Vilnius University, Faculty of Law

Department of Public Law

Raminta Matulytė

5th-year student of

International and European Union Law

Master Thesis

Comparing Data Protection Regulation Models of the EU and the US: Which One Is More Preferred by the Society?

Promoter: assist. dr. D. Murauskas

Reviewer: assist. dr. D. Prapiestytė

Vilnius

2022

ANNOTATION AND KEYWORDS

This work analyses the data protection regulation models in the European Union and the United States. The models are compared by indicating the main features of these models and assessing their social costs and efficiency through the lens of economic analysis of law. The economic approach to the evaluation of the European Union and United States data protection regulation models attempts to define a social preference for each model in terms of *ex-ante* regulation and *ex-post* liability.

Keywords: data protection regulation, EU model, US model, economic analysis of law, social preference, *ex-ante* regulation, *ex-post* liability

CONTENTS

LIST OF TABLES

LIST OF IMAGES

LIST OF TERMS

Compliance	the fact of obeying a particular law or rule (Cambridge Dictionary, 2019); in this thesis – obeying particular data protection law or rule
Data (personal data)	any information relating to the data subject (Article 4(1) of the EU General Data Protection Regulation)
Data breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 4(12) of the EU General Data Protection Regulation)
Data controller	an organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4(7) of the EU General Data Protection Regulation)
Data subject (individual)	an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly (Article 4(1) of the EU General Data Protection Regulation)
Data processing	any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) of the EU General Data Protection Regulation)
Data processor	an organisation that processes personal data on behalf of the data controller (Article 4(8) of the EU General Data Protection Regulation)
Data protection (privacy)	a set of strategies and processes used to secure the privacy, availability, and integrity of the data; the term “privacy”, “data privacy” is more common in the US, while in the European context, it is usually understood as concerning more areas than data protection; however, in this thesis, these terms are used as synonyms

Efficiency	effective operation as measured by a comparison of production with cost (as in energy, time, and money) (Merriam-Webster, 2019); in this thesis, efficiency concerns the balance between the aim of protecting individuals and social costs for achieving this aim
Social costs	costs estimated from the viewpoint of society, rather than individual stakeholders, representing the total burden imposed on the economy; in this thesis, social costs are evaluated in relation to data protection regulation
Supervisory Authority	an independent public authority that is established by an EU Member State under the GDPR (Article 4(21) of the EU General Data Protection Regulation); in this thesis, this term is also used for the US jurisdiction and refers to public authorities in general that supervises the enforcement of data protection legislation
Preference	the act of giving priority (Merriam-Webster, 2019); in this thesis, this term is used to describe societal priority for the evaluated data protection regulation models

INTRODUCTION

Relevance of the topic. How should we cope with the increased use of data by tech companies? Over the last few decades, rapid technological development resulted in the need to search for data protection regulation opportunities. However, with the introduction of different data protection standards, discussions on which standard to follow or how to improve existing ones are as relevant as ever.

It is widely accepted that at the moment, the most advanced data protection standard setting numerous obligations to companies and a list of rights of individuals is adopted at the European Union (**EU**) level – the General Data Protection Regulation (**GDPR**) (Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data…, 2016). The opposite to such comprehensive and strict regulation enshrined in one legal act is the United States (**US**) data protection framework, which is fragmentary and does not foresee obligations for organisations or rights to individuals in every case concerning data processing. In recent years, issues related to these different legislative approaches came to the forefront of the Court of Justice of the European Union (**CJEU**) cases. They undermined prior attempts to harmonise the different data protection approaches and forced the EU and US to search for a new coordinated framework.

Such developments gather discussions in academia on the essence of data protection regulation. Does digital freedom have to stop where that of the user begins? Will the value of data ever stop increasing? Is the end of privacy closer than we think, as privacy is becoming less and less an option for most citizens? Which way is more preferred and efficient – putting strict requirements on organisations to comply or leaving any data-related issues for market participants to self-regulate? Is data protection the necessary mechanism to guarantee individual rights, or is it an artificial construct robustly used to prevent businesses from using data? Privacy has become something that is not just for lawyers anymore; therefore, the author considers that in order to have a comprehensive approach to enacting and enforcing data protection regulation, including national jurisdiction in Lithuania, it is crucial to understand compliance and enforcement costs.

Objective of the research. The main objective of this thesis is to compare the EU and US data protection models by indicating their main features and assessing their social costs and efficiency through the lens of economic analysis of law.

Tasks of the research. To achieve the set objective, the author distinguished the following tasks for the research:

1) to identify the main features and challenges of the EU data protection regulation,
2) to identify the main features and challenges of the US data protection framework,
3) to compare these two models by way of identifying which is more economically preferred and efficient in terms of social costs.

Structure of the research. To better understand each of the models' social preference and their costs of compliance and enforcement, the author first describes the fundamental aspects of each data protection regulation model. The first part of this thesis concerns the EU data protection regulation model – mainly the GDPR, its fundamental rules, compliance, and enforcement issues. The second part follows the same structure for analysing the US data protection regulation model. The third part then describes the economic approach to privacy costs and the applicability of this approach to EU and US data protection regulation models.

Object of the research. The author analyses the EU and US data regulation models – their development, primary statutory laws and their features, and practical impacts for data economy participants. In addition, this thesis aims to evaluate the social costs caused by each of these models.

The author considers that legal acts establishing data protection regulation models shall be regarded as an object of the research, not key sources. At the EU level, it is mainly the GDPR. At the US level, the author examines selected US sectoral data protection laws (e.g., Health Insurance Portability and Accountability Act, 1996; Gramm-Leach-Bliley Act, 1999 and others).

In works concerning a comparative analysis of EU and US data protection regulation models, it is typical to comprehensively analyse data transfer requirements in both jurisdictions and compare certain provisions of legal acts. The author does not analyse these topics in detail, only provides a contextual description to the extent necessary to apply the models of economic analysis of law. In addition, the author does not extensively analyse data protection rules at EU Members States' and separate US States' levels. This research mainly concerns the data protection in the relationship between private parties and individuals rather than government performed data processing.

Methodology of the research. The fundamental methodology of this research is the ***comparative analysis*** of the EU and US data protection regulation models. The author

systemically analysed the statutory data protection legislation in the EU and the US, mainly focusing on the changes in the global privacy arena after the adoption of the GDPR. The author also introduces a ***historical analysis*** of the mentioned regulations' development and distinguishes their main features. The main issues of both models were identified by analysing their impact on businesses and individuals in terms of required resources and gained benefits. The author, where relevant, provides an analysis of privacy case law and decisions of data protection Supervisory Authorities. By way of ***economic analysis of law***, the author applied developed theoretical economic concepts to the US and EU established data protection regulation models to determine their efficiency and social preference. ***The teleological method*** in this research was used to assess the objectives of selected data protection legislation.

