involved in the transfers. This means that appropriate safeguards do not, at least not alone, ensure that the rights of the data subjects are not undermined when the personal data is moved outside of the Union. Although this is not mentioned in Article 46 of the GDPR, a controller or a processor that wishes to use appropriate safeguards as a ground for third-country transfers must always assess the domestic laws and practices of the specific country. In essence, this determination by the CJEU means that data exporters that provide appropriate safeguards must carry out a similar, but most likely not as comprehensive, assessment as the one behind the Commissions adequacy decisions. Otherwise, there is a risk that the personal data protection granted to data subjects by EU law is undermined.

It is when this assessment shows deficiencies in the domestic laws and practices of that specific third country, that the main topic for this thesis, Privacy Enhancing Technologies, comes into play. Simply explained, these shortcomings can be healed with the implementation of Privacy Enhancing Technologies. However, Privacy Enhancing Technology is a broad concept that involves many different technologies. In conclusion, the main factors for whether a Privacy Enhancing Technology successfully can ensure that personal data protection is not undermined during third-country transfers are (i) the characteristics of that specific technology and (ii) the purpose of the transfer. Thus, *some* Privacy Enhancing Technologies are successful tools in protecting the rights of the data subjects in *some* cases. It can be argued that the main contributing factor to whether the implementation of a Privacy Enhancing Technology is successful is the question of visibility. It can be established from the various definitions of Privacy Enhancing Technologies that they aim to prevent disclosure and visibility. Fittingly enough, the visibility of personal data, whether that be to national authorities or other third parties, is a direct threat to the rights of the data subjects. Therefore, in situations where visibility is not required for the recipient in the third country, the tools, which are the Privacy Enhancing Technologies, are compatible with satisfying the rules of personal data protection in the EU.

It can be understood from the judgments of the CJEU that it is a requirement, placed upon data exporters that transfer personal data to third countries without adequacy decisions and with deficient domestic laws and practices, to implement some sort of supplementary measures in combination with the appropriate safeguards. As of today, it is only a recommendation to implement Privacy Enhancing Technologies. Although it can be established that encryption is a successful

tool in transfers for storage purposes and pseudonymization is a successful tool in transfers for research purposes, the recommendations from the EDPB are not sufficient in solving the balancing act of ensuring the protection of personal data and still encouraging and enabling cross-border transfers outside of the EU on a broader scale. On the one hand, they are just recommendations, and on the other hand, their scope is too narrow as they only prove the effectiveness of two technologies in two cases.

Therefore, more extensive work on the issue of transfers to third countries with deficient laws and practices is needed. The narrowness of the current recommendations from the EDPB entails that clear instructions from the EU on both technical and organizational supplementary measures that can be implemented effectively in other cases are vital. Otherwise, there is a risk of European controllers and processors, that transfer personal data for other reasons than storage and research, avoiding transferring personal data to third countries with deficient laws and practices in fear of sanctions.

Furthermore, the question arises whether the recommendations from the EDPB will have sufficient impact as they are voluntary for data exporters to follow. It can be argued that the implementation of encryption and pseudonymization, in the cases where it has been proven effective, should be legally required, especially since the CJEU stated in Schrems II that the implementations of additional measures are required when the laws and practices in a third country are deficient. This would act as an incentive for data exporters to further protect personal data during transfers to certain third countries, ensuring that the EU law is not undermined. In addition, some of the principles in the GDPR, mainly the principle of data protection by design, suggest that encryption and pseudonymization should be legally required in cases such as this.

The difficult balancing act between on one hand ensuring that the protection of personal data is not undermined during third-country transfers and on the other hand attending to the needs of the globalization of today and the future is evident. This thesis has shown how encryption and pseudonymization in some cases can be used to solve this balancing act. How this can be done in more ways remains to be explored.

Bibliography

Legislation

Consolidated Version of the Treaty on European Union, 2016, OJ C 202/13 [cit. TEU].

Consolidated Treaty on the Functioning of the European Union, 2016, OJ C 202/47 [cit. TFEU].

European Convention on Human Rights [cit. Convention].

Convention for the Protection of Individuals with regard to the Processing of Personal Data [cit. Convention 108].

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Cit. Data Protection Directive].

Charter of Fundamental Rights of the European Union, 2016 OJ C 202/389 [cit. Charter].

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [cit. General Data Protection Regulation].

Official document

Commission

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**.**

Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

EDPB

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data [cit. Recommendations 01/2020].

Case Law

Court of Justice of the European Union

Judgment of the Court of 5 February 1963. – NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherklands Inland Revenue Adminstration, ECLI:EU:C:1963:1.

Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, ECLI:EU:C:2014:317.

Judgment of the Court (Grand Chamber) of 6 October 2015, Maximilian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 [cit. Schrems I].

Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems, C-311/18, ECLI:EU:C:2020:559 [cit. Schrems II].

