UNIVERSITY OF TURKU
Faculty of Law

Two sides of data protection

Examining the complex and political nature to the personal data transfers between the European Union and the United States

Advanced International Law and Technology/Faculty of Law, University of Turku
Master's thesis

Author(s):
Miska Lundén

03.05.2022

UNIVERSITY OF TURKU
Faculty of Law

Master's thesis

Subject: Faculty of Law

Author(s): Miska Lundén

Title: Two sides of data protection: Examining the complex and political nature to the personal data transfers between the European Union and the United States

Supervisor(s): Ekaterina Markovich

Number of pages: 54 pages

Date: 03.05.2022

This thesis investigates the complexity and the political aspects of the data protection. This thesis is viewed from the perspective of international transfers of personal data between the European Union and the United States. These two parties were chosen because of the special role each one has - the US in the cloud storages and the EU in the privacy regulation sphere. The thesis follows legal dogmatic methodology based on legal and doctrinal research materials with a focus on the importance of well-functioning data protection legislation by placing an interest towards technology-based approach rather than political. The thesis contains in-depth analysis on the history of EU's data protection legislation and to events that have influenced it trying to answer the question what is wrong and why. Furthermore, the thesis attempts to resolve underlying problems with the current data protection legislation and analyse whether technological innovations could be used to our benefit. The thesis reaches the result that the possibility of having political sway in the data protection legislation has an impact and does not resolve the underlying problem of trust. Furthermore, technological innovations such as Fully Homomorphic Encryption could be used to resolve, at least partially, the problems faced in data protection. I reached the conclusion that if the EU chooses not to go with technology based problem-solving methods, adequacy decisions should be approved by the European Data Protection instead of the European Commission.

Key words: Data protection, Privacy, GDPR

Table of contents

References

Legislation, Treaties & Case Law

Case C-362/14 *Schrems* [2015] ECLI:EU:C:2015:650

Case C-311/18 *Facebook Ireland and Schrems* [2020] ECLI:EU:C:2020:559

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 [1995] OJ L 281

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119

Articles, Books, Reports, Submissions & Internet sources

'Free Trade | Definition & Facts' (Encyclopaedia Britannica) <https://www.britannica.com/topic/free-trade> accessed 3 March 2022.

'Adam Smith And "The Wealth Of Nations"' (Investopedia, 2021) <https://www.investopedia.com/updates/adam-smith-wealth-of-nations/> accessed 3 February 2022.

'What Is Protectionism?' (Investopedia) <https://www.investopedia.com/terms/p/protectionism.asp> accessed 12 March 2022.

Gregory Mankiw, 'Economists Actually Agree On This: The Wisdom Of Free Trade' The New York Times (2015) <https://www.nytimes.com/2015/04/26/upshot/economists-actually-agree-on-this-point-the-wisdom-of-free-trade.html> accessed 1 May 2022.

'What Is Network Society' (Igi-global.com) <https://www.igi-global.com/dictionary/network-society/20182> accessed 24 March 2022.

Michalis Zinieris, 'Data: A Small Four-Letter Word Which Has Grown Exponentially To Such A Big Value' (Deloitte Cyprus)

<https://www2.deloitte.com/cy/en/pages/technology/articles/data-grown-big-value.html> accessed 15 April 2022.

'18 Most Popular Iot Devices In 2022 (Only Noteworthy Iot Products)' (https://www.softwaretestinghelp.com/, 2022) <https://www.softwaretestinghelp.com/iot-devices/> accessed 3 March 2022.

'Mobile App Download Statistics & Usage Statistics (2022) - Buildfire' (BuildFire, 2022) <https://buildfire.com/app-statistics/> accessed 10 April 2022.

'Data Is More Valuable Than Oil – Tidalscale' (Tidalscale.com) <https://www.tidalscale.com/data-is-more-valuable-than-oil/> accessed 3 May 2022.

Theresa Fauerbach, 'More Valuable Than Oil, Data Reigns In Today's Data Economy' <https://www.northridgegroup.com/blog/more-valuable-than-oil-data-reigns-in-todays-data-economy/> accessed 26 April 2022.

'Proposal For An Eprivacy Regulation' (Shaping Europe's digital future) <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation> accessed 1 May 2022.

Emerson H. Tiller and Frank B. Cross, 'What Is Legal Doctrine?' [2005] SSRN Electronic Journal <https://core.ac.uk/download/pdf/76622332.pdf> accessed 5 April 2022. p.1.

'What Is The Safe Harbour Agreement? | Experian Business' (Experian.co.uk) <https://www.experian.co.uk/business/glossary/safe-harbour-agreement/> accessed 8 April 2022.

'The Cost Of ISO Certification - ISO Update' (ISO Update, 2020) <https://isoupdate.com/general/the-cost-of-iso-certification/> accessed 13 April 2022.

'Welcome To The U.S.-EU Safe Harbor' (export.gov, 2017) <https://2016.export.gov/safeharbor/eu/eg_main_018365.asp> accessed 3 April 2022.

European Parliament, 'Safe Harbour Ruling: Meps Called For Clarity And Effective Protection' (2015) <https://www.europarl.europa.eu/news/en/press-room/20151015IPR97903/safe-harbour-ruling-meps-called-for-clarity-and-effective-protection> accessed 10 April 2022.

'Snowden Revelations' (Lawfare) <https://www.lawfareblog.com/snowden-revelations> accessed 2 May 2022.

Ben Wolford, 'What Is GDPR, The EU'S New Data Protection Law? - GDPR.Eu' (GDPR.eu) <https://gdpr.eu/what-is-gdpr/> accessed 2 May 2022.

HIPAA Journal, 'Does GDPR Apply To EU Citizens Living In The US?' (HIPAA Journal, 2021) <https://www.hipaajournal.com/does-gdpr-apply-to-eu-citizens-living-in-the-us/> accessed 1 May 2022.

'Area By NUTS 3 Region' (Eurostat, 2021).

www.baltimoresun.com

'Federal Trade Commission Enforcement Of The U.S.-EU And U.S.-Swiss Safe Harbor Frameworks' (*Federal Trade Commission*, 2012) <https://www.ftc.gov/business-guidance/resources/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor-frameworks> accessed 9 April 2022.

Impact Advisors, '7 Principles Of The EU-U.S. Privacy Shield Framework - Impact Advisors' (*Impact Advisors*) <https://www.impact-advisors.com/security/eu-us-privacy-shield-framework/> accessed 10 March 2022.

'Adequacy Decisions' (European Commission - European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 3 April 2022.

European Data Protection Board, Who Are We <https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en/> Accessed 25 April 2022.

Lukas Feiler and Wouter Seinen, 'Bcrs As A Robust Alternative To Privacy Shield And Sccs' (Iapp.org, 2020) <https://iapp.org/news/a/binding-corporate-rules-as-a-robust-alternative-to-privacy-shield-and-sccs/> accessed 9 March 2022.

European Data Protection Board, Approved Binding Corporate Rules <https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_el/> Accessed 8 April 2022.

European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted on 10 November 2020) p. 2-3. <https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf/> Accessed 12 March 2022.

Cynthia O'Donoghue and others, 'EDPB Adopts Final Recommendations On Supplementary Measures Nearly A Year After The CJEU’S Schrems II Ruling' (Technology Law Dispatch, 2021) <https://www.technologylawdispatch.com/2021/07/privacy-data-protection/edpb-adopts-final-recommendations-on-supplementary-measures-nearly-a-year-after-the-cjeus-schrems-ii-ruling/> accessed 9 April 2022.

The high Court judicial review, Facebook Ireland Limited and Data Protection Commission, 14th day of May 2021, [2021] IEHC 336.

Natasha Lomas, 'Meta Sent A New Draft Decision On Its EU-US Data Transfers' (TechCrunch, 2022) <https://techcrunch.com/2022/02/21/dpc-meta-draft-data-transfers-decision/> accessed 23 March 2022.

Meta Inc., 'ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGE ACT OF 1934 For The Fiscal Year Ended December 31, 2021' (Meta Platforms, Inc 2022) <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf> accessed 14 April 2022.

Max Schrems, '"Privacy Shield 2.0"? - First Reaction By Max Schrems' (noyb.eu, 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 7 April 2022.

Jeran Wittenstein, 'Meta Loses Top-10 Ranking By Market Value Amid Worst Month Ever' Bloomberg (2022) <https://www.bloomberg.com/news/articles/2022-02-17/meta-platforms-falls-from-ranks-of-10-most-valuable-companies> accessed 24 April 2022.

Jon Hill, 'Data Vs Information: What's The Difference?' (Bloomfire, 2021) <https://bloomfire.com/blog/data-vs-information/> accessed 2 May 2022.

'52.227-14 Rights In Data-General.' (Acquisition.gov, 2014) <https://www.acquisition.gov/far/52.227-14> accessed 7 February 2022.

OECD Directorate, 'OECD Glossary Of Statistical Terms - Data Definition' (Glossary of Statistical Terms, 2001) <https://stats.oecd.org/glossary/detail.asp?ID=532> accessed 26 March 2022.

'Definition Of Data' (PCMAG) <https://www.pcmag.com/encyclopedia/term/data> accessed 9 January 2022.

Gavin Wright, 'What Is Raw Data And How Does It Work?' (SearchDataManagement, 2021) <https://www.techtarget.com/searchdatamanagement/definition/raw-data> accessed 15 February 2022.

Chepalskei, 'DATA PROCESSING' (Kenya Cheplaskei Boys High School, 2018). <https://peda.net/kenya/css/subjects/computer-studies/form-three/driac2/data-processing/> Accessed 22 February 2022.

'What Is Machine Data Analytics? | Sumo Logic' (Sumo Logic) <https://www.sumologic.com/glossary/machine-data/> accessed 24 March 2022.

Mugdha Ghotkar and Priynka Rodke, 'An Outlook On India's Healthcare System With A Medical Case Study And Review On Big Data And Its Importance In Healthcare' [2016] International Journal of Science and Research (IJSR) https://www.ijsr.net p. 1-5.

Salman Zafar, 'How Businesses Can Benefit From Big Data | Techie Loops' (Techie Loops, 2021) <https://techieloops.com/how-businesses-can-benefit-from-big-data/> accessed 16 April 2022.

Nally C, 'How Much Data Does A Jet Engine Produce?' <https://www.mcnallyinstitute.com/how-much-data-does-a-jet-engine-produce/> accessed 9 April 2022.

'Most Used Social Media 2021 | Statista' (Statista, 2022) <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> accessed 7 April 2022.

SeeUnity, 'The Main Differences Between The DPD And The GDPR And How To Address Those Moving Forward' (2017) <https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf> accessed 13 February 2022.

'Sheet N°1: Identify Personal Data' (https://www.cnil.fr, 2020) <https://www.cnil.fr/en/sheet-ndeg1-identify-personal-data> accessed 2 May 2022.

Jiri Kohout, 'Why Is Data Encryption Necessary Even In Private Networks?' <https://teskalabs.com/blog/seacat-encryption> accessed 12 April 2022.

Nate Lord, 'Data Protection: Data In Transit Vs. Data At Rest' <https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest> accessed 18 March 2022.

Dale Walker, 'What Is End-To-End Encryption And Why Is Everyone Fighting Over It?' <https://www.itpro.co.uk/security/encryption/359943/what-is-end-to-end-encryption-and-why-is-everyone-fighting-over-it> accessed 8 April 2022.

'What Is Data Encryption?' (www.kaspersky.com) <https://www.kaspersky.com/resource-center/definitions/encryption> accessed 18 February 2022.

Hugh Aver, 'What End-To-End Encryption Is, And Why You Need It' <https://www.kaspersky.com/blog/what-is-end-to-end-encryption/37011/> accessed 11 January 2022.

Anne-Catherine Berg, 'New EU-US Privacy Shield To Replace Safe Harbour Agreement' The European Broadcasting Union (2016) <https://www.ebu.ch/news/2016/02/eu-us-privacy-shield> accessed 22 February 2022.