Originality of the research. Currently, available research focuses on identifying issues related to separate requirements of the established data protection regulation frameworks or a straightforward comparison of EU and US data protection regulation models regarding conflicts in their harmonisation. However, available research is not comprehensive when it comes to comparing which model is more efficient. Even research describing such issues is either rather outdated (e.g., Romanosky & Acquisti, 2009), meaning published before major changes in the data protection regulation arena, or related more to an economic or political angle rather than analysing possibilities to improve legal regulation and its enforcement (e.g., Chander et al., 2021). Master theses defended in Lithuania in the past five years concern issues of extraterritorial applicability of the GDPR, analysis of separate rules of the GDPR and their applicability or data transfer mechanisms outside the EU and their harmonisation with the US framework. However, none of the defended works provides a comprehensive approach to comparing the EU and US data protection regulation models.

The author believes that this thesis is original concerning recent developments in the EU and US data protection regulation systems, measuring their social costs and attempting to define the most efficient combination of the data protection regulation standard. In the author's opinion, it is innovative to raise the question of whether the "golden" data protection regulation model is aimed to find an optimal balance between the costs and benefits of data protection and commercial flows of information, or the legislator is trying to achieve a given standard of data protection independently of its economic value. The findings of this research are relevant for enforcement strategies and future law-making on the union level of the EU and federal level of the US, as well as the national and state level, including Lithuanian authorities. The

author considers that analysing data protection regulation models through the lens of social costs may provide a new point for finding solutions for harmonising EU-US data protection regulation models and help to rethink the direction of the data protection law development in both jurisdictions.

Key sources of the research. Interpretation and the impact of the statutory laws establishing data protection regulation models are described by analysing the judgments of courts and decisions of data protection authorities. This thesis comprehensively analyses articles and other doctrine research to describe the EU and US data protection regulation models. The various scholar's articles (e.g., Romanosky & Acquisti, 2009; Shavell, 1984) and soft law sources are used to evaluate social costs imposed by the described data protection regulation models and assess social preference for each of them.

1. EU'S APPROACH TO DATA PROTECTION REGULATION: GOLDEN STANDARD OR UNDERESTIMATED BURDEN?

With the introduction of the GDPR, the EU's standard of data protection is often referred to as the most far-reaching globally. However, the EU's comprehensive approach to data protection originates from the ambitious European approach to human rights protection and had been developing for decades before the adoption of the GDPR. Despite the broad EU's data protection regulation, GDPR does not escape criticism regarding its efficiency and balance between business and individuals' interests.

1.1. The Chicken or the Egg: European Data Protection Standard Before the GDPR

While the GDPR brought the EU fully into the digital era, privacy rights have long been a part of the EU's history in response to the atrocities endured by millions of people during World War II (Newman et al., 2020, p. 273). Italy's (1947) and Germany's (1949) postwar constitutions were at the forefront of this evolution as these countries learned the importance of protecting human dignity through their catastrophic experiences with fascism and nazism (Schwartz & Peifer, p. 2017, p. 121). Following these examples, in 1950, the right to privacy was enshrined on an international level – in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (**ECHR**) (Convention for the Protection of Human Rights and Fundamental Freedoms, 1950).

Consequently, following the human rights field developments, the most technologically advanced Western Europe countries began to adopt national legislation specifically for data protection. Sweden's Data Act of 1973 was the first comprehensive national data privacy law and the first to establish what we now consider to be a fundamental set of data protection principles (Greenleaf, 2013, p. 5); Germany followed this example in 1977, France in 1978 and other countries subsequently. The adoption of different national legislation revealed that differences in these laws might obstruct the unrestricted flow of information and data across countries. Data protection legislation has become a concern of the international community and European countries in the first place.

Countries of the Council of Europe realised that the growing use of computers and the automatic processing of personal data necessitated new data protection legislation. As a result, a new instrument, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (**Convention 108**) (Convention for the Protection of Individuals

…, 1981), was adopted and opened for signing in 1981. While Convention 108 functioned as a model for national data protection laws, it did not harmonise such laws across Europe (Newman et al., 2020, p. 274). However, together with the Organisation for Economic Co-operation and Development Recommendations Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data (Recommendations Concerning Guidelines Governing the Protection of Privacy…, 1980), these legal acts contributed to shaping the EU data protection framework.

Understanding the rising importance of data protection legislation, the EU also included this topic in its agenda. With the adoption of the Single European Act (Single European Act, 1986), which set a deadline for creating a single market in goods by 1992, the movement for a European-wide data privacy regulation gained attention. The European Commission acknowledged that foreign data flows were crucial to the single market's progress, and in 1992 they released a draft directive (Newman et al., 2020, p. 274). The Data Protection Directive (Directive 95/46/EC on the protection of individuals…, 1995) (**Data Protection Directive**) was adopted in 1995. It established general rules on the lawfulness of personal data processing (including data protection principles and a list of legal bases for data processing), the rights of data subjects, the establishment of independent supervisory authorities (**Supervisory Authority**(**-ies**)) in the EU Member States and other fundamental elements of data protection (Protection of Personal Data, Fact Sheet, 2020, p. 2).

As the Data Protection Directive was not directly applicable in the EU Member States, interpretation of its rules differed across the EU. Therefore, CJEU's case law development in interpreting the Data Protection Directive's provisions was significant. CJEU, for example, developed the concept of personal data by ruling that IP addresses (Breyer case, 2016) or data related to the professional activity (Manni case, 2017) shall be considered personal data under the Data Protection Directive. CJEU also defined what type of data processing is performed only for personal use and cannot fall within the scope of the Data Protection Directive (Lindqvist case, 2003) and how to determine data processing in search engines (Google Spain and Google case, 2014). Under the Data Protection Directive, CJEU also developed rules on other matters such as the legal basis for lawful data processing (Rīgas satiksme case, 2017), data subjects' rights (Google Spain and Google case, 2014), the status of Supervisory Authorities (Commission v. Hungary case, 2014) and others. As many rules and basic

principles of the Data Protection Directive were transferred to the GDPR, these CJEU's judgments are still relevant for the interpretation of the GDPR.