European Court of Human Rights

Costello-Roberts v. the United Kingdom, Judgment of 25 March 1993, European Court of Human Rights (ECHR), 13134/87.

Amann v. Switzerland, Judgment of 16 February 2000, European Court of Human Rights (ECHR), 27798/95.

Rotaru v. Romania, Judgment of 4 May 2000, European Court of Human Rights (ECHR), 28341/95.

Literature

Belanger, France & Crossler, Robert, *Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems,* MIS Quarterly*,* 2011*,* pp.1017-1041, [cit. Belanger & Crossler (2011)].

Frydlinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline & Beyer, Sandra, *GDPR - juridik, organisation och säkerhet enligt dataskyddsförordningen,* 1:a. uppl., Norstedt Juridik, Stockholm, 2018 [cit. Frydlinger et al. (2018)].

Greenstein, Stanley, *Elevating Legal Informatics in the Digital Age*, In Petterson, Sonya (ed.), Digital Human Sciences, Stockholm: Stockholm University Press, 2021 [cit. Greenstein (2021)].

Hettne, Jörgen & Otken Eriksson, Ida (red.), *EU-rättslig metod - teori och genomslag i svensk rättstillämpning*, 2. uppl., Norstedt Juridik, Stockholm, 2011 [cit. Hettne & Otken Eriksson (2011)].

Hjertstedt, Mattias, *Beskrivningar av rättsdogmatisk metod: om innehållet i metodavsnitt vid användning av ett rättsdogmatiskt tillvägagångssätt*, In: Ruth Mannelqvist, Staffan Ingmanson, Carin Ulander–Wänman (ed.), Festskrift till Örjan Edström (pp. 165–173). Umeå: Juridiska institutionen, Umeå universitet, 2019 [cit. Hjertstedt (2019)].

Leenes, Ronalds, van Brakel, Rosamunde, Gutwirth, Serge & De Hert, Paul, *Data Protection and Privacy: (In)visibilites and infrastructures*, 1st edn., Springer, 2017 [cit. Leenes at al. (2017)].

Magnusson Sjöberg, Cecilia, *Rättsinformatik - Juridiken i det digitala informationssamhället,* 4:e uppl., Studentlitteratur, Lund, 2021 [cit. Magnusson Sjöberg (2021)].

Michael Holtz, Hajo, *Den nya allmänna dataskyddsförordningen — några anmärkningar,* Svensk Juristtidning, [cit. Michael Holtz (2018)].

Reichel, Jane, *EU-rättslig metod*, in *Juridisk metodlära*, Nääv, Maria & Zamboni, Mauro (red.), 2 uppl., Studentlitteratur, Lund, 2018, pp. 109–142 [cit. Reichel (2018)].

Seipel, Peter, *Juridik och IT - introduktion till rättsinformatiken*, 8:e uppl, Norstedts juridik, Stockholm, 2004 [cit. Seipel (2004)].

Web sources

EU institutions

Article 29 Data Protection Working Party, *"Opinion 03/2013 on purpose limitation",* European Commission, 2 April 2013, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (Accessed 2 March 2024).

Council of the European Union, *"The General Data Protection Regulation"*, 11 January 2024, Available at: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/, (Accessed 14 May 2024).

Enisa, *"Promoting Data Protection by Design: Exploring Techniques"*, 27 January 2022, Available at: https://www.enisa.europa.eu/news/enisa-news/promoting-data-protection-by-design-exploring-techniques, (Accessed 1 April 2024).

EUR-Lex, *"The non-written sources of European law – supplementary law",* 12 March 2018, Available at: https://eur-lex.europa.eu/EN/legal-content/summary/the-non-written-sources-of-european-law-supplementary-law.html, (Accessed 28 April 2024).

European Commission, "*Commission finds that EU personal data flows can continue with 11 third countries and territories*", 15 January 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161, (Accessed 17 February 2024).

European Commission, *"United States – EU trade relations with the United States. Facts, figure and latest developments",* No date, Available at: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en, (Accessed 25 February 2024).

European Commission, "*Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation",* No date, Available at: https://health.ec.europa.eu/document/download/c3042973-b36d-4094-a1fb-a6fc980f065e_en, (Accessed 19 April 2024).

European Parliament, *"The EU as a community of law – Overview of the role of law in the Union"*, March 2017, Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599364/EPRS_BRI(2017)599364_EN.pdf, (Accessed 22 April 2024).

European Union Agency For Fundamental Rights, "EU Charter of Fundamental Rights", Available at: https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data, (Accessed 1 March 2024).

Wiewiórowski, Wojciech, *"Accountability needs technology",* European Data Protection Supervisor, 8 September 2016, Available at: https://www-edps-europa-eu.translate.goog/press-publications/press-news/blog/accountability-needs-technology_en?_x_tr_sl=en&_x_tr_tl=sv&_x_tr_hl=sv&_x_tr_pto=sc, (Accessed 17 April).