'What Is Fully Homomorphic Encryption?' (Inpher) <https://inpher.io/technology/what-is-fully-homomorphic-encryption/> accessed 5 April 2022.

Ryan Yackel, 'What Is Homomorphic Encryption, And Why Isn’t It Mainstream?' (Keyfactor, 2021) <https://www.keyfactor.com/blog/what-is-homomorphic-encryption/> accessed 28 January 2022.

Ryan Ko and Kim Choo, The Cloud Security Ecosystem (1st edn, Elsevier Inc 2015) p. 101-127.

Flavio Bergamaschi, 'IBM Releases Fully Homomorphic Encryption Toolkit For Macos And Ios; Linux And Android Coming Soon' <https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/> accessed 15 January 2022.

'Homomorphic Encryption Services' (Ibm.com, 2022) <https://www.ibm.com/security/services/homomorphic-encryption> accessed 19 March 2022.

Steven Yue, 'Fully Homomorphic Encryption Part One: A Gentle Intro' (Medium, 2020) <https://stevenyue.medium.com/fully-homomorphic-encryption-part-one-a-gentle-intro-94c3c3850568> accessed 1 February 2022.

Flavio Bergamaschi, 'IBM Releases Fully Homomorphic Encryption Toolkit For Macos And Ios; Linux And Android Coming Soon' <https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/> accessed 15 January 2022.

'Press Corner' (*European Commission - European Commission*, 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 12 April 2022.

European Commission, 'Trans-Atlantic Data Privacy Framework' (2022) <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 9 April 2022.

Ellysse Dick Nigel Cory, '‘Schrems II’: What Invalidating The EU-U.S. Privacy Shield Means For Transatlantic Trade And Innovation' (*Itif.org*, 2020) <https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic> accessed 10 March 2022.

List of Abbreviations

DPD	Data Protection Directive
EU	European Union
US	United States
GDPR	General Data Protection Regulation
EEA	European Economic Area
PII	Personally Identifiable Information
DOT	Department of Transportation
FTC	Federal Trade Commission
CJEU	Court of Justice of the European Union
OECD	Organisation for Economic Co-operation and Development
FHE	Fully Homomorphic Encryption
OECD	Organisation for Economic Co-operation and Development

1 Introduction

The inter-connected world we currently live in, especially in the European Union, was built around the ideas such as the free movement of persons and goods. In the digital era, data is included in these values. These core values have been seen as the driving force of the EU. Furthermore, many countries around the world have seen these values as something to admire and even take an example. Free movement of goods was influenced by the concept of free trade. According to Britannica, free trade is defined as "a policy by which the government does not discriminate against imports or interfere exports by applying tariffs or subsidies"[1]. In summary, an idea that governments should impose as little restrictions to trade as possible.

Free flow of data serves as one of the main cores in this thesis. It might not seem like it straight away because I support the idea that in order to enjoy free flow of data, it first requires that the data about to move freely in the digital era to be protected well-enough beforehand. We have truly come a long way as a civilisation. Rarely one stops to consider how different the world was before the invention of the smartphone. Smartphones have taken the sharing of data to a new level. As early as 18th century, Adam Smith recognized the potential value of free trade in relation to prosperity and efficiency.[2]

Serving as the opposite ideology in the spectrum is protectionism. Protectionism is defined as "policies that restrict international trade in pursuit of helping domestic industries"[3]. In a way, the European Union's General Data Protection Regulation serves as an example of protectionist regulation. However, the world we are currently living in was not built on a protectionist ideology. Economists have long understood the importance of free and effortless trade in a global world.[4] In the wake of COVID-19 pandemic, the realisation of just how connected the world was came to light as companies started to struggle with not being able to produce end-product because certain parts had ended from warehouses and suppliers faced problems sending

[1] 'Free Trade | Definition & Facts' (Encyclopaedia Britannica) <https://www.britannica.com/topic/free-trade> accessed 3 March 2022.

[2] 'Adam Smith And "The Wealth Of Nations"' (Investopedia, 2021) <https://www.investopedia.com/updates/adam-smith-wealth-of-nations/> accessed 3 February 2022.

[3] 'What Is Protectionism?' (Investopedia) <https://www.investopedia.com/terms/p/protectionism.asp> accessed 12 March 2022.

[4] Gregory Mankiw, 'Economists Actually Agree On This: The Wisdom Of Free Trade' The New York Times (2015) <https://www.nytimes.com/2015/04/26/upshot/economists-actually-agree-on-this-point-the-wisdom-of-free-trade.html> accessed 1 May 2022.

new orders. The importance of connectivity has grown at an incredible fast pace in the past few decades as we are transforming towards a data-driven society.

Connectivity can mean many things to different readers, but for the purpose of this thesis we shall consider connectivity to mean society brought together by the Internet communication technologies in which individuals and organisations around the world are connected to digital information networks.[5] Different innovations have played an important role in bringing people together and most notable ones of such innovations are the internet and a modern smartphone. Modern smartphone refers to the smartphone that is operated by touch controls and has advanced functions. Smartphones have had the biggest impact on the way human interaction is conducted in the 21st century. This is because a smartphone is a lightweight multifunctional handheld powerhouse that is a controller with touches of the screen and most notably, it enables easy access to virtually everywhere the user wants.

Along with the Internet and the smartphone, the importance of data has grown exponentially.[6] Growth of the amount of data produced can be divided into two by different source origins; produced by humans and produced by machines. In the early stages of the information era, we humans as data subjects were responsible for the biggest portion of produced data. Portability of the smartphones played a key role here as it enabled smartphones to be carried everywhere we went. The more smartphones are with us, the more we are connected to the Internet and thus produce data. Without the portability function of the smartphone the situation could have been completely different. Consider a scenario where a smartphone would still have physical buttons and 1,5-inch non-touchscreen and weight 5 kilograms. Would smartphones still hold the same status as it currently has?

The second source are Internet of Things (IoT) devices – data is produced by machines and sensors. IoT devices are considered to be smart in, at least, some way. It is simple to draw the line between normal a device and an IoT device. In order for a product to be considered smart, it 1) has to be ability to connect to the Internet in any way, and 2) sensors and software of the

[5] 'What Is Network Society' (Igi-global.com) <https://www.igi-global.com/dictionary/network-society/20182> accessed 24 March 2022.

[6] Michalis Zinieris, 'Data: A Small Four-Letter Word Which Has Grown Exponentially To Such A Big Value' (Deloitte Cyprus) <https://www2.deloitte.com/cy/en/pages/technology/articles/data-grown-big-value.html> accessed 15 April 2022.

device must have technology with supports network connections and actuators.[7] IoT devices include, for example, laptops, smart watches, smart vehicles and smart gadgets.

Another feature to the smartphone is its role as the center of our daily activities and our attention. The increased usage of smartphones is closely related to the amount of mobile applications (“apps”) available for us to focus our attention to. Smartphones have been such a success story that the amount of smartphones is estimated to have around 6,3 Billion users across the world.[8] The popularity of apps has increased steadily as the popularity of smartphones. These can be downloaded from Apple’s App Store or Google’s Play Store. Combined there are over 4,5 million apps to download. A recent study shows that in the US, an average consumer checks smartphone whopping 262 times per day.[9]

After explaining how dramatically the popularity of smartphones has increased and how much data we do produce, it should not come as a surprise that data is considered by some measures to be more valuable than oil. According to recent estimations, data has surpassed oil in its value.[10] Data’s worth cannot be yet measured by traditional means, but it has been understood to hold a certain value since data can be used for so many purposes. This can be observed by the fact that companies, whose business is not data driven and not related to data collection at all, still collect larger amounts of data because of the potential value in it. One data point does not hold large value, but a large dataset might. Thus data’s value essentially comes from its potential to be refined into an essential commodity.[11]

Countries and organisations have understood the importance of data and protecting it. Data protection as a field has grown in popularity within the last decade. Even though it is a relatively new field, it is slowly evolving. This can cause trouble as the technology field is in a stage of constant change. For example, if the use of cookies would be prohibited from this day onwards, it is highly possible that the technology sector would come up with a way around the

[7] '18 Most Popular Iot Devices In 2022 (Only Noteworthy Iot Products)' (https://www.softwaretestinghelp.com/, 2022) <https://www.softwaretestinghelp.com/iot-devices/> accessed 3 March 2022.

[8] 'Mobile App Download Statistics & Usage Statistics (2022) - Buildfire' (BuildFire, 2022) <https://buildfire.com/app-statistics/> accessed 10 April 2022.

[9] 'Mobile App Download Statistics & Usage Statistics (2022) - Buildfire' (BuildFire, 2022) <https://buildfire.com/app-statistics/> accessed 10 April 2022. https://buildfire.com/app-statistics/

[10] 'Data Is More Valuable Than Oil – Tidalscale' (Tidalscale.com) <https://www.tidalscale.com/data-is-more-valuable-than-oil/> accessed 3 May 2022.

[11] Theresa Fauerbach, 'More Valuable Than Oil, Data Reigns In Today’s Data Economy' <https://www.northridgegroup.com/blog/more-valuable-than-oil-data-reigns-in-todays-data-economy/> accessed 26 April 2022.

prohibition. I guess no one has a problem with cookies if they are used for improving services but the problem lies within the unwanted use of the information.

More than ever is our world connected which means data is flowing across nation’s borders. We are just starting to grasp all the ways data can be used. Depending on the actor, data can be used for different purposes. One actor might use it to offer personalised content and advertisements. On the other hand, it can even be used in an anonymized form to teach artificial intelligence to improve cancer diagnostics. Disregard the large scale of use cases for which data can be used, I consider the free flow of data being a good thing for the whole humankind. My only caution is that it should be protected and used for those purposes that it was acquired to. Something that we have to realise by now is that it is, by its virtue, borderless.

It is the personal opinion of the writer that all actors in the international plane benefit from being connected and from working together towards a better future for all. I strongly believe that only by working together can we achieve the best results. It is understandable this eager goal possesses problems because different jurisdictions operate according to different principles and have differentiating values. For some time now, some members of the EU have been displaying a trend of moving towards protectionist ideology in relation to data protection rules. Keeping in mind that the EU’s GDPR is already one of the strictest privacy laws in the world. Imagining something like that seems hard in this connected world. There is a potential to halt, or cause disruptions, to the free flow of data. In addition, it could potentially lead to economically disadvantageous settings where companies might not see the value of operating anymore. All this might sound like something from far away, but as we will later explore with the Facebook saga, it could be possible, nevertheless.

For this thesis I will be considering two counterparts, the EU, and the US. Both of which have different approaches to privacy. While reading this thesis, it should be kept in mind that the EU has introduced laws and regulations that control transfers of personal data outside the European Economic Area (EEA). In addition, it should be noted that there are countries included in the EEA that are participants of the EU data protection laws alongside the EU member states. I intend to use the term EU as a reference for the sake of simplicity. This is not intended to undermine those countries’ important contribution to the EU data protection laws, but rather make comparison of the EU and US data protection field more readable for the viewer.

1.1 Purpose and Research Questions

The purpose of this thesis is to provide an extensive overview of the world of data protection as it currently stands from the European point of view. This includes taking in depth look at the events that have had an effect on the data protection and thus have impacted the formation of the current European Union's data protection regulation "General Data Protection Regulation" (GDPR). Noteworthy is to point out that the GDPR was supposed to be accompanied by the E-Privacy Regulation[12] which was supposed to be replacing the Directive 2002/58/EC (E-Privacy Directive) from 2002. Unfortunately, E-Privacy Regulation has not seen massive progress in the years that have passed since the GDPR went into effect. The importance here is from the companies and organisations point of view that are operating on a global scale, they are international by their nature which means they have to comply with legislations in different jurisdictions. All this builds up to my first research question which is **in what ways the current data protection regulation does not work and why is that?**

My second research question is **how technology could assist in resolving the current problems the data protection industry is facing?** For this reason the thesis will have a deeper and more technical side to a thesis as well. I will start from the standpoint that the reader should thoroughly understand concepts such as data and encryption in detail in order to understand data protection regulations. Having this thorough knowledge will play a key role in assessing whether data protection regulation works as it currently stands and where have we come this far. This relates to problems data protection is facing and the problems have to do with uncertainty and the problem of having to rely on another party. The old saying "know your roots" applies here as well. Furthermore, as an important feature of this thesis I will explore the political aspect to data protection regulation. In order to evaluate the political aspect I have chosen the European Union and the United States as the relevant parties for my thesis.

In relation to the political aspect of data protection, I write this thesis with a different view to data protection and the issues it is currently facing. I will do this by evaluating data protection from a deeper perspective in a way that what if data protection would not be political at all? What if the underlying problems the field is facing could be resolved by addressing the core problems and using technology to our benefit in the quest of finding a working solution. To support this thinking I will present an innovative technology that could, in my opinion, resolve

[12] 'Proposal For An Eprivacy Regulation' (Shaping Europe's digital future) <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation> accessed 1 May 2022.

the key concerns data protection is currently facing and this would help organisations by providing stability as compared to changing political mood.

I have purposefully chosen the EU and the US as the parties I will assess in relation to international data transfers. The EU and the US come from very different approaches to personal data, and this sets up nicely to the difficulty of the data protection regulation. Major reason for this is that the EU is a major player in the international plane from personal data point of view and the US is the location where most of personal data is flowing towards due to large technology companies originating from there. Flow of personal data plays a key role as large companies have built around data and data analysis which relates closely to the advertisement industry.

1.2 Structure

This thesis follows a logical chronological order in which data protection has evolved and events have occurred. I would really love to write about every single event that has occurred but due to limitations I have to focus on the large-scale events that did take place. The thesis begins with introducing the evolution of our world towards an information centred global place which is more interconnected than ever before. Gaining this knowledge is important to understand how far technological innovations have helped us come and the benefits of these new innovations. Furthermore, similar to a coin, innovations have two sides to them and sometimes there are unintended by-products as a result of these innovations. We will see that even the best innovations can be turned upside down and used for different purposes depending on what perspective is the most beneficial.

First, I will introduce a regulatory scheme that was in place long before data protection and the importance of it became such an important topic in the current world. Here I am referring to the European Union (EU) Directive 95/46/EC which came to be known as the “Data Protection Directive” (DPD). The DPD was a first of its kind in the EU and that made it revolutionary. It set the tone for all further data protection related discussions and regulations to come. The section about the DPD helps the reader to understand the underlying importance of focusing on the real issues, not figuring out a way around by different means. Implications of the DPD could have not been seen beforehand. Essentially, the DPD was the first data protection legislation that started the EU’s journey towards high data protection standards and also prohibited personal data transfers outside the EU if certain conditions were met. This includes the other party in this thesis – the US. Furthermore, the DPD gave the Commission power to assess if adequate level of protection could be ensured in a third country and thus if the personal data could be transferred there. Now we can understand that the stage is set for politics to enter the world of data protection. This is the very first origin of the political aspect to data protection.

Afterwards, the thesis observes the first political agreement between the EU and the US to allow free flow of personal data between the two. In 2000, the Safe Harbour principles were introduced to allow this flow of personal data. Safe Harbour principles were intended to provide security to ensure adequate level of protection that was needed for third-country transfers such as the US that was not considered to have the EU standards matching privacy legislation without further guarantees. The thesis will evaluate the Safe Harbour principles and whether it was a working solution to tackle the problems in data protection. Safe Harbour principles were questioned at points but remained largely untouched until the event that shocked the privacy world and started the collapse of politically agreed data protection agreements. The Snowden revelations came to be known as the point when data protection measures started to be questioned.

Next, the thesis will logically progress forward in a chronological order by moving to the next big scale event which was the invalidation of Safe Harbour principles as a result of the Court of Justice of the European Union (CJEU) case brought by Max Schrems. The case would later be known as the Schrems I ruling which had a large-scale impact on the data protection community. A lot happened during a period of one year as the next major event took place when the current EU wide data protection regulation – GDPR – was adopted on 27th of April 2016 with a later set date for coming into force on 25th of May 2018. Not long after the Safe Harbour was invalidated and the GDPR was adopted, the Privacy Shield, the second political data protection agreement, was announced on 12th of July 2016. Privacy Shield had the same aim as its predecessor, to ensure security of personal data transfers between the EU and the US and most importantly enable the free flow of this information.

Next in line is to move and analyse the CJEU case Facebook Ireland and Schrems, also known as the Schrems II case, that was laid down on 16th of July 2020. This decision was another major case that sent shockwaves across the data protection waters because once again the political agreement had been found not doing what it was supposed to do. It was apparent that it failed to ensure the same level of data protection similar to the EU. Schrems II case relates to the long saga of Max Schrems against Facebook. Here the political aspect of data protection regulation should be clear.

At this point of the thesis, the reader should have a detailed understanding of the data protection from the regulatory side of things. Now I would like to continue and focus on the deeper level of understanding data protection. This means digging deep into the grassroot level into data. Questions such as what data is, why it is valuable, why it needs to be protected, how it can be protected and more, are answered in this next chapter. I consider this chapter highly important for the overall experience of this thesis because understanding what is below the surface can often help resolve problems laying above it.

Coming to a near end of the thesis, the reader should by now have understanding of data protection legislation, deeper knowledge of data and encryption and, in addition, understand the underlying problems with data protection. Next chapter focuses on the analysing previously discussed points of the thesis such as political nature and technical details. Furthermore, this chapter will focus on the future of data protection and discusses this by going through technical means of resolving underlying problems and also the political aspect. Here I will present what I believe could solve the underlying problem of data protection, and if not solve, at least be part of the solution without having to trust for another political decision on the matter.

Lastly, I will do a conclusion that tries to wrap up the whole thesis from the beginning to the end. Including extensive chapters on regulation, data and future. I will clarify the idea behind the thesis which I have hopefully managed to provide to the reader as this thesis is going to be read. Furthermore, I will critically evaluate how well research questions were answered, the outcomes of them and what was learned as a result of the thesis.

1.3 Research methodology

This thesis logically follows legal dogmatic methodology based on legal and doctrinal research materials with a focus on the importance of well-functioning data protection legislation by placing an interest towards technology-based approach rather than political. Furthermore, understanding the current situation requires in-depth understanding of the past which plays an important factor in the research material. Undermining how the past reflects current is something this thesis will not do. Emerson Tiller and Frank Cross summarize legal doctrine in a way that suits this thesis: “Legal doctrine is the currency of the law. In many respects, doctrine, or precedent, is the law, at least as it comes from courts. Judicial opinions create the rules or standards that comprise legal doctrine… Legal doctrine sets the terms for future resolution of cases in an area. Doctrine may take many forms, it may be fact dependent, and therefore limited, or sweeping in its breadth".[13] Here is highlighted best the purpose of creating consistent legal rules for the long-term in a field that is divided but can be unified. There is so much potential in modern technologies and their usability. This is a factor that should be accounted for when considering data protection's future as well as resolving the underlying problems hands-on approach.

As we understand data protection is both political and technical in its nature: I possess an understanding that it might be the easy way forward to have respective officials negotiate a common approach that is followed until something goes wrong, and I can truly see why this has been the case so far. I consider we should pour down more resources and time to consider other possibilities out there. One way to do this is think outside the box in order to have progressive ideas that could foster better results in the long-term. We should not be short-sighted with such an important topic.

The most important research material and base for the analysis lies mostly in the legal framework of the European Union, such as the General Data Protection Regulation, the Data Protection Directive and the Commission decision on the adequacy of the protection provided by the Safe Harbour privacy principles. Furthermore, legislations are complemented with the case law of the Court of the Justice of the European Union and smaller decisions made by, for example, the Irish Data Protection Commissioner. As the thesis is partly highly technical in nature, the sources related to chapters can be technical rather than legal and should be accounted for due to the special nature of the thesis. Further procedures such as recommendations, doctrinal sources and statistical material is also included in the research as a whole.

Before the GDPR came into force, the DPD was the main legal source when it came to processing personal information. Further along came the Commission decision on the adequacy of Safe Harbour principles which enabled free flow of information in an international plane between the two parties – the EU and the US. It should be noted that neutral countries such as Switzerland have followed the EU's suit and had their own Safe Harbour principles, Privacy Shield and are part of the GDPR as well. Here we can clearly see that neutrality is favouring workable solutions.

This thesis has a positive approach towards technology and has adopted the view that it does benefit the society as a whole. I am sure most people will agree with me, at least, partly. What

[13] Emerson H. Tiller and Frank B. Cross, 'What Is Legal Doctrine?' [2005] SSRN Electronic Journal <https://core.ac.uk/download/pdf/76622332.pdf> accessed 5 April 2022. p.1.

comes to the downsides of technology will be considered carefully as well, but overall technology is surrounded with a positive approach. On the contrary, political decisions do not have the same positive approach towards them. I have adopted a view that if they do work there is nothing wrong with having a political decision to ease up the difficulties. However, this will be demonstrated in the thesis that unfortunately political decisions do not stand longevity and are subject to renew.

2 Regulatory framework

2.1 Directive 95/46/EC – The Data Protection Directive

Directive 95/46/EC, or more commonly known as the Data Protection Directive (hereinafter referred as the DPD), was adopted by the European Union (EU) back in 1995. The DPD can be regarded as the first EU-wide legislation aimed at the protection of individuals and their personal data. An attempt was made to combine the need for protection of personal data without halting free movement of data. The Directive had clear goals; standardise and secure the free flow of data in a manner that did not compromise the protection of personal data that is moving across national borders. Consequently, data containing personal information meant from now onwards more than just zeros and ones, it was regarded as a fundamental right.

As a directive, the DPD sets out objectives to member States which they need to transform into their national legislation. Even though the objectives are defined in a clear way, Member States have some say on the way they decide to implement objectives of the directive due to respective national differences. The directive sets the minimum requirement which leaves Member States the possibility to implement stricter national requirements. As a result, it was possible for one Member State to have stricter legislation than the neighbouring Member State. Logically, this caused the Directive to be applied in a different way across the EU. This is one of the reasons why the EU is currently moving away from directives towards regulations.

2.1.1 Adequate data protection measures – Safe Harbour Principles 2000

The DPD was intended to be Union wide data protection legislation and thus a key component in the protection of privacy and human rights of the EU citizens. It laid down rules for the processing of personal data – storage and transfer – within the EU. In addition, the DPD introduced a new concept into the field of data protection called “an adequate level of data protection”. This vague concept would later turn out to be an extremely meaningful one because it was the only obstacle standing between a third country whether having all rights to process data from the EU or not having that right. The responsible EU body to have this power to issue adequacy decisions was placed on the European Commission (the Commission). The term “adequacy decisions” has bigger power than I believe it was intended to have.

By default, the DPD set forth a prohibition on the personal data transfers to third countries such as the US. However, this did not make data transfers to third countries impossible, but it required an adequacy decision issued by the Commission.

Adequacy was evaluated based on data protection measures in place in the receiving country to ensure security of the data transferred or processed there. The US, as the center of information technology companies, was one of the main destinations to where personal data was flowing. That did not stop the EU from not issuing an adequacy decision to the US. US national laws were seen as not corresponding to themselves with the EU values. Nevertheless, there was a commercial interest to enable free flow of information between the EU and the US. Because DPD prohibited transfers outside EEA, a way to ensure free flow of data needed to be invented while ensuring the security of the personal information.

One concern was the unauthorised access of the data or the loss of personal data. Together, the EU and the US officials negotiated a set of principles that ensured future data processing operations complied with the requirements set out in the DPD. The result was called the "Safe Harbor Privacy Principles". In 2000, the European Commission exercised its powers and adopted a decision declaring the transfers to the US being safe.[14] The Decision was based on the newly negotiated principles and would inherit the name "Safe Harbor Framework". The Framework consisted of seven key principles that were the following:[15]

1. Notice - The data subject should be informed that their data has been collected, how it will be used and how to contact the data holder for any queries.

2. Choice - The data subject should be able to opt out as well as forward the relevant data to another third party.

3. Onward Transfer - The transfer of any data can only happen with a third party that meets the required data protection principles.

4. Security - A reasonable effort must be made to keep the data safe from loss/theft.

[14] 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 2000/520/EC.

[15] 'What Is The Safe Harbour Agreement? | Experian Business' (Experian.co.uk) <https://www.experian.co.uk/business/glossary/safe-harbour-agreement/> accessed 8 April 2022.

5. Data Integrity - The data must be relevant and reliable for its original purpose of collection.

6. Access - The data subject should be able to access, correct and delete any information held about them.

7. Enforcement - There must be effective means of enforcing these rules.

In essence, the program consisted of only a few requirements; US companies had the option to comply with requirements of the DPD by adhering to the seven key principles and 15 privacy questions, and then "certify" in writing that it agrees to comply with the principles of Safe Harbor framework. Certification was done either by the company itself as a self-assessment or by a third-party assessment. Understandably, this led to a situation where companies would rather self-certify that they were complying with the requirements rather than paying for external reviewers. Companies that agreed to the terms were given the permission to freely process personal data from the EU under the Safe Harbor framework. Notable is that the program was voluntary and was not available to all organisations. Only private organisations regulated by the Federal Trade Commission (FTC), or the Department of Transportation (DOT) were allowed to participate in the program.

2.1.2 Self-certification

As mentioned in the previous section, the DPD laid down rules that prohibited transfers of personal data to third countries unless they were able to prove that adequate protective methods for data were in place. In order to ensure efficient transfers between the EU and the US, a mutual agreement was reached that ensure security of transfers to the US and would bear the name Safe Harbour Principles. Safe Harbour scheme provided for the participating US companies with two options; either to self-certify or have a third-party conduct an assessment. Self-certification was the term used to describe the actions by the US companies where they asserted their commitment to comply with the Safe Harbour Principles. With the certification, the companies demonstrated that they meet the EU data protection standards and thus were permitted to process and store personal data originating from the EU.

Self-certification would bear the cost of $ 100 annually. Even though there is no data regarding the cost for certification done by a third-party audit, that is why we have to assume it did cost more than the cost of self-certification because a third-party requires thorough assessment into organisations operations. The sheer lack of data regarding third-party certification speaks to the unpopularity of this option. To get sense of what could have been the cost, we can consider the ISO certification for the sake of comparison. Average ISO certification requires thorough assessment, and it costs around $ 3000 to 5000 annually.[16] A third-party assessment requires a company to demonstrate to an independent third party - that has no previous knowledge of the company – their procedures and operations. It is a classic case example of cost and benefit analysis. Nevertheless, independent third-party assessment offers a more reliable overview of the data protection level in a company when compared to companies self-certifying themselves. The Safe Harbour scheme did not provide any incentives to conduct third-party assessments. Cost analysis clearly favoured self-certification as the less-costly option.

Joining the Safe Harbour scheme was not a difficult task but reeked many benefits. An entry requirement was that the company had to be a private organisation regulated by the Federal Trade Commission (FTC) or the Department of Transportation (DOT). Secondly, a company only had to 1) read the Safe Harbour overview, 2) go through Safe Harbour documents, 3) review compliance requirements, 4) bring organisation's policies to compliance with the Safe Harbour, and 5) submit the application.[17] After completing the steps, a company was allowed to process personal data originating from the EU.

According to the press release by the European Parliament, over 4000 US companies were relying on the Safe Harbour scheme to transfer personal data.[18] Years later, we can say without a doubt that in the end the protection of personal data relied on the self-assessment of the private organisations. As we later found out, the Safe Harbour scheme did not provide the adequate level of protection that was required of it to allow the personal data transfers. What comes to self-certification, who is to blame? If we create a situation where one benefits a lot by doing the bare minimum without the fear of supervision, what else can we expect from this situation?

2.1.3 Schrems I and the invalidation of the Safe Harbour scheme

The Court of Justice of the European Union (CJEU) case - C-362/14 Maximillian Schrems v Data Protection Commissioner – or better known as the Schrems I case, was a landmark case in the field of international data protection. What seemed to be a small complaint made by one

[16] 'The Cost Of ISO Certification - ISO Update' (ISO Update, 2020) <https://isoupdate.com/general/the-cost-of-iso-certification/> accessed 13 April 2022.

[17] 'Welcome To The U.S.-EU Safe Harbor' (export.gov, 2017) <https://2016.export.gov/safeharbor/eu/eg_main_018365.asp> accessed 3 April 2022.

[18] European Parliament, 'Safe Harbour Ruling: Meps Called For Clarity And Effective Protection' (2015) <https://www.europarl.europa.eu/news/en/press-room/20151015IPR97903/safe-harbour-ruling-meps-called-for-clarity-and-effective-protection> accessed 10 April 2022.

individual against the tech giant Facebook, turned out to be one of the biggest privacy case in recent history. This is a case which has shaped the future of Europe in many ways. I bet the future impact could have been evaluated when the CJEU gave its judgement on the matter. Without Edward Snowden's revelations, it is possible that Schrems would have not been concerned about the data flows to the US and would have not lodged his complaint in 2013 to the Data Protection Commissioner .

In order to understand exactly how Max Schrems' complaint ended up shaking the world of data protection, we have to go back to the beginning. Max Schrems is an Austrian citizen, and he became worried about the security of his data in Facebook. What made him so concerned about the security of his data was the shocking Snowden revelations that had come into light less than month before he lodged his claim. Edward Snowden revelations[19] took place in the early days of June 2013, and they revealed the extent of US surveillance coverage. Secret practices that the US was doing to conduct surveillance were now public information. In my opinion, the event rightfully caused concern about the security of personal data transferred from the EU to the US. Exactly how well protected was that personal information after all? This question was to be answered by the CJEU during what was to be known as Schrems I case.

The Snowden revelations showed that surveillance overrides the protection of data, and the reach of NSA's world-wide spying on other countries. Max Schrems based his complaint on the basis that the recent revelation clearly demonstrated that the US could not provide "adequate level of data protection" which was a requirement by the DPD and was supposed to be guaranteed by the Safe Harbour Principles. I see Snowden revelations to be the tilting point in the data protection in which the shift from old practices towards new ones started. Up until the revelations became known to the public, personal data had been moving freely without major supervision between the EU and the US. This was a first step in a long sequel of occurrences to be happening that would determine under which condition the EU – US transfers could be done while remaining compliant. The decision of the Court had a huge impact as it took down the 15-year-old regime for data transfers between the EU and the US.

2.1.4 Safe Harbour aftermath

The Safe Harbour Principles had long been the mechanism used for the personal data transfers between the EU and the US. As the CJEU judgement ruled the Safe Harbour Principles was

[19] 'Snowden Revelations' (Lawfare) <https://www.lawfareblog.com/snowden-revelations> accessed 2 May 2022.

invalid and could no longer be used, there was a need to find a way to keep the transfers going on. It should be noted that the CJEU ruling did not prohibit all transfers of personal data to the US and ruled them unlawful, rather the judgement invalidated the framework that had been used to transfer personal data freely. The ruling pointed out that national supervisory authorities had the power to evaluate whether a third country could provide adequate level of protection to transfers of personal data.[20] Because of this the continuation of transfers to the US could be ensured by using less known mechanism for transfer, namely derogations listed in the Article 26 of the DPD – the standard contractual clauses.

Back in 2015, SCCs were a little-known mechanism of transfers, but as we now know, they will become the main mechanism for transferring personal data later on. This was years away as officials attempted to resolve the matter by political decision. Following the invalidation of the Safe Harbour Framework, many companies were left struggling on how to proceed with the data transfer.

2.2 General Data Protection Regulation

General Data Protection Regulation (GDPR) is considered one of the toughest data protection legislations in the world.[21] It was published 27th of April 2016 and came into effect 25th of May 2018. It is a legal framework that controls the collection and processing of personal information of individuals located in the European Union (EU). Here the GDPR draws its line between those who are afforded the protection and those who are enjoying the protection of the GDPR. There is a specific requirement of residency. Residency requirement requires the personal data of an individual residing in an EU country to be subject to safeguards and their data rights and freedoms must be protected[22]. At first glance this does not appear that big a deal, but the GDPR has surprisingly large extent to its application. Because GDPR affords certain protection to individuals residing in the EU regardless of their citizenship, it ends up applying to a large portion of the world’s protection. According to Eurostat, close to 450 million inhabitants are residing in the EU.[23]

[20] Case C-362/14 Schrems [2015] ECLI:EU:C:2015:650

[21] Ben Wolford, 'What Is GDPR, The EU’S New Data Protection Law? - GDPR.Eu' (GDPR.eu) <https://gdpr.eu/what-is-gdpr/> accessed 2 May 2022.

[22] HIPAA Journal, 'Does GDPR Apply To EU Citizens Living In The US?' (HIPAA Journal, 2021) <https://www.hipaajournal.com/does-gdpr-apply-to-eu-citizens-living-in-the-us/> accessed 1 May 2022. https://www.hipaajournal.com/does-gdpr-apply-to-eu-citizens-living-in-the-us/

[23] 'Area By NUTS 3 Region' (Eurostat, 2021).

If we can understand that the world is a global place and data is moving on the internet and processed in the cloud storages, surely we can understand the importance of the GDPR. Even though a business is not established in the EU, it still has to comply with the rules of GDPR if it processes data of the EU citizen. This places an obligation on multinational companies to comply with the data protection rules of another region. Furthermore, not only businesses but all organisations no matter public or private are subject to the GDPR if they process the data. This has had an effect on businesses and organisations regardless of their size. Overall, this might be the most important point of GDPR to emphasise because businesses are global, they are international actors operating in many countries.

There is no physical presence requirement of organisation in the EU for an organisation to be subject to GDPR. It is rather simple: all organisations need to comply with the GDPR if they process data of the EU citizens. For example, if you have a website and an individual from the EU enters your website, you are processing the data of EU citizen and thus you need to comply with the GDPR. This led to extreme scenarios where business owners blocked EU users from entering their website. This was more common in 2018 than it is now, but websites such as the Baltimore Sun (www.baltimoresun.com)[24] cannot be entered from the EU today. Only thing you get is a notice that “website is currently unavailable in your country”. For clarification purposes, it is important to note that there are exceptions to the applicability of the GDPR as there are always in large-scale legislations. Requirements for the applicability are the following: data of EU citizens is processed regularly; rights and freedoms of the data subjects may be at risk and if the data processed is related to special data categories. For the sake of simplicity, it is more consistent to assume that everyone needs to comply with the requirements of the GDPR.

Similarly to the DPD, the GDPR requires that data transfers outside the EU can only take place to a country where adequate level of data protection can be ensured. Understandably, the US did not make the shortlist – currently 14 countries have made the list - after the Schrems I case which was based on the 2013 surveillance revelations.

2.2.1 Privacy Shield

Privacy Shield is the term used to refer to the framework agreement conducted between the EU and the US. The agreement made it possible to ensure continuation of the transatlantic personal data flows between the EU and the US. It was unveiled by the European Commission on 29th

[24] www.baltimoresun.com

of February 2016 with the intention of restoring trust to data transfers taking place between the two. Officials managed to negotiate a political consensus for the transfers in less than six months. We can say with certainty that the issue of data protection is more political in nature and can be sensitive in that regard. However, they are not resolved that way. Privacy shield intended to ensure high levels of data protection, especially in relation to law enforcement.

Privacy shield introduced stronger supervision and enforcement of activities by the organisations of the U.S. Government, it improved co-operation and transparency, introduced new privacy protection for the EU individuals and enhanced complaint resolution. Furthermore, it introduced Seven Key principles to adhere to. Now, seven principles of data protection agreement should sound familiar to the reader. The Safe Harbour framework also contained Seven Key principles for the enhancement of data protection. We can observe from the principles that there is a true intent behind the agreement. Unfortunately, these Seven Key principles do look awfully similar to the late Safe Harbour framework's seven key principles. I hope I am wrong, but it feels like data protection is only a political issue. From the table[25][26] below we can observe the differences, or the similarities, of the two politically negotiated frameworks to ensure maximum data security.

Safe Harbour Framework 7 key principles:	Privacy Shield Framework 7 key principles:
Notice - The data subject should be informed that their data has been collected, how it will be used and how to contact the data holder for any queries.	Notice: Organisations must publish privacy notices containing specific information about their participation in the Privacy Shield Framework; their privacy practices, and EU residents' data use, collection, and sharing with third parties.
Choice - The data subject should be able to opt out as well as forward the relevant data to another third party.	Organisations must provide a mechanism for individuals to opt out of having personal information disclosed to a third party or used for a different purpose than that for which it

[25] 'Federal Trade Commission Enforcement Of The U.S.-EU And U.S.-Swiss Safe Harbor Frameworks' (*Federal Trade Commission*, 2012) <https://www.ftc.gov/business-guidance/resources/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor-frameworks> accessed 9 April 2022.

[26] Impact Advisors, '7 Principles Of The EU-U.S. Privacy Shield Framework - Impact Advisors' (*Impact Advisors*) <https://www.impact-advisors.com/security/eu-us-privacy-shield-framework/> accessed 10 March 2022.
https://www.impact-advisors.com/security/eu-us-privacy-shield-framework/

	was provided. Opt-in consent is required for sharing sensitive information with a third party or its use for a new purpose.
Onward Transfer - The transfer of any data can only happen with a third party that meets the required data protection principles.	Accountability for Onward Transfer: Organisations must enter into contracts with third parties or agents who will process personal data for and on behalf of the organisation, which require them to process or transfer personal data in a manner consistent with the Privacy Shield principles.
Security - A reasonable effort must be made to keep the data safe from loss/theft.	Security: Organisations must take reasonable and appropriate measures to protect personal data from loss, misuse, unauthorised access, disclosure, alteration and destruction, while accounting for risks involved and nature of the personal data.
Data Integrity - The data must be relevant and reliable for its original purpose of collection.	Data Integrity and Purpose Limitation: Organisations must take reasonable steps to limit processing to the purposes for which it was collected and ensure that personal data is accurate, complete, and current.
Access - The data subject should be able to access, correct and delete any information held about them.	Access: Organisations must provide a method by which the data subjects can request access, correct, amend, or delete information the organisation holds about them.
Enforcement - There must be effective means of enforcing these rules.	Recourse, Enforcement and Liability: This principle addresses the recourse for individuals affected by non-compliance; consequences to organisations for non-compliance; and compliance verification.

The striking similarities between the two frameworks is evident. These seven key principles act as the core of the political agreement which is intended to change the status from prohibited to transfer allowed. Sceptical me has to wonder how much political influence does large multinational tech companies have to ensure data flows continue flowing smoothly? This is something we will look more closely in the upcoming section with Facebook as a case example to study.

2.2.2 Adequacy decisions

Adequacy decisions are referred to as a situation in which the European Commission has the power to determine whether or not a non-EU country (third country) can ensure adequate level of data protection, similar to the EU's standard. With the GDPR's entry into force, the Commission's power derives from the Article 45(1) "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation".[27] Paragraph 2 of the Article 45 states the following: when assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

> a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in

[27] Article 45(1) of the General Data Protection Regulation

> exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Now that it is established what is meant by adequacy decisions, we need to understand what they mean. In my view, adequacy decisions brought the politics into data protection way back when the DPD was introduced. It allowed sway in the assessment of adequate level of protection. Having adequacy decisions in this form opened the door to politics to enter into the field of data protection.

Currently, the Commission is required to ask for an opinion from the European Data Protection Board (EDPB) and get an approval from representatives of EU countries.[28] It seems there are safeguards in place against political influence, but this is something we do not have absolute certainty of. What I would have suggested instead is that EDPB does not only give an opinion, but they should also approve the proposal from the Commission as the EDPB's role as an independent body with the sole purpose of ensure GDPR is applied consistently across the EU and to promote cooperation among the EU's data protection authorities.[29] I believe this way we the data protection aspect of every proposal could be examined always with privacy as a priority prevailing other interests. Furthermore, this would clear by far any doubts of political decision-making having influence over adequacy decisions. Political play is something that has been suggested by None of Your Business (NOYB), a non-profit organisation working to enhance EU's privacy rights, with the timely announcement of Privacy Shield 2.0.[30]

2.3 Schrems II case and Facebook saga

Facebook serves to demonstrate the political aspects of the current data protection landscape and by Facebook I am referring to a larger entirety than simply one court case. Multinational

[28] 'Adequacy Decisions' (European Commission - European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 3 April 2022.

[29] European Data Protection Board, Who Are We <https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en/> Accessed 25 April 2022.

[30] Max Schrems, '"Privacy Shield 2.0"? - First Reaction By Max Schrems' (noyb.eu, 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 7 April 2022. https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems

companies such as Facebook and Google are subjects of various data protection regulations which they need to comply with. If data protection measures are essentially political in nature, the question arises of how much sway can large multinational technology companies, worth trillions of dollars, have? In this chapter, my intention is to look at the CJEU's case Facebook Ireland and Schrems (2020) [C-311/18], or better known as the Schrems II decision. Schrems II decision essentially invalidated the EU-US Privacy Shield, a political framework that was used for international data transfers after the invalidation of Safe Harbour. The decision did not question the validity of the Standard Contractual Clauses (SCCs) as an alternative mechanism for international data transfers. However, the CJEU placed the responsibility of ensuring an equivalent level of protection on the data importer and exporter which has to be done on a case-by-case basis and what supplementary measures should be taken in order to provide additional safeguards. In summary, SCCs alone do not comply with the Schrems II ruling as the ruling required additional "supplementary measures" to be in place in order to make the international data transfer to third-countries possible. Shortly after the CJEU came up with the Schrems II decision, Facebook received a preliminary decision from the Irish Data Protection Commissioner (DPC) to stop data transfers between its European headquarters and Facebook USA. I will explore the events that have taken place after the Schrems II decision, how it has impacted the data protection field and the objections Facebook has applied to delay the final decision prohibiting the transfers by the Irish DPC.

Since the Schrems II decision caused uncertainty among privacy specialists and companies relying on fluent EU-US data transfers in their daily operations, we have seen how uncertainty breeds complexity around data transfers because companies want to be compliant but do not know how to and the fear of fines remains. Schrems II ruling left companies somewhat out in the open with no clear understanding on how to proceed forward. Privacy shield was a framework that had been in place for four years and more than 5000 companies relied on the framework to transfer data between the EU and the US. However, the CJEU stated that standard contractual clauses (SCCs) could be used as an alternative transfer mechanism if they are accompanied by additional safeguards – supplementary contractual commitments to ensure security of the data transfers.[31] Keeping in mind that the evaluation of whether the receiving party of transfers could respect the level of data protection required by the GDPR and what supplementary measures should be taken, was left for the parties of the transfer to decide. Ultimately, the evaluation whether supplementary measures are sufficient enough is based

[31] Case C-311/18 Facebook Ireland and Schrems [2020] ECLI:EU:C:2020:559 119.

solely on the assessment of the respective national data protection authority. Therefore, there was a lack of uniformity after the Schrems II decision. Furthermore, the CJEU did not invalidate binding corporate rules (BCRs), a less known method for international data transfers for a reason. BCRs are seen as the ”gold standard” for international data transfers. BCRs are subject to regulatory approval which makes them special in this way.[32] We can easily compare the popularity of Privacy Shield compared to BCRs. As previously mentioned, more than 5000 companies relied on Privacy Shield as their transfer mechanism. Compared to 175 companies that are using BCRs as their transfer mechanism.[33]

Many companies were left to wait on further guidance from the European Data Protection Board (EDPB) on the supplementary measures for international data transfers. Finally, almost six months later, on 10th of November 2020, EDPB released its first guidance – draft recommendations - on the long-awaited supplementary measures. The supplementary measures included six steps for companies to follow in order to ensure compliance with the GDPR while transferring data between third countries. The six steps provided guidance and were ultimately adopted to the final EDPB Guidelines. The following steps were: [34]

Step 1: Know your transfers

Step 2: Identify your transfer tools

Step 3: Assessment of legislation in the third country

Step 4: Identify and adopt supplementary measures

Step 5: Necessary formal procedural steps

Step 6: Re-evaluate and monitor at appropriate intervals.

It took another six months to wait for the European Commission to issue the modern version of the standard contractual clauses (new SCCs) but finally this took place on 4th of June 2021.

[32] Lukas Feiler and Wouter Seinen, 'Bcrs As A Robust Alternative To Privacy Shield And Sccs' (Iapp.org, 2020) <https://iapp.org/news/a/binding-corporate-rules-as-a-robust-alternative-to-privacy-shield-and-sccs/> accessed 9 March 2022.

[33] European Data Protection Board, Approved Binding Corporate Rules < https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_el/> Accessed 8 April 2022.

[34] European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted on 10 November 2020) p. 2-3. <https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasures transferstools_en.pdf/> Accessed 12 March 2022.

Main new features of the new SCCs were that they were designed to respond to the requirements of Schrems II case, they modernised the SCCs to reflect GDPR alike approach to data – compared to the old SCCs being framed according to the 1995 DPD, and finally introduced modular approach to include not two but four data transfer parties. There were many more changes introduced, but these were the most important to list a few. It should be noted that the new SCCs are currently in force already, but the old SCCs can be relied upon until 22 December 2022 when they have to be replaced with the new SCCs. However, 27 September 2021 was the last day when you could include old SCCs into a contract. Exactly two weeks after the new SCCs were released, the EDPB introduced its final recommendation to supplement international data transfers to third countries. These remained much similar as the draft recommendations discussed above. Few changes include: 1) focus on the circumstances around the data transfer assessment, 2) organisations must not only consider laws but also practices of the third country and 3) emphasise is placed on the fact that transfers to not adequate third countries shall remain as an exception, not standard practise.[35]

As was mentioned above, after the Schrems II ruling Irish DPC released a preliminary decision that stated Facebook needs to stop data transfers between its EU headquarters and the Facebook USA. Facebook challenged this on many occasions and my take on this is their sole objective was to consume as much time as possible. Finally, on 14 May 2021, Irish High Court rejected Facebook's last attempt to prevent the Irish DPC from ordering Facebook to suspend its data transfers to the US.[36] One could assume that after the rejection from the High Court it would be straightforward to order Facebook to halt data transfers, but unfortunately this is not the case. Fast-forward to February 2022 when Facebook received a revised preliminary decision from the Irish DPC. This time setting a deadline for Facebook's response and setting a timetable for the initial order. Facebook received 28 days – from 21st of February 2022 to make submissions on the preliminary decision after which a draft Article 60 decision is prepared.[37] Unfortunately, there are no guarantees of how long this could potentially drag.

[35] Cynthia O'Donoghue and others, 'EDPB Adopts Final Recommendations On Supplementary Measures Nearly A Year After The CJEU'S Schrems II Ruling' (Technology Law Dispatch, 2021) <https://www.technologylawdispatch.com/2021/07/privacy-data-protection/edpb-adopts-final-recommendations-on-supplementary-measures-nearly-a-year-after-the-cjeus-schrems-ii-ruling/> accessed 9 April 2022.

[36] The high Court judicial review, Facebook Ireland Limited and Data Protection Commission, 14th day of May 2021, [2021] IEHC 336.

[37] Natasha Lomas, 'Meta Sent A New Draft Decision On Its EU-US Data Transfers' (TechCrunch, 2022) <https://techcrunch.com/2022/02/21/dpc-meta-draft-data-transfers-decision/> accessed 23 March 2022.

On 2 February 2022, Facebook's parent company "Meta" submitted its annual report of the fiscal year 2021. In the quarterly report was mentioned growing concerns of the EU-US data transfers and in relation to that the potentiality of Meta leaving the EU behind.[38] Not that long after the "threat" of leaving the EU was circling around in the news, on 25 March 2022 the EU and the US officials announced they have conducted an "agreement in principle" or plans for the next transatlantic transfer framework.[39] Not saying that this was unexpected to come at a certain point in the future nor that having a working framework would be bad, but for the sceptical mind this rather interesting timing appears to raise some questions. Let's do a recap. The Schrems II decision was laid out by the CJEU back in 2020. Since then Facebook has used all procedural delays to stop Irish DPC from providing a final ruling concerning their data transfers.

February 2022, news about Facebook's annual report hit the news and less than two months later the officials announced the "Privacy Shield 2.0". Something that has been in the makings for almost two years. This causes some speculations that could be untrue and without merit, but we need to factor in the timeline in which these occurrences took place. If we remember that the Irish DPC sent Facebook a deadline to answer submissions and Facebook had 28 days to respond. For trained eyes there are almost a perfect overlap between the date of releasing Privacy Shield 2.0 and the deadline for submissions. Just when the national data protection authority was closing in, political decision-makers possibly rendered the upcoming DPC order worthless in this sense. Could it really be that Facebook, 11th most valuable company in the world[40], is large enough corporation that it can persuade officials to come up with a transfer framework just as the Irish DPC is about the deliver their judgement on the Facebook's use of SCCs to enable data transfers between the EU and the US. New transfer framework, being political albeit, provides companies an escape from the situation they were facing with the review of the use of SCCs and their reliability.

[38] Meta Inc., 'ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGE ACT OF 1934 For The Fiscal Year Ended December 31, 2021' (Meta Platforms, Inc 2022) <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf> accessed 14 April 2022.

[39] Max Schrems, '"Privacy Shield 2.0"? - First Reaction By Max Schrems' (noyb.eu, 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 7 April 2022.

[40] Jeran Wittenstein, 'Meta Loses Top-10 Ranking By Market Value Amid Worst Month Ever' Bloomberg (2022) <https://www.bloomberg.com/news/articles/2022-02-17/meta-platforms-falls-from-ranks-of-10-most-valuable-companies> accessed 24 April 2022.

3 Data

At this point of the thesis it is time to dive deeper into the world of data protection. It should be noted that data is not something to be afraid of. In order to proceed, a clear understanding about data is needed. What is data and how is it generated? What are the potential threats towards data and what are the possible ways to protect data? One problem that data protection faces in todays' world is related to the large amounts of data that is produced thanks to latest technological developments in the field such as Internet of Things (IoT) devices. As there are a growing amount of data from a variety of categories available, the important question for this thesis is "what data available are considered to be personal data and thus subject to the data protection regulations"? Another problem faced relates to sensitivity of data and the trust required.

The following text gets technical and demanding at certain points to read, but bear with me as this is essential in order to progress further into the thesis and gain that deeper knowledge. Furthermore, sources in this relation are more of technological nature likewise is the subject at hand. Technology can be viewed from the legal perspective, but certain definitions are needed from the computing sphere. It is noteworthy to point out that data and information are often used interchangeably in popular culture, even though they do not have the same meaning. This largely depends on the perspective they are viewed from. The difference can be demonstrated with the following definition: "data is a collection of facts, while information puts those facts into context"[41].

Let's start with relevant definitions and explain why these are relevant to know. Data is referred to as, and commonly understood to mean, all recorded information regardless of the form on which it may be recorded.[42] Most of this information is stored in electronic form. The Organisation for Economic Co-operation and Development (OECD) defines data as "characteristics or information, usually numerical, that are collected through observation".[43] A more comprehensive definition is needed for thorough explanation about data to cover all

[41] Jon Hill, 'Data Vs Information: What's The Difference?' (Bloomfire, 2021) <https://bloomfire.com/blog/data-vs-information/> accessed 2 May 2022.

[42] '52.227-14 Rights In Data-General.' (Acquisition.gov, 2014) <https://www.acquisition.gov/far/52.227-14> accessed 7 February 2022.

[43] OECD Directorate, 'OECD Glossary Of Statistical Terms - Data Definition' (Glossary of Statistical Terms, 2001) <https://stats.oecd.org/glossary/detail.asp?ID=532> accessed 26 March 2022.

aspects related to it. This serves the objectives of this thesis and taking into consideration the technical nature of this thesis I consider it important.

> Data is “raw facts and figures, such as orders and payments, which are processed into information, such as balance due and quantity on hand. The term data is really the plural of "datum," which is one item of data. But datum is rarely used, and data is used as both singular and plural in practice. The amount of data versus information kept in the computer is a trade-off. Data can be processed into different forms of information, but it takes time to sort and sum transactions. Up-to-date information can provide instant answers. A common misconception is that software is also data. Software is run by the computer. Data are processed. Thus, software causes the computer to process data.”[44]

Essentially, “data” is considered to be raw facts, or raw data, such as numbers, letters, and symbols that have not been processed yet for use.[45] This is the most common approach to data itself by the people coming from the computing sphere. Viewing data as these raw facts that by itself do not have a whole lot of meaning. On the other hand, “information” is understood to mean the meaningful output that has been achieved after processing the data or the raw facts in question.[46] This points out an important factor that is key in today’s world. Data needs to be processed in order for it to become meaningful output – information. Importance of data processing is growing as the amount of available data out there grows. Without processing data, it is only raw information without a meaningful output. Data processing is defined as the process of transforming raw data into meaningful output - information that has relevance.[47]

How is data generated? The sources of data can be divided into two sub-sections: Machine generated and Human generated. Machine generated data refers to the “digital information that is automatically created by the activities and operations of networked devices, including computers, mobile phones, embedded systems, and connected wearable products”[48]. It is unimaginable how much data is generated by these machines and in real time. For example,

[44] 'Definition Of Data' (PCMAG) <https://www.pcmag.com/encyclopedia/term/data> accessed 9 January 2022.

[45] Gavin Wright, 'What Is Raw Data And How Does It Work?' (SearchDataManagement, 2021) <https://www.techtarget.com/searchdatamanagement/definition/raw-data> accessed 15 February 2022.

[46] Chepalskei, 'DATA PROCESSING' (Kenya Cheplaskei Boys High School, 2018). <https://peda.net/kenya/css/subjects/computer-studies/form-three/driac2/data-processing/> Accessed 22 February 2022.

[47] Chepalskei, 'DATA PROCESSING' (Kenya Cheplaskei Boys High School, 2018). <https://peda.net/kenya/css/subjects/computer-studies/form-three/driac2/data-processing/> Accessed 22 February 2022.

[48] 'What Is Machine Data Analytics? | Sumo Logic' (Sumo Logic) <https://www.sumologic.com/glossary/machine-data/> accessed 24 March 2022. https://www.sumologic.com/glossary/machine-data/

activity trackers such as fitness watches are constantly generating data as it tracks your heart rate, distance travelled, body temperature, stress levels, blood oxygen levels and sleep quality. On the other hand, human generated data refers to data generated by us while using social media platforms. This data contains status updates, tweets, photos, videos and texts.[49] The amount of human generated data has increased exponentially as a result of web 2.0. Web 2.0 is a term coined to refer to the current state of the internet, which is ever more user-generated and thus the end-user is active in web 2.0 compared to being passive in web 1.0.

Both machine and human generated data are the sources of Big Data. Term big refers to the sheer amount of the data that traditional databases fail to process. Big data is defined as "high–volume"', high–velocity and/or high–variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization"[50]. To understand the amount of data that is generated and needs to be processed can be demonstrated by an example: Every day more than 4000 terabytes were generated into Facebook's databases, and an airplane's **both jet engines** combined can generate more than 480 terabytes in a day[51]. This difference may not appear that big but considering that Facebook is the largest social media platform in the world with 2,9 Billion active users[52] compared to a set of jet engines. There are many social media platforms alike, but consider how many jet engines there are? Now the perspective might be clearer.

From the perspective of data protection, it is relevant to differentiate what kind of data are relevant and require ensuring integrity of the data. Because not all data is personal data and afforded the protection of the GDPR. Countries and multinational unions have taken similar approaches to define these data, but definitions vary slightly between different economic actors. The European Union has adopted an approach that defines these protection worthy data using the term "personal data". As we know by now, the Data Protection Directive was the predecessor of the General Data Protection Regulation. Before 2016, and until the entry into force of GDPR in 2018, the DPD defined personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can

[49] Mugdha Ghotkar and Priynka Rodke, 'An Outlook On India's Healthcare System With A Medical Case Study And Review On Big Data And Its Importance In Healthcare' [2016] International Journal of Science and Research (IJSR) https://www.ijsr.net p. 1-5.

[50] Salman Zafar, 'How Businesses Can Benefit From Big Data | Techie Loops' (Techie Loops, 2021) <https://techieloops.com/how-businesses-can-benefit-from-big-data/> accessed 16 April 2022.

[51] Nally C, 'How Much Data Does A Jet Engine Produce?' <https://www.mcnallyinstitute.com/how-much-data-does-a-jet-engine-produce/> accessed 9 April 2022.

[52] 'Most Used Social Media 2021 | Statista' (Statista, 2022) <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> accessed 7 April 2022.

be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[53] A definition which may sound comprehensive enough, and certainly was historically when the DPD came into force back in 1995. However, the DPD did not reflect the innovative technological changes of the 21st century. DPDs "personal data" included information such as "name, photo, e-mail address, phone number, address, and personal identification numbers".[54]

With the introduction of the GDPR, the definition of personal data was widened to include recent technological developments. The GDPR defines personal data as "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[55] GDPR widened the scope of personal data to reflect recent changes that were mostly due to technological innovations and the rapid growth of their usage. Now the definition of personal data included, in addition to the data categories of the DPD, IP address, "mobile device identifiers, geo-location data, biometric data, psychological identity, genetic identity, economic status, cultural identity, and social identity"[56].

Before I started working on this project, I did not fully appreciate how comprehensive the definition of personal data is under the GDPR nor did I fully understand all the data that are considered personal data. To this date, I do not think many people and businesses around the world understand it either. For example, contrary to common beliefs, raw data is not always anonymised data and can be an important source of meaningful data and thus should be protected as well, not only the meaningful output. French data protection authority CNIL is recommending that raw datasets are never to be considered anonymous.[57]

[53] Article 2 of the Directive 95/46/EC

[54] SeeUnity, 'The Main Differences Between The DPD And The GDPR And How To Address Those Moving Forward' (2017) <https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf> accessed 13 February 2022.

[55] Article 4 of the General Data Protection Regulation

[56] SeeUnity, 'The Main Differences Between The DPD And The GDPR And How To Address Those Moving Forward' (2017) <https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf> accessed 13 February 2022.

[57] 'Sheet N°1: Identify Personal Data' (https://www.cnil.fr, 2020) <https://www.cnil.fr/en/sheet-ndeg1-identify-personal-data> accessed 2 May 2022.

3.1 Data movements and protective measures

By now the reader should have a general understanding about what data is and the importance of it. In this chapter the thesis will progress to the next logical topic: data movements and protective measures. Having an understanding about these is important for the overall experience of the thesis and provides a deeper understanding into the world of data. So that the reader will not only understand why data needs to be protected but also how it is done at the technical level. Compared to general discussion about the importance of data protection where the importance is stated many times and protective measures are listed, but not explained in a deeper level how these protections are actually ensured. My aim is to provide a deeper understanding at the technical level. After reading this chapter, it is suggested to take a moment and consider how secure our data is really out there? Is your being used the way you thought, or should you consider reviewing certain settings? I should state that I consider myself biased to certain degree because, on the one hand, I really enjoy technological innovations and all the benefits brought along them, but on the other hand, I do see how regular end-users are misled by large companies trying to hide the true extent of data collection and data sharing taking place. That is why I consider it to be so important that data sharing takes place, but it is done with the informed consent of the end-user and in a protected manner.

Worth to note is that all data transfers take place using a public or a private network. Public network is "a type of network wherein anyone, namely the general public, has access and through it can connect to other networks"[58]. Public network is more commonly known as the Internet. Let us explore data movements. Data can be found in one of three different stages; "in use", "in transit" and "at rest".[59] When we are talking about ensuring integrity of the data, we are referring to data when it is in transit or at rest. When data is "in transit", it simply means data is actively moving from one location to another such as across the internet or through a private network[60]. On the other side is data at rest which can be explained simply as to mean that data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way[61]. We will

[58] Jiri Kohout, 'Why Is Data Encryption Necessary Even In Private Networks?' <https://teskalabs.com/blog/seacat-encryption> accessed 12 April 2022.

[59] Ryan Yackel, 'What Is Homomorphic Encryption, And Why Isn't It Mainstream?' (Keyfactor, 2021) <https://www.keyfactor.com/blog/what-is-homomorphic-encryption/> accessed 28 January 2022.

[60] Nate Lord, 'Data Protection: Data In Transit Vs. Data At Rest' <https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest> accessed 18 March 2022.

[61] Nate Lord, 'Data Protection: Data In Transit Vs. Data At Rest' <https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest> accessed 18 March 2022.

focus on these two movement stages of data as they are the most important from the perspective of this thesis. In both of these stages, data is considered to be, theoretically, at a vulnerable state. Data faces different threats when it is in different movement stages. We can explore this by imagining a bank vault and armoured transport car. Should one decide to attack one of these, the means of achieving the objective are very different even though the objective is the same. Nevertheless, both the content of the armoured truck and the bank vault face risk and thus have to be prepared for different scenarios in case of an attack.

Evaluating vulnerabilities of data in transit and at rest, I would say that when data is in transit, it is at a more vulnerable state. This is because firstly, just because it is moving between one place and another so there is always a risk associated with the movement and secondly, data can be intercepted while it is in transit between places and thirdly, because data needs to be decrypted in order to be transferred. Data can be encrypted in both stages: in transit and at rest. These can be explained with a clarifying example: "Encryption at rest is like storing your data in a secure vault and encryption in transit is like putting the data in an armoured car for transport. It's harder to intercept, access, or transform. You have stronger guarantees that whatever you put into the armoured vehicle will arrive at its ultimate destination without any tampering along the way. And most potential threats will go after an easier mark"[62]. However, it should be kept in mind that not all data is encrypted. Few factors play a role here: firstly, not all data is considered to be worthy of encryption – the lack of resources and economic reason – and secondly, not everything can be decrypted – these can be network applications and configurations that need to be in a decrypted form in order to run.

How is encryption done? Cryptographic key, or encryption key, is a set of mathematical values – a string of bits – that is used to decrypt the data into the readable plaintext.[63] Afterwards, the data is secured by the encryption algorithm and theoretically it is considered to be safe. What I mean by theoretical safety is that generally the data is only accessible by using the cryptographic key to decrypt the data back into human-readable plaintext. It should be kept in mind that no encryption is impenetrable and thus can be accessed but requires a lot more effort than text in human-readable format. Encryption can be broken by deploying large amounts of computing power that keeps on inputting numbers until the correct mathematical combination

[62] Dale Walker, 'What Is End-To-End Encryption And Why Is Everyone Fighting Over It?' <https://www.itpro.co.uk/security/encryption/359943/what-is-end-to-end-encryption-and-why-is-everyone-fighting-over-it> accessed 8 April 2022.

[63] 'What Is Data Encryption?' (www.kaspersky.com) <https://www.kaspersky.com/resource-center/definitions/encryption> accessed 18 February 2022.

is guessed and thus encryption is penetrated. Logically, we can understand that the more complex the cryptographic key is the more secure the encryption is.

We do understand the importance of encryption but what does it do? Well it transforms human-readable plaintext into unreadable ciphertext. Therefore, it is important to encrypt data at rest and also while in transit. However, there remains a problem with the encryption in transit which can be explained by the following simple data flow example: where messages are encrypted on the sender's end, delivered to the server, decrypted there, re-encrypted, and then delivered to the recipient and decrypted on their end.[64] This places awfully lot trust into the actor in the middle. This is seen as a potential threat to the integrity of the data because there are no guarantees the party in the middle will respect the data. Systems should be built in a way that makes possible for end-to-end encryption to be in place or consider fully homomorphic encryption.

[64] Hugh Aver, 'What End-To-End Encryption Is, And Why You Need It' <https://www.kaspersky.com/blog/what-is-end-to-end-encryption/37011/> accessed 11 January 2022.

4 Future

When I started writing this thesis over a year ago, I had witnessed the complex state of data protection as it was after the Schrems II ruling. The ruling had invalidated the Privacy Shield framework which was by far the most popular transfer mechanism used by different sized organisations for the personal data transfers between the EU and the US. Furthermore, it had confirmed standard contractual clauses as an applicable transfer mechanism if accompanied by these elusive "further guarantees". What was meant by these "further guarantees" organisations had to be patient and wait for the EDPB to clarify the matter. First came the draft which was followed by the revised SCCs and the final version of the EDPB guidelines - a total of one year after the CJEU laid down the Schrems II ruling. During this period many organisations had to continue operations but there was never certainty whether it was done in a compliant manner. Most of this had to do with the fact that the assessment of whether an organisations was transferring personal data between the US in compliance with the GDPR was handed to respective national supervisory authorities to assess on a case-by-case basis.

After realising this all well-in detail, I knew this was so important as I should write about it as my master's thesis. I wanted to record thoroughly all the complexity building around the international data transfers. My initial thought was that this has to be too complex for many organisations to navigate and asked myself a question whether this was the intention behind data protection? I would have to assume the answer to the question is no. Data protection should not be this complex because the initial idea behind data protection, at least in my opinion, is to ensure security of the data from unauthorised access. This is the reason why I set out to write a comprehensive thesis detailing events that have occurred which have influenced data protection measures in order for the reader to fully grasp the complexity which organisations, small and big, have been trying to navigate.

Ever since the Schrems II ruling came out, I have been considering the possible options for what comes next. I decided to look back in order to understand the past decisions and their patterns. So, after the DPD came into force it prohibited the personal data transfers outside the EU unless there is adequate level of protection for the personal data in the receiving country. Adequacy, or inadequacy, is to be assessed by the European Commission on the basis of the receiving country's international commitments or the national data protection laws. Therefore, by default, personal data transfers to the US are not permitted due to reasons that the US national law does not ensure adequate level of protection for personal data by the EU standards. In 2000, a political agreement was found between the officials of the EU and the US which intended to ensure adequate level of protection for the personal data. Safe Harbour was invalidated 6th of October 2015, and the new politically agreed framework "Privacy Shield" was announced less than four months later on the 2nd of February 2016[65]. It should be noted that Safe Harbour principles were used as a transfer mechanism for over 15 years. Reaching a political agreement to ensure the continuation of transatlantic data flows did not take that long. As a result, when Privacy Shield was invalidated by the CJEU on 16th of July 2020, I thought another political agreement was probably going to be reached in order to clarify the complex situation that organisations were left to operate in.

Year 2021 was an exceptional year by all measures. However, as time passed, I started to consider other possible ways to resolve the prevailing situation without having to realise the certainty of political agreement. I asked myself: what if there were no need to rely on political decisions but it could be solved by using technology as to our advance? Concerns around data protection are mainly issues related to trust and unauthorised use of. I realised these are such issues that they can be solved either by means of political agreement, as has been done so far, or by means of technology. This is when I stumbled on the Fully Homomorphic Encryption. I did extensive research on the topic and realised the potential it could have if commercial use was made possible. FHE will be discussed in more detail in the next section.

4.1 Fully Homomorphic Encryption (FHE)

In the end of the previous section I mentioned stumbling on fully homomorphic encryption and realising the potential that it could have in the field of data protection – especially to the EU and US relations. Now what is fully homomorphic encryption? It is defined as "an encryption scheme that enables analytical functions to be run directly on encrypted data while yielding the same encrypted results as if the functions were run on plaintext".[66] In essence, it makes possible to make use of data that is encrypted while preserving the security. When data is shared FHE has the ability to restrict access only to necessary data.

In the beginning I explained that we are living in a world that is more connected than ever before. Data and personal information about us are shared between parties in unimaginable

[65] Anne-Catherine Berg, 'New EU-US Privacy Shield To Replace Safe Harbour Agreement' The European Broadcasting Union (2016) <https://www.ebu.ch/news/2016/02/eu-us-privacy-shield> accessed 22 February 2022.

[66] 'What Is Fully Homomorphic Encryption?' (Inpher) <https://inpher.io/technology/what-is-fully-homomorphic-encryption/> accessed 5 April 2022.

large scale. Organisations need to share their data to their contractors and business partners in order for them to do their objective. Here the business partner needs data to be decrypted into plaintext. Ordinary people share information about more than they understand. Personal information is shared with companies and organisations for convenience and improved services. In some scenarios, data that is shared is not sensitive in everyone's opinion. People have varying opinions on what information they consider important to them. For example, sharing location information about your location information to Google Maps might not concern all users because the convenience outweighs the downside of sharing your up-to-date location information. Don't get me wrong here, I think Google Maps is an amazing tool and incredibly accurate, but all that is possible because billions of users are constantly sharing up-to-date location data via their devices. Have you ever stopped to wonder how Google Maps can tell you that there is a five-minute delay in the route you are driving? Well, because a person's phone is giving its exact location while navigating in the traffic. If a person's phone is not moving in a normal road at all and is accompanied by 30 others staying put at the same time, it knows there is something happening which causes a delay.

Location data might not be considered sensitive by all, but universally it can be accepted that health data and personal medical records are considered sensitive by all means. Most people would argue that the same applies to financial data. Here trust is placed on the other party as sensitive information is shared. Suddenly, there is a growing need to know your health or financial information is securely stored and not shared with third parties without your permission. What comes to data, security is one of the most important elements and most often a lot of weight is based on trusting others involved.

So far we have discussed different stages of data. These were "at rest", "in transit" and "in use". Encryption is applied for at rest and in transit cases. Quick recap on what is the purpose of encryption. While data is in plaintext, it is in a vulnerable state. Purpose of encryption is to remove the relationship between plaintext and corresponding ciphertext and lock it with a key. Afterwards, no correlation should remain between the plaintext and the ciphertext. Using the key to decrypt is the only way to figure out which plaintext corresponds to which ciphertext. By now we do understand why applying encryption to an "in use" scenario would be a difficult task. Why is that? Because data "in use" scenario is actively changing – most operations on ciphertext change the value of the corresponding plaintext.[67] This is where fully homomorphic

[67] Ryan Yackel, 'What Is Homomorphic Encryption, And Why Isn't It Mainstream?' (Keyfactor, 2021) <https://www.keyfactor.com/blog/what-is-homomorphic-encryption/> accessed 28 January 2022.

encryption comes into play. FHE algorithms have accomplished to solve the problem. Here is how it is done: 1) algorithm manages to create a relationship between plaintext and ciphertext, 2) it enables adding or multiplying two ciphertexts together and have these results be identical should they be performed on two plaintexts and then encrypting it, and 3) manages to hide this established relationship from the person running the operation.[68] Most important thing to know here is the encryption is broken if ciphertext does reveal information about the plaintext.

Understandably FHE might still be a bit unclear to every reader. I hope to provide a few examples to clarify the importance of FHE in detail. Mark Will and Ryan Ko provide a well-demonstrating example in their article The Cloud Security Ecosystem. This first example contains imaginatory person "Alice" who runs an accounting firm. [69]

"Alice runs an accounting firm, which stores all of her customers' balances on the cloud. By utilising the cloud, it means that she does not have to manage the underlying infrastructure of the cloud. Instead it is managed by a third-party cloud service provider. The problem Alice faces is that in order to keep her customers' accounts secure, she encrypts them when they are in the database/storage. This prevents a malicious outsider gaining direct access to the information, while also stopping the cloud service employees from being able to see the data. But when she needs to make a change to an account balance, she has to either transfer the encrypted account back to her trusted environment, or decrypt the account data in the cloud, update the account, then encrypt it again before storage. This creates a risk where the data has to be decrypted at a point before it can be used. Because homomorphic encryption can process data while encrypted, Alice can simply apply changes to the encrypted account balance by sending encrypted data to the cloud and have the account updated without it ever being in decrypted form (i.e., plaintext). This allows Alices' cloud accounting firm to keep its customers secure, while having the added benefits of using the cloud."

Second example is one that many can closely relate to and was already discussed briefly above. If a hypothetical case example of Alice the Accountant left some unclarities, this example shall do the trick as I consider this example being ever more relatable by any average person. Let's consider a person named Gordon. Gordon is going out of town, and he needs to use a navigation app to get through from place A to B. The whole-time navigation is active, the navigation app needs to know Gordon's exact location, what direction Gordon is heading and what places are

[68] Ryan Yackel, 'What Is Homomorphic Encryption, And Why Isn't It Mainstream?' (Keyfactor, 2021) <https://www.keyfactor.com/blog/what-is-homomorphic-encryption/> accessed 28 January 2022.
[69] Ryan Ko and Kim Choo, The Cloud Security Ecosystem (1st edn, Elsevier Inc 2015) p. 101-127.

close by whilst driving to provide Gordon a route towards his destination. If FHE would be applied to the same exact example, the scenario would be different. The navigation app could provide Gordon with the same route from place A to B, but in this scenario the app would not need to know and save every detail surrounding Gordon's trip. Here we can see FHE at use in scenarios that concern many of us on daily bases. Navigation app could provide a route while running on encrypted data.

Personally, I consider FHE to be well suited to industries which are highly regulated – such as the healthcare industry. FHE can help make use of private and confidential information, because the technology behind FHE can make it possible to strictly confidential information such as patient health records broadly while restricting access to all but the necessary data.[70] I can see how FHE has the potential to revolutionise computing while promoting end-to-end privacy. As persons involved in data protection understand, ensuring privacy is the key and end-to-end encryption serves as the best examples of complete trust between the sender and the receiving of information. This is exactly what, for example, IBM's fully homomorphic encryption is attempting to achieve.[71]

At this point one might wonder why FHE is not out there in every place if it is as revolutionising as it sounds. Well this has to do with FHE being rather slow performing and it is computationally heavy to apply. This means that algorithms are slow to run and require large amounts of storage in order to operate.[72] If we compare running operations on plaintext versus FHE, as it currently stands compared to operations run on plaintext. FHE is not considered a new innovation because it was first proposed in 1978 by Rivest, Adleman and Dertouzos.[73] They proposed "a scheme that enables secret evaluations of plaintexts by manipulating only the ciphertext without knowing the decryption key"[74]. For a long time the FHE project was forgotten until 2009 Craig Gentry, a cryptographer, demonstrated FHE's use capabilities in his

[70] Flavio Bergamaschi, 'IBM Releases Fully Homomorphic Encryption Toolkit For Macos And Ios; Linux And Android Coming Soon' <https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/> accessed 15 January 2022.

[71] 'Homomorphic Encryption Services' (Ibm.com, 2022) <https://www.ibm.com/security/services/homomorphic-encryption> accessed 19 March 2022.

[72] Ryan Yackel, 'What Is Homomorphic Encryption, And Why Isn't It Mainstream?' (Keyfactor, 2021) <https://www.keyfactor.com/blog/what-is-homomorphic-encryption/> accessed 28 January 2022.

[73] Steven Yue, 'Fully Homomorphic Encryption Part One: A Gentle Intro' (Medium, 2020) <https://stevenyue.medium.com/fully-homomorphic-encryption-part-one-a-gentle-intro-94c3c3850568> accessed 1 February 2022.

[74] Steven Yue, 'Fully Homomorphic Encryption Part One: A Gentle Intro' (Medium, 2020) <https://stevenyue.medium.com/fully-homomorphic-encryption-part-one-a-gentle-intro-94c3c3850568> accessed 1 February 2022.

Ph.D. thesis.[75] Not that many had faith on the project but a team at IBM took the idea and thanks to them we have now functioning FHE, albeit FHE being still in training-wheels. If we consider the surprisingly short timespan it has been working on during the modern era of high-speed computers, the improvements are looking fantastic and there is a potential for FHE to become industry standard – at least in highly regulated industries - in the near future.

4.2 Privacy Shield 2.0 – Agreement in principle?

I had a gut feeling that told me whilst I was writing this thesis, there would be some progress made in the political front of data protection. I assumed this to be so because too long a time had passed since the Schrems II judgement and Facebook's saga with the Irish DPC was coming to an end. Consequently, on 25th of March 2022, European Commission and the US officials made the announcement that "agreement in principle" has been reached between the two that serves as a first step towards a new data sharing system between the EU and the US.[76] When I heard about this I was not even surprised. Well I have to admit that I was a little surprised in the beginning because it was released without any prior leaks of such. However, if we consider that this has probably been in the making ever since the Schrems II ruling, it does not surprise at all. Rather it was something that was expected but no one was sure when the announcement would come. Notwithstanding the fact that the announcement is only a political one and there is no text existing that could be analysed so far.

According to the European Commission's factsheet on Privacy Shield 2.0 free and secure flow of data between the EU and the US organisations is at the center of the agreement. It would also place limitations on the US intelligence authorities which would be subject to oversight to ensure necessity and proportionality. Furthermore, a whole "data protection review court" setup would be established to resolve complaints of the EU citizens in the US. One thing that has not changed from the Safe Harbour principles is the need to self-certify. Something that we have seen in the past that does not work as organisations do not adhere to it unless there is proper oversight on the matter. Interesting finding from the factsheet is that the data from EU citizens has received an estimated monetary value of 900 Billion per year. [77]

[75] Flavio Bergamaschi, 'IBM Releases Fully Homomorphic Encryption Toolkit For Macos And Ios; Linux And Android Coming Soon' <https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/> accessed 15 January 2022.

[76] 'Press Corner' (*European Commission - European Commission*, 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 12 April 2022.

[77] European Commission, 'Trans-Atlantic Data Privacy Framework' (2022) <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 9 April 2022.

We can draw an obvious conclusion from the announcement that there is willingness to have such a data sharing agreement in place from both parties, but solution to all issues raised in the Schrems II decision has not yet been finalised. Main issues the CJEU found in the Schrems II ruling related to the court identified Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, which allow U.S. intelligence agencies to collect data on foreign nationals, as inconsistent with rights guaranteed in the EU Charter.[78] It is going to be fascinating to examine how are the problems tackled by political means. Will there be an executive order from the President that grants EU citizens certain rights that they would not otherwise have. If this is the case, how can it be ensured that the next president of the US will not repeal the executive order just as easily as it was ordered. It remains to see what the Privacy Shield 2.0 will bring along with it and how long does it take to reach a state of implementation. Something that can be said is it appears as though we still are staying in the realm of political agreements and not trying to advance innovations that could solve the underlying problem of data protection.

[78] Ellysse Dick Nigel Cory, ''Schrems II': What Invalidating The EU-U.S. Privacy Shield Means For Transatlantic Trade And Innovation' (*Itif.org*, 2020) <https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic> accessed 10 March 2022.

5 Conclusion

Here I will do my best to wrap up my entire thesis by choosing the most relevant sections and points that have come up in the course of the thesis. Looking back at the goal of the thesis which was to provide in-depth overview to the data protection regulation, both past and the present. This we started by first examining the current world we are living in – meaning that the world is more connected than before and data about us shared it in more ways than ever before. We discussed concepts such as free trade versus protectionism because they were important to understand for the thesis. As a believer in the free flow of data, I see excessive data protection legislation posing troubles in the field.

Also, it was my goal to analyse the current data protection status and whether it is working properly or not, and if not what is wrong? We went through the major steps that have occurred during the time period beginning from the 1995 Data Protection Directive which was, during the time, a ground-breaking legislation that set the tone for all future developments in the EU's data protection sphere. It prohibited personal data transfers outside the EU by default. In addition, it provided a mechanism for the European Commission to evaluate third-countries state of data protection whether it did or did not conform with the EU's level and thus gave the power to allow personal data transfers to countries where it was otherwise prohibited. Of course, there were additional measures in place to ensure the security of the transferrable personal data. One case example was provided in the thesis as the Safe Harbour principles which intended to make personal data transfers safe, but after the objection by Max Schrems. The CJEU invalidated the politically agreed mechanism for personal data transfers between the EU and the US.

Following to the next major events that took place, the GDPR, Privacy Shield and the Schrems II. As we saw in the thesis, Safe Harbour principles were followed by yet another politically agreed framework for the data transfers which bears the name Privacy Shield. Privacy Shield was just announced shortly after the GDPR was adopted. Privacy Shield was similar to Safe Harbour as it consisted of Seven Key Principles which were at the core of the framework. We did a comparison on the similarities between the seven key principles of Safe Harbour and the Privacy Shield and made the conclusion that these have oddly unfortunate similarities, but this was expected because of the political nature of the frameworks. Here I raised the issue of political nature of the data protection as it currently stands. My view is that this is not efficient way to ensure sufficient data protection level, however I do recognize that it is more simple way forward than digging into the technical measures that could be deployed if they were adopted in a large scale that would enhance their development.

Eventually, we found out that the Privacy Shield did not either held in court as the CJEU decided to invalidate the Privacy Shield in a case that came to be known as Schrems II case. After the Schrems II case, the data protection field has been lost because it was difficult to continue personal data transfers and remain compliant if you did not possess team of experts. Only exception here was those organisations that were using Binding Corporate Rules as their transfer mechanism. These could be viewed as the golden standard of transfer mechanism because they are subject to regulatory review from the makings. With a statistic, I provided fascinating information on the popularity of Privacy Shield, thousands of organisations used them, but only little over 100 used the Binding Corporate Rules as their personal data transfer mechanism.

I managed to explain well in detail the deeper level of data itself and why it is a concern of data protection legislation. The thesis explored the grassroots level of the data itself. Where does data come from and why it is important to protect it. Methods for protecting data were explained well-in detail as well as use cases for different scenarios. Encryption was explained and also data movements. These were clarified with a hypothetical examples of armoured truck and the bank vault. It was explained how the data comes into vulnerable state and what would be the best possible option to secure data in an almost fault-proof method.

As highly important part of the thesis, fully homomorphic encryption was introduced as an idea for the betterment of data protection as a whole. It was in my opinion the best solution to offer the answers to the grassroots level problems industry is facing. These related to the trust and uncertainty around transfers. If fully homomorphic encryption would be widely adopted, it would have the potential to change the whole industry because it would enable limiting access to other than required data and this way it would solve many problems. There would be no more excessive data gathering because it could be limited. There would be no need to decrypt data while changing something in a file that is located in the Cloud. There were two hypothetical cases that explained what fully homomorphic encryption and what possibilities it is could have.

Lastly, the thesis discussed the possibility of resolving current data protection emptiness, caused by the Schrems II case, by means of political decision once again. This would be probably fix issues for the short time-period, but I honestly do not think that is the right way forward if we are considering the long-run. Furthermore, if the intention is to continue using political decision-making as the resolve, we should consider increasing EDPB's role as an independent body that would ensure the data protection aspect is covered in depth.

In summary, first research question "in what ways the current data protection regulation does not work and why is that" was answered by explaining the political nature of the decision-making and the problems that causes. It was also explained that political decisions do not stand the time as well as technical developments could do. It was also explained that there is too much importance put on resolving the underlying matters of trust and security. The ways these could be truly achieved are not utilised currently.

Second research question is "how technology could assist in resolving the current problems the data protection industry is facing" was explained by introducing the problems faced by the industry. Explained well in detail on how these could be targeted from the technical side of problem-solving. Importance of encryption and limiting access were provided as methods to ensure security. Ultimately, fully homomorphic encryption could answer all the questions and problems presented in the thesis up to this point. There were problems with it but those related to the slow speed which it currently stands, but it was also mentioned that this could be expedited if enough applications and use cases would be for the fully homomorphic encryption. Some party has to be on the edge of the technological development, and I am going to assume it will be one of the companies operating in highly regulated industry such as healthcare and finance. With the help of such companies the full potential of fully homomorphic encryption could be realized and provided to masses.