To prove the importance of the fundamental principle of data protection, in the adopted Charter of Fundamental Rights in 2000 (**Charter**) (Charter of Fundamental Rights of the European Union, 2000), the EU included an explicit right to personal data protection (Article 8 of the Charter). In 2009, the Lisbon Treaty granted the Charter the same legal status as the EU's constitutional treaties, making it legally binding. Furthermore, the EU is required by Article 16 of the Treaty on the Functioning of the EU to establish data protection rules for the processing of personal data (Newman et al., 2020, p. 274). Such recognition of the right to data protection distinguishes the EU's approach from the approach chosen by the Council of Europe. The right to data protection is not explicitly enshrined in the ECHR; it is covered by Article 8 (right to privacy). Only years after the adoption of the ECHR European Court of Human Rights (**ECtHR**) expanded the scope of the mentioned article in its case law. In *Leander v. Sweden*, ECtHR confirmed that the right to privacy also includes the right to data protection (Leander v. Sweden case, 1987). Later on, ECtHR ruled that data collected at the workplace is also protected under the right to privacy (Niemietz v. Germany case, 1992). ECtHR also adopted judgments on matters such as processing geolocation (Uzun v. Germany case, 2010) or biometric (S. and Marper v. the United Kingdom case, 2008) data, video surveillance (Antović and Mirković v. Montenegro case, 2017) and others. Despite the lack of explicit mention of the right to data protection in the ECHR, it is evident that European organisations have a uniform approach toward protecting personal data as part of the human rights protection framework.

With the skyrocketing technological development in the 21st century, the EU understood that the Data Protection Directive rules adopted twenty years ago could no longer be applied without changes. In 2016, the EU reformed the overall legal framework in the data protection area. To raise an approach to data protection with human rights at its centre to a higher level, in 2012, the European Commission proposed an extensive revision of the Data Protection Directive. This proposal aimed to enhance online privacy rights and boost Europe's digital economy. As a result of extensive debate and negotiations, the European Parliament (**EP**) adopted GDPR in 2014, while the agreement between the EP, European Council and European Commission was reached in 2015. GDPR was adopted in 2016 and came into effect on May 25, 2018. Further analysis of the GDPR requirements is provided in section 1.2 below.

In addition to the GDPR, the EU has adopted other legal acts related to specific data processing activities. Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (**E-privacy Directive**) includes important rules for the use of cookies and processing data for direct marketing purposes. EU is aiming to transfer these rules to E-privacy regulation, which will be directly applicable and impose similar fines to the GDPR. In addition, together with the GDPR, the EU adopted Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (**Law Enforcement Directive**). The Law Enforcement Directive, in many ways, reflects the rules of the GDPR; however, it applies to the data processing performed by law enforcement actors. As these legal acts are not comprehensive data protection legislation and are not directly applicable, for the scope of this thesis, further analysis concerns only the GDPR as the cornerstone of the EU data protection regulation model.

1.2. Key Requirements that Make the GDPR the "Golden" Standard

Despite its building blocks having been established in the European law framework for decades, the GDPR is regarded as the most controversial regulation in EU history (Powles from Kessler 2019, p. 101). The unified data protection paradigms are usually built around two features: (1) a list of statutory rights granted to individuals in relation to their personal data and (2) the imposition of legal obligations on organisations that process personal data. Since the beginning of the data protection law, the established European data protection framework emphasised the data subject as a right holder. Over the years, the EU came to the point where it considers data privacy a component of its fundamental rights legal culture (Schwartz & Peifer, p. 2017, p. 126).

Unlike its predecessor Data Protection Directive, GDPR is directly applicable, meaning that without any domestic implementation, it became part of each EU Member State's national law. GDPR sets numerous standards that entities processing personal data are obliged to implement. Even though many rules and principles were transferred or elaborated from the Data Protection Directive, GDPR introduced a number of significant changes. The author further summarises selected requirements relevant to the objective of this research.

Compared to the Data Protection Directive, GDPR now imposes a much broader definition of protected personal data; under the GDPR, IP addresses, mobile device identifiers, geolocation, biometric information also constitute personal data (Article 4(1) of the GDPR). It is widely acknowledged that such development reflects advancements in technology and how corporations collect data on individuals. Supervisory Authorities have already imposed fines regarding misuse of these expanded categories of personal data. For example, the Lithuanian State Data Protection Inspectorate imposed a fine on a sports club for infringements of fingerprint data processing under the GDPR (EDPB, 2022). In Italy, a food delivery company was fined for misusing a geolocation data algorithm used to manage riders' work shifts (Data Guidance, 2022). These expanded categories result in mandatory compliance for organisations that, before the GDPR, potentially never considered themselves as actors processing personal data.

It could be considered that the GDPR's international influence is the regulation's most significant victory. Article 3 of the GDPR foresees that the GDPR applies to organisations in the EU and organisations outside the EU if they offer goods and services to data subjects in the EU or monitor their behaviour. In practice, this means that the EU *de facto* forces non-EU companies to follow the GDPR rules if they intend to maintain or establish their businesses in the EU and seek to avoid being fined. This GDPR approach is far from being a dead letter and has already been enforced several times on American tech giants through their establishments in the EU – *Amazon* was fined in Luxembourg for various GDPR infringements, *WhatsApp* was fined in Ireland, French Supervisory Authority fined *Facebook* and twice *Google* (GDPR Enforcement Tracker, 2022). The extraterritoriality of the GDPR is also one of the key points in the discussions on data transfer regimes in the EU and US and the harmonisation of the data protection regulation models.

The Data Protection Directive also established certain data subject rights; however, GDPR imposes an expanded and comprehensive list of these rights (Articles 13 – 22 of the GDPR). For example, these, among others, include the right to be forgotten (Article 17 of the GDPR), which means that any individual, if there are no exemptions under this article, may ask the data controller to erase all their personal data, cease further use of such data, and, if applicable, halt any third-party use of that data. This data subject right, until now, is an object of numerous discussions as businesses argue that such restrictions prevent them from developing technologically advanced products because individuals at any time may limit the

use of their data. With an extensive GDPR list of data subject rights comes additional requirements for organisations in their fulfilment. The GDPR sets time frames for responding to data subjects' inquiries, exemptions for not responding to these requirements and others (Article 12 of the GDPR). Mere insufficient fulfilment of data subjects' rights has already brought fines to numerous companies across Europe, with the total sum reaching almost 18 million euros at 99 fines (GDPR Enforcement Tracker, 2022).

The GDPR introduces additional rules for data processors, which is a significant update from the Data Protection Directive. One of the requirements under the GDPR is that a data processor can process personal data only by following the instructions set in the agreement with a data controller. The contents of this agreement are listed in Article 28 of the GDPR and include obligations such as allowing to perform audits, ensuring personnel confidentiality and others (Article 28 of the GDPR). For example, French Supervisory Authority fined a biotechnology corporation for failing to determine data processing status with data processors and the absence of an agreement under Article 28 (CNIL, 2022). The practical implication of the concept of a data processor is that there are almost no organisations that access data and would not have to comply with at least some of the GDPR requirements.

There is a single standard of data breach notification procedure to follow once the GDPR was adopted. Under the Data Protection Directive, EU Member States were allowed to enact their own laws regarding data breach notification procedures. This meant that when businesses in the EU experienced data breaches, they had to investigate and assure compliance with the national laws of each EU Member State. Under the GDPR, data controllers must notify the Supervisory Authority within 72 hours of discovering a personal data breach. In addition, the GDPR specifies what information must be included in the notice (Article 33 of the GDPR). Furthermore, GDPR requires to notify affected data subjects when the data breach is likely to result in a high risk to those individuals (Article 34 of the GDPR). Supervisory Authorities have already fined companies for failing to comply with the GDPR data breach notification requirements. For example, the Dutch Supervisory Authority fined the online travel agency *Booking.com* for notifying it of the data breach 22 days later instead of the required 72 hours (Forbes, 2021).

Compared to the Data Protection Directive, the GDPR also expanded rules related to data transfers to third countries. Under Chapter V of the GDPR, an organisation is allowed to transfer data to third countries only where 1) the European Commission has adopted an

adequacy decision that third countries provide an adequate level of data protection (Article 45 of the GDPR) or in cases where there is no adequacy decision, 2) the organisation has provided one of the appropriate safeguards listed in Article 46 of the GDPR. These conditions may not be followed in specific situations that provide derogations in Article 49 of the GDPR (e.g., the transfer is necessary for important public interests and others). This chosen EU mechanism causes headaches for many organisations that operate internationally, and data transfers are an essential part of their day-to-day business activities. With the *Shrems II* judgment (Shrems II, 2020), CJEU expanded Article 46 of the GDPR, concluding that if a third country's laws allow national intelligence institutions to access Europeans' data, mere appropriate measure is not sufficient; organisations are obliged to perform additional assessment of such transfer and adopt additional data protection measures, if necessary. This judgment confirms that the EU's chosen approach to data protection remains strict regardless of the excessive regulatory burden on organisations that is not even explicitly included in the GDPR.

Compared to the Data Protection Directive, GDPR imposes comprehensive enforcement mechanisms. First, organisations are obliged to designate a data protection officer (**DPO**) if 1) the processing is carried out by a public authority or body, 2) the core activities of an organisation consist of processing operations that require regular and systematic monitoring of data subjects on a large scale, or 3) the core activities of an organisation consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences as understood under the GDPR (Article 37(1) of the GDPR). The primary function of the DPO is to supervise how an organisation complies with the GDPR requirements. GDPR grants DPO status that prevents an organisation from any punishment for performing listed DPO's tasks (Article 38 of the GDPR). Such an independent position in an organisation results in the internal enforcement of the GDPR requirements. Recently Supervisory Authorities took a closer look at how organisations protect DPO status under the GDPR. For example, Luxembourg Supervisory Authority fined three companies for insufficient involvement of data protection officers in companies' matters (GDPR Enforcement Tracker, 2022).

Second, external enforcement of the GDPR is established via the requirement to appoint an independent public authority and unification of mechanisms for imposing fines. Even before the adoption of the GDPR, EU Member States were required to appoint a Supervisory Authority monitoring the application of the national provisions adopted by the EU Member

States under the Data Protection Directive. With the introduction of the GDPR, Supervisory Authorities now are the watchdogs of the GDPR application. A Supervisory Authority should be given the financial and personnel resources, facilities and infrastructure required to carry out its duties effectively (Preamble 120 of the GDPR). Under the Data Protection Directive, CJEU had already confirmed that Supervisory Authorities must be granted independence to ensure the effectiveness and reliability of the monitoring compliance with the provisions concerning data protection (Commission v. Germany case, 2010; Commission v. Austria case, 2012; Commission v. Hungary case, 2014).

GDPR lists violations that may result in a fine as well as the possible amount of a fine (up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher) (Article 83(3)-83(6) of the GDPR). In addition, the GDPR sets factors that affect the individualisation of imposing a fine (Article 83(2) of the GDPR). This is a result of the GPDR risk-based approach. This approach means that an organisation's compliance requirements and associated costs vary significantly depending on the risks created by its data processing operations (Chander et al., 2021, p. 4). By the day of submission of this thesis, the overall sum of the EU Supervisory Authorities' fines reaches more than 1.6 billion euros (GDPR Enforcement Tracker, 2022).

It must be acknowledged that Supervisory Authorities do not necessarily have to impose fines under the GDPR. They have the power to choose the most appropriate corrective measure in each case. Warnings, reprimands, data processing restrictions, and orders that data breach notifications be provided to data subjects are only some of the possible corrective measures (Hilliard, 2020, p. 1261). Based on their GDPR implementation strategy, EU Member States could choose how quickly and severely they fined GDPR violators. Some governments took their time issuing fines, preferring to focus on GDPR implementation education rather than imposing fines (Hilliard, 2020, p. 1264). However, following the tendency in multiple EU Member States' jurisdictions, it seems that the imposition of fines more and more often becomes the general harmonised European approach.

Compared to its predecessor, the Data Protection Directive, GDPR sets numerous strict requirements for data processing performed by organisations, many of which are already enforced by EU Member States' Supervisory Authorities. The central question is whether these GDPR requirements are the most efficient way to achieve the set data protection goals that the European community has been establishing for more than fifty years.

1.3. GDPR: Regulation with No Winners?

One point of view is to look at the GDPR from the human rights law perspective. With the GDPR, individuals are granted the possibility to gain more control over their data. In addition, unlike the Data Protection Directive, the GDPR unifies data protection standards across the EU, providing the same level of protection for Europeans. At the same time, companies that misuse and abuse data processing face more rigorous enforcement risks. It is also claimed that the GDPR's extraterritorial reach is increasing the bar of data protection for people outside the EU since businesses are adopting a uniform data management standard that complies with the GDPR, and third countries aim to receive an adequacy decision from the European Commission. Overall, looking at the GDPR strictly from the human rights perspective – it is undisputedly the global "golden" standard for data protection.

Proponents of the GDPR claim that this EU regulation benefits organisations as well. Firstly, organisations operating in more than one EU Member State now need to comply with one legal act instead of a variety of national laws. It is also argued that the GDPR increases companies' trust, credibility, and brand reputation as it requires transparency from companies regarding the processing of data. Furthermore, GDPR allows for improving companies' data management to ensure compliance. One positive outcome of data management is the possibility of reducing maintenance costs by encouraging the company to retire any data inventory software and legacy applications that are no longer relevant to the business.

On the other hand, there is a widely accepted opinion that GDPR has shown to be a costly and challenging burden on Europe's digital economy rather than functioning as a "golden" standard data regulation for the rest of the world to follow. Canadian Marketing Association (**CMA**) has recently published a report on the GDPR pitfalls (CMA, 2022). Even though it is agreed that the GDPR has drawn significant attention to privacy-related issues, CMA concludes that it has "proven to be costly, unmanageable, or prohibitively expensive without providing a commensurate privacy benefit" (CMA, 2022, p. 6).

First, many concerns are related to the extraterritorial applicability of the GDPR – what may look like a success from the EU's perspective is not seen the same in the international arena. While, for example, some US organisations see the regulation as a business opportunity that allows them to rethink their privacy policies and realise the actual value of data, others regard the GDPR as a significant burden that has pushed them to make an expensive change to their business while also causing compliance issues (Newman et al., 2020, p. 270). CMA

argues that the GDPR obstructs international data transfers, and the adequacy scheme enshrined in the GDPR has a chilling impact on cross-border businesses (CMA, 2022, p. 28).

According to Goldsmith and Wu, the EU has become an effective sovereign in the data protection field since it has passed a unilateral worldwide data protection legislation due to Europe's combination of great market power and unprecedented concern for its residents' privacy. Because the EU is such an important market for global corporations, many do not have the choice to pull out of the European market. Furthermore, foreign corporations are often unable to filter their EU consumers geographically and, even if they could, would not want to offer separate services for them. According to Goldsmith and Wu, as a result, many US companies have opted to surrender to the EU's market power and follow the established data protection regulation model (Goldsmith & Wu, 2006, p. 174-176).

The EU's unilateral exercise of authority in certain data protection situations has had consequences for global enterprises, governments, and Internet users, as an example of the "Brussels effect." Due to normative socialisation and EU bargaining power, EU data protection standards have moved outside, influencing and even forcing changes in foreign or non-EU companies' data protection procedures, third-country legislation and practices (Ryngaert & Taylor, 2020, p. 9). Some countries have even grabbed an opportunity to lessen the burden of the GDPR. For example, in the post-Brexit era, the United Kingdom's (**UK**) regulator is consulting the stakeholders on implementing a more pro-growth and pro-innovation data regulation framework instead of the adopted UK GDPR (CMA, 2022, p. 6).

Second, most rules in the GDPR are formed as abstract principles and contain vague terminology. In addition, such terminology is often found quite expansive (e.g., the concept of personal data). Heiman argues that such vagueness is the opposite of the well-drafted law, in his view – this major data privacy law lacks clarity surrounding its terms, therefore, has fallen short, especially when parallelly imposes a significant rise in the fine's regime (Heiman 2020, p. 950).

Third, the GDPR's complexities and responsibilities are carried most easily by the market's largest players. These businesses have the financial resources, legal teams and compliance professionals to assure compliance. Smaller businesses find it hard to comply with the GDPR's standards. Compliance expenses are insignificant for a major corporation, but they are a significant burden for small and medium enterprises in the EU. Those who cannot afford compliance face the danger of being exposed to fines or are forced to refuse to serve the EU

citizens (Heiman, 2020, p. 950). It is even argued that companies have ceased applying competing tracking systems, giving the established players, such as *Google* or *Facebook*, a more significant portion of the market. Finally, users are less willing to experiment with new platforms and tools, preferring to remain with the "devil they know" regarding privacy compliance (Layton, 2019, p. 3).

Fourth, it is suggested that the GDPR raises threats to the current Internet business model and that compliance costs are passed on to consumers through higher costs and diminished services (Heiman, 2020, p. 951). In addition, some global companies are adjusting their operations and refusing to serve EU citizens rather than making substantial compliance expenses; therefore, the availability of goods and services for EU customers has decreased. Furthermore, the GDPR creates complexity for consumers. The GDPR imposes requirements to provide data subjects with clear and understandable information regarding their data processing. However, it is argued that with the GDPR, consumer notices have become even more frequent and complicated, making it less possible for users to properly read the content and make informed decisions (CMA, 2022, p. 19).

The fifth identified threat is posed risks to critical emerging technologies – such as artificial intelligence or blockchain, that are based on massive datasets. However, the GDPR user's right to be forgotten or data minimisation and storage limitation requirements prevent companies from using non-anonymised data without significant restrictions (Heiman, 2020, p. 951-952). Kessler also proposes that while the GDPR was meant to safeguard consumers and improve EU citizens' fundamental right to privacy, several major technology businesses argue that it stifles innovation because of its rigorous compliance requirements (Kessler, 2019, p. 105). The GDPR generates uncertainty for technology developers, engineers, and entrepreneurs because of the wording of the legislation and its interpretation and because the GDPR's standards and principles contradict the functioning of machine learning and artificial intelligence (Layton, 2019, p. 6). CMA argues that the GDPR hampers the ability of organisations to innovate and contribute to economic growth. Many organisations dedicated resources to lawyers, consultants, and compliance professionals once the GDPR was implemented, leaving other organisational priorities with fewer assets (CMA, 2022, p. 11). In addition, despite the intention of the technologically neutral text, GDPR is considered incompatible with many technological solutions, such as artificial intelligence or automated

decision-making. Following this, companies choose to innovate less or pursue their ideas in less restrictive jurisdictions (CMA, 2022, p. 25).

Another significant concern is GDPR's disproportionality relating to the human rights framework. The primary assumption is that the purpose of the GDPR is to protect individuals and their data-related rights. However, according to CMA's report, it is often not taken into account that data can be highly beneficial to individuals and society as a whole in numerous cases. CMA suggests that data protection should be assessed via a human rights lens in cases of government surveillance and other state-run privacy-intrusive activity. The nature of the relationship between an individual and a private organisation, on the other hand, is fundamentally different, necessitating a different perspective and legislative approach. In addition, it is presumed that if customers share their data with an organisation, this organisation is expected to use customers' data to serve their customers better (CMA, 2022, p. 23-24).

Another source of dissatisfaction with the GDPR is that, in some cases, it still allows the EU Member States to deviate from the regulation and apply national rules instead, despite its direct applicability. A number of provisions in the regulation allow for derogations, resulting in differing norms that threaten the primary idea of the GDPR to have a unified European law (Newman et al., 2020, p. 284). It is also claimed that, rather than harmonising data framework across Europe, the GDPR has allowed for different interpretations of its provisions depending on a Supervisory Authority. Furthermore, while one of the GDPR's key organisational objectives was to reduce administrative burdens, it ended up increasing costs for governments across the EU (CMA, 2022, p. 8).

In the doctrine, additional shortcomings of the GDPR may be found. One of the most escalated GDPR benefits was more transparency and greater trust online. However, with the introduction of the GDPR, users' visits to digital domains result in intrusive pop-ups and disclaimers. Surveys show that this results in no greater sense of trust online (Layton, 2019, p. 6). Some critics of the GDPR even state that with the adoption of the regulation, free speech and freedom of expression are restricted due to rigorous GDPR compliance standards (Layton, 2019, p. 5).

Heiman suggests that the GDPR is more of a protectionist economic instrument than it is about protecting European privacy ideals (Heiman, 2020, p. 953). It is evident that despite the far-reaching EU's approach to data protection regulation and strict compliance requirements, the GDPR has numerous shortcomings or at least challenging opinions regarding

actual compliance at the organisational level. While it is undisputed that GDPR certainly benefits the human rights framework approach, the question remains whether this approach is the one preferred by society. Part 3 of this thesis looks at these shortcomings from the economic analysis perspective.

2. US DATA PROTECTION REGULATION MODEL: FALLING BEHIND THE GDPR OR TAKING A STEP AHEAD?

DLA Piper's research attributes the EU and US data protection models to countries with heavy data protection regulation and enforcement (DLA Piper, 2022). However, the author considers that the US model significantly contrasts with the EU model. Even though the US does not have one comprehensive data protection legislation applicable at the federal level, specific data protection rules apply to different fields of activities. Nevertheless, it is fair to claim that, at the federal level, it is challenging to protect all individuals irrespective of the field of activity of the organisation which processes data. This results in extensive discussions about whether the US needs comprehensive federal data protection law or should stick to the notion that the company is the one to know better how to process data and protect data subjects.

2.1. The US Model – Polar Opposite of the EU Data Protection Regulation Framework

While it is claimed that privacy regulations in the US and the EU share conceptual foundations and developed in similar directions early in their histories, their progress has taken different pathways in recent decades. These jurisdictions now occupy what may be viewed as the polar opposites of liberal democracies' regulatory approaches to data privacy. The EU has emerged as a leader in enacting comprehensive privacy law, which creates broad standards of protection that limit both public and private actors' acquisition and use of personal data. There is no such complete list of rules in the US. Federal business legislation is limited to specific subfields (Frankenreiter, 2021, p. 23).

In the US, there is no constitutional right to data privacy comparable to the EU's right to data protection established in the Charter. The US Constitution does not include "horizontal-to-horizontal" or private relationships between persons. Furthermore, the Constitution does not require the government to adopt proactive measures to allow for the existence of fundamental privacy rights (Schwartz & Peifer, 2017, p. 132-133). Even though the US Constitution does not expressly mention privacy, the US Supreme Court has repeatedly acknowledged "zones of privacy" within the constitutional text (Maldoff & Tene, 2019, p. 296). Scholars state that even in the lack of official regulation, accountability mechanisms arose in the private sector in the US as a way to safeguard brand reputation, meet customer expectations, and reduce risk. With the growth of data technology in the late 1990s, corporations were obliged to spend internal

resources to safeguard customer expectations in the emerging digital economy (Maldoff & Tene, 2019, p. 301).

The fact that the US does not regard the right to privacy as a fundamental right, according to academics, relates to the US's weak heritage of data privacy that is entirely opposed to the EU's comprehensive data protection framework. As the EU headed towards the Data Protection Directive's broad approach in 1995, the US chose a limited, sectoral approach. The US has selected corporate freedom as a fundamental value in the privacy field by focusing the federal legislation on specific areas of concern. Outside of specialised areas, the focus is on enforcing businesses' privacy obligations to consumers rather than detailed laws defining what companies can and cannot do with data (Chander et al., 2021, p. 5).

Even though the US has a broad range of regulations, most focus on data usage and disclosure rather than data collection limitations. Scholars assume that such a tendency is unsurprising given that US corporations are the world's leading commercial profiteers of personal data. Until the development of the Data Protection Directive and its replacement – GDPR – US companies and the US government could use their economic and political power to use personal data as they wished with very few negative consequences (Greenleaf, 2013, p. 39). However, with the extraterritorial scope of the GDPR, US companies targeting EU users are obliged to *de facto* comply with the EU data protection standards even if their main activity focuses on users in the US.

To understand the variety of legislation concerning data protection issues and the asymmetry in the scope of different laws, the author further summarises the main features of the selected federal sectoral laws that include some types of data protection rules (Table 1).

Table 1. US Federal Sectoral Data Protection Laws and Their Main Features

Sectoral law	Main features
Health Insurance Portability and Accountability Act (**HIPAA**)	• Data protection rules are enshrined in the HIPAA Privacy Rule. • Applies to communication between individuals and "covered entities," such as doctors, hospitals, pharmacies, insurers, and other organisations of a similar nature. • Applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. Does not apply to all health data (e.g., health data collected through various apps). • Requires appropriate safeguards to protect health data and sets limits and conditions on the uses and disclosures that may be made of such data without an individual's consent.

	• Gives individuals rights over their protected health data, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health data in an electronic health record, and to request corrections.
Gramm-Leach-Bliley Act (**GLBA**)	• Consists of three sections: o The Financial Privacy Rule regulates the collection and disclosure of private financial data. o The Safeguards Rule stipulates that financial institutions must implement security programs to protect such data. o The Pretexting provisions prohibit the practice of pretexting or accessing data using false pretences. • Governs the use of non-public personal data by financial institutions and organisations, such as banks, insurers, and brokerage firms. • Requires consumer financial products (e.g., loan or investment services) to disclose how they share data and allow customers to opt-out. • GLBA compliance requires that companies develop privacy practices and policies that detail how they collect, sell, share and otherwise reuse consumer data. • Grants the Federal Trade Commission (**FTC**) the authority to enforce obligations that create standards for financial institutions on administrative, technological, and physical data protection.
Federal Trade Commission Act (**FTC Act**)	• Allows the FTC to pursue companies that violate their published privacy policies and other data protection notices. The FTC can also investigate breaches of privacy-related marketing language and is granted the possibility to issue advisory opinions on privacy matters. • Grants the FTC broad jurisdiction to regulate data activities that are "unfair or deceptive acts or practices in or affecting commerce." • Gives FTC the power of the nation's *de facto* privacy regulator, and its rulings constitute a sort of common law privacy (Chander et al., 2021, p. 5).
Children's Online Privacy Protection Rule (**COPPA**)	• Imposes certain limits on a company's processing of children under 13 years old data. Companies are obliged to: o Give notice and obtain parental approval before collecting data from children. o Publish a privacy policy that is "clear and comprehensive." o Keep the data they gather from children privately and secure. o Grant a right to revoke consent and have data deleted. • Entitles FTC to take law enforcement actions against organisations that fail to comply with the provisions of COPPA. • Since 2013 FTC brought legal actions under COPPA before 20 companies, including big tech actors such as *Google*, *YouTube*, *Miniclip* and others.
Fair Credit Reporting Act (**FCRA**)	• Covers data from a person's credit report. • Obliges to comply with consumer reporting agencies, furnishers, and consumer report users. • Restricts who has access to a credit report, what the credit bureaus may collect, and how data is collected. • Grants individuals with rights such as being notified if a company takes any adverse action against them based on data in a consumer

	report, to have inaccurate, incomplete or unverifiable data corrected or deleted and others.
Family Educational Rights and Privacy Act (**FERPA**)	• Details who can request a student's educational records. This includes allowing parents, eligible students, and other schools to review a school's educational records. • Parents or eligible students may request that a school corrects a record they believe to be inaccurate or misleading. • Allows schools to disclose data from a student's education record, without consent, to other parties under the set conditions
Electronic Communications Privacy Act (**ECPA**)	• Protects wire, oral, and electronic communications from government surveillance while those communications are being made, are in transit, and when they are stored on computers. ECPA applies to email, telephone conversations, and data stored electronically. However, because ECPA was designed before the Internet revolution, it is considered to not grant protection against current surveillance techniques. • Prohibits government wiretapping of phone calls and other electronic communications. Includes provisions that protect a person's wire and electronic communications from being intercepted by another private individual. • Establishes guidelines for companies' monitoring of employee communications.
Video Privacy Protection Act (**VPPA**)	• Prevents the disclosure of Video Home System (VHS) rental records. • Specifies that this audio-visual customer data may only be disclosed to a law enforcement agency if it relates to a warrant issued.
Computer Fraud and Abuse Act (**CFAA**)	• Addresses legal and illegal access to federal and financial IT systems. • Imposes liability when a person uses a computer without authorisation or exceeds permitted access and acquires data from any protected federal computer.

Source: Compiled by the author based on the US Congress database, available at: https://www.congress.gov/ and other publicly available sources (such as FTC published information and others)

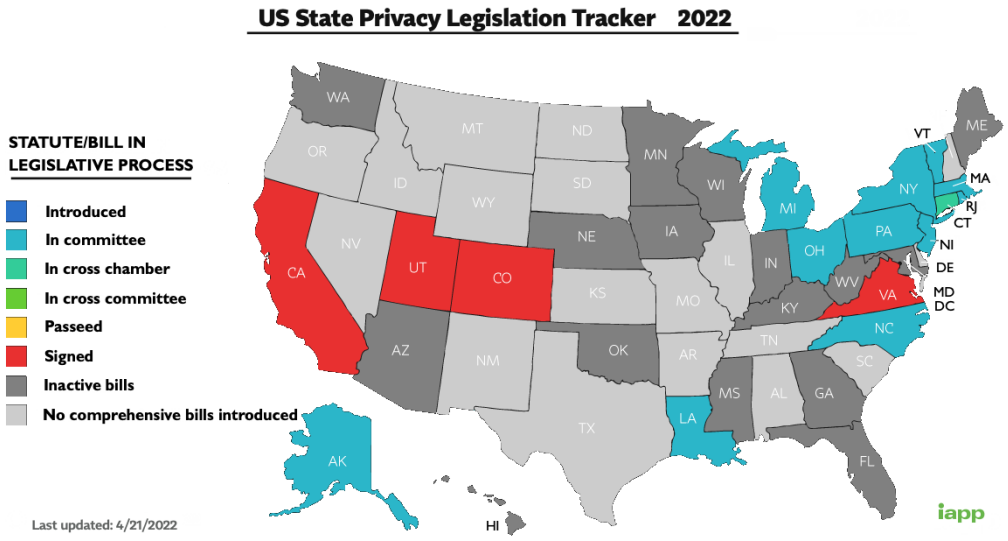
Because of the VPPA, which was passed in 1988, consumers may be confident that their VHS rental records will never be released without their authorisation. However, it seems fair to claim that in the 21st century, with significantly more widespread and pervasive technology, these regulations provide insufficient protection for US citizens because of being outdated and their limitations in scope.

The sectoral US framework does not provide similar rules for actors in different fields; therefore, it creates asymmetry in the market regarding the protection granted to individuals. However, these sectoral legal acts mainly concern data protection rules related to data security and information disclosure. All legal acts apply to specific actors (e.g., educational institutions) or concern the processing of specific data (e.g., credit report processing). Some of these legal acts establish specific institutions (e.g., FTC Act) or grant an institution a supervisory power (e.g., COPPA). Some of these legal acts establish a certain list of rights for data subjects (e.g.,

HIPAA, FCRA); others are closely related to individuals' protection from state-performed surveillance (e.g., ECPA).

Apart from the choice of sectoral legislation framework, another notable feature of the US data protection regulation model is that each state is entitled to set its general data protection rules. Even though states may enact state-level laws, there is no consistent tendency in this matter. Until the date of submission of this thesis, only four states have enacted comprehensive privacy laws – California, Virginia, Colorado and, very recently, Utah. Numerous other states have introduced such legislation or referred it to committees, while others did not begin any procedures at all (Image 1).

Image 1. US State Privacy Legislation Tracker



Source: International Association of Privacy Professionals, 2022. Available at: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

However, scholars propose that if each state passes its data privacy legislation, there will undoubtedly be enough variations between them that it will be challenging to comply with all of them (Kessler, 2019, p. 127). These concerns are supported by the legislative history in the EU when one of the GDPR adoption reasons was the inconsistency of national data protection laws across Europe.

The California Consumer's Privacy Act (**CCPA**) (passed in July 2018 and came into force in January 2020) is considered the "most far-reaching privacy bill ever adopted" in the US (Kessler, 2019, p. 102). Scholars declare that it is no surprise that California was the first state in the US to enact comprehensive privacy legislation as, unlike the US Constitution, California's Constitution has an explicit right to privacy in Article 1 (Newman et al., 2020, p.

276). In addition, California has historically been a privacy watchdog, with its legislative measures frequently inspiring other states to follow. For example, California was the first state to implement a data breach notification legislation. Unlike the GDPR, the CCPA generally applies only to large businesses that profit significantly from the sale of consumer data. Subsequently, California enacted the California Privacy Rights Act (**CPRA**), scheduled to take effect on January 1, 2023. The CPRA is anticipated to strengthen certain features of the CCPA and bring state legislation closer to the GDPR.

However, the US chosen federal sectoral and state-level approach does not necessarily mean that the progress of privacy protection has ceased to operate. Some scholars argue that an entire business is devoted to creating corporate responsibility and reducing privacy threats to protect brand reputations and customer confidence (Maldoff & Tene, 2019, p. 309). Data privacy in the US is essentially a question of the contractual relationship between customers and companies in practice where sectoral regulation is not applicable. Businesses are not subject to significant restrictions regarding their data practices as long as they offer customers an accurate and transparent explanation (Frankenreiter, 2021, p. 24-25). On the other hand, leaving privacy to self-regulation may lead to significant asymmetry in the market depending on the company's responsibility and approach to data protection.

Over the last few decades, the US has attempted to balance data privacy and its leadership role in inventing emerging technologies. A number of high-profile data breaches in both the public and private sectors and concerns about disinformation and the misuse of personal data are influencing public perceptions of privacy in the US. For example, the 2018 *Cambridge Analytica* incident, in which up to 87 million users' data may have been unlawfully shared with a political consulting business, has heightened citizens' awareness of the need for a data protection framework review (Newman et al., 2020, p. 268). In addition, with the introduction of various tracking apps and surveillance performed by states, the Covid-19 pandemic has only heightened the importance of privacy and cybersecurity considerations.

One of the distinguishing elements of the consumer privacy legislation in the US is that businesses are by default free to collect, process, and share data obtained from their consumers. Consumers are only legally protected in a limited number of situations. First, sectoral federal legislation concerns only data actors in certain fields and/or specific data types; general privacy legislation applies only in a few states. The US has rejected broad data privacy legislation a number of times, choosing a patchwork of industry-specific legislation. Second, data practices

may violate rules, not of a particular data privacy legislation but rules of consumers' protection in general (e.g., FTC jurisdiction focuses on enforcing civil antitrust legislation in the US and promoting consumer protection) (Frankenreiter, 2021, p. 24).

The US relies on the premise that companies better know their clients, therefore, can better establish self-regulatory privacy rules. However, the US has established specific sectoral laws that protect a certain type of data or certain data subjects at the federal level. These sectoral laws focus on what could be considered market fields that require more protection due to their sensitive nature. Such a framework means that there are entities not covered by any type of data protection law if they fall out of the scope of sectoral legislation. In addition, separate states are granted the right to decide on their state-level data protection framework, with the possibility to create different protection for residents of different states. It is also evident that the US does not have a unified data protection enforcement system.

2.2. One Law to Rule Them All: Does the US Need a Federal Data Protection Law?

The support for the lack of unified federal data protection law mainly relies on the freedom of business and the possibility to use personal data almost unrestrictedly. In the current market model, processing personal data means more profit for technology-based organisations. More personal data – more possibilities to provide personalised advertisement, create customer profiles and use other methods to increase sales or benefit otherwise. In addition, broad data protection regulation creates more limitations for technological developments. Personal data is usually necessary to improve machine learning and artificial intelligence-based technologies; therefore, any restrictions or obligations related to data protection are additional burdens for companies developing new technologies. It is even said that because of the lack of comprehensive data protection legislation in the US, this jurisdiction is more technology-friendly than the EU, hence putting the US ahead in the technological development race.

Despite clear advantages for business activity and advanced technological development, the US data protection framework faces severe criticism. First, although there is sectoral privacy legislation and many of the fifty states have passed some type of data breach notification legislation and begun adopting general privacy laws, the application, scope, enforcement, and sanctions vary greatly. This inconsistency in state laws has necessitated a thorough examination of applicable state policies, resulting in increased costs for US businesses that process personal data and the complexity of responding to a potential data breach scenario. In addition, this asymmetry creates uncertainty for data subjects as their data

processing depends on the state, field of activity, type of organisation and other variables. So far, the adoption of comprehensive state-level data protection legislation has received mixed reviews. For example, as for the CCPA, Kessler indicates that many have criticised the law's quick passage through the legislature, allowing for little input from those affected by it. According to both proponents and opponents of the law, the current version of the CCPA is considered unacceptable. Some privacy supporters feel the legislation only protects customers' rights in a limited way and that it should be expanded. At the same time, opponents contend that it is a "serious danger" to businesses in California (Kessler, 2019, p. 110).

Second, the US chosen model is often seen as not providing individuals with the necessary level of human rights protection. There are visible tendencies that US citizens are becoming more concerned about their privacy. In 2016, Pew Research Centre (**PRC**) published a report stating that many Americans believe that having their online behaviour tracked is in their best interests or that it is a price to pay for free or discounted products (Rainie and Maeve Duggan, 2016). Four years later, another PRC research found that about half of adults in the US (52 per cent) indicated they recently opted not to use a product or service because they were concerned about how much personal data would be gathered (Perrin, 2020). It may be considered that such a shift in the mindset is supported by massive data breaches, such as *Cambridge Analytica*, and the increased global attention to privacy due to the introduction of the GDPR.

In addition, the fact that the FTC *de facto* acts as the federal Supervisory Authority creates uncertainty for companies operating in the US. When businesses pledge to protect their customers' data, the FTC supervises and takes legal action to keep these commitments. The legal actions are taken before the companies when they have violated consumers' privacy rights, misled them by failing to maintain the security of their personal data, or caused significant harm to consumers. In many cases, FTC has charged organisations with violation of Section 5 of the FTC Act, which prohibits unfair and deceptive actions and