Other

Aslak Juliussen, Bjorn, Kazory, Elisavet, Johansen, Dag & Petter Rui, Jon, *"The third country problem under the GDPR: enhancing protection of personal data transfers with technology"*, Oxford Academic, 19 July 2023, Available at: https://academic.oup.com/idpl/article/13/3/225/7226249, (Accessed 1 March 2024).

Cloudflare, *"What is pseudonymization",* No date, Available at: https://www.cloudflare.com/learning/privacy/what-is-pseudonymization/. (Accessed 3 April 2024).

Duarte, Fabio, "*Amount of Data Created Daily (2024)"*, Exploding Topics, 13 December 2023, Available at: https://explodingtopics.com/blog/data-generated-per-day, (Accessed 17 February 2024).

Federal Register – The Daily Journal of the United States Government), *"Request for Information on Advancing Privacy-Enhancing Technologies",* 6 September 2022, Available at: https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, (Accessed 23 April 2024).

Google Domains Help, *"About hosting providers",* available at: https://support.google.com/domains/answer/3288265?hl=en, (Accessed 17 April 2024).

Hansen, Marit, Hoepman, Jaap-Henk & Jensen, Meiko, *"Towards Measuring Matutiry of Privacy-Enhancing Technologies"*, No date, Available at: https://www.cs.ru.nl/~jhh/publications/pet-maturity.pdf, (Accessed 21 April 2024).

Humadi, Ahmed, "*Encryption*", ResearchGate, 8 December 2020, Available at: https://www.researchgate.net/publication/347301480_enycryption, (Accessed: 4 April).

Information Commissioners Office, *"Chapter 3: Pseudonymisation – Draft anonymization, pseudonymization and privacy enhancing technologies guidance",* February 2022. Available at: https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf. (Accessed 2 April 2024).

Integritetsmyndigheten, *"Europeiska Dataskyddstyrelsen (EDPB)"*, 22 February 2022, Available at: https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-eu-niva/edbp/, (Accesssed 23 April).

Intersoft Consulting, *"Encryption"*, Available at: https://gdpr-info.eu/issues/encryption/ (Accessed 12 March 2024).

Keyfactor, *"When to use symmetric encryption vs. asymmetric encryption"*, 17 June 2020, Available at: https://www.keyfactor.com/blog/symmetric-vs-asymmetric-encryption/. (Accessed 1 April 2023).

Liss, Joseph, Peloquin, David, Bernes, Mark & Bierer E Barbara, *"Demystifying Schrems II for the cross-border transfer of clinical research data*, Oxford Academic, 23 October 2021, Available at: https://academic.oup.com/jlb/article/8/2/lsab032/6407729?itm_medium=sidebar&itm_source=trendmd-widget&itm_campaign=Journal_of_Law_and_the_Biosciences&itm_content=Journal_of_Law_and_the_Biosciences_0, (Accessed 20 April 2024).

Morkel, T & Eloff, JHP, *"Encryption techniques: A Timeline Approach"*, Available at: https://digifors.cs.up.ac.za/issa/2004/Proceedings/Research/062.pdf, No date, (Accessed 15 March 2024).

OECD, "The OECD Privacy Framework", 2013, Available at: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (Accessed 9 March 2024).

OECD, *"Emerging Privacy Enhancing Technologies – Current Regulatory and Policy Approaches"*, OECD Digital Economy Papers, March 2023, Available at: https://www.oecd-ilibrary.org/docserver/bf121be4-en.pdf?expires=1715594818&id=id&accname=guest&checksum=DA4D55D5E9D92FAC062BDC7DCFFCAEE1, (Accessed 15 March 2024).

Richman, Amitai, "*Pseudonymization vs Encryption: Understanding the differences"*, k2view, 7 June 2023, Available at: https://www.k2view.com/blog/pseudonymization-vs-encryption/#How-Pseudonymization-Works-Preserving-Privacy-Through-Data-Anonymization. (Accessed 8 April 2024).

The Center for the Promotion of Imports from Developing Countries - Netherlands Ministry of Foreign Affairs, *"What is the demand for IT Outsourcing Services on the European Market?"* , 27 March 2024, Available at: https://www.cbi.eu/market-information/outsourcing/trade-statistics, (Accessed 17 April 2024).

Ubaidullah Bokhari, Mohammed & Makki Shallal, Qahtan, "*A Review on Symmetric Key Encryption Techniques in Cryptography",* ResearchGate, August 2016, Available at: https://www.researchgate.net/publication/333118027_A_Review_on_Symmetric_Key_Encryption_Techniques_in_Cryptography, (Accessed 2 April 2024).

Whitelane Research, *"France 2022"*, Available at: https://whitelane.com/france-2022/, (Accessed 5 April 2024).

Whitelane Research, *"Germany 2022",* Available at: https://whitelane.com/germany-2022/, (Accessed 5 April 2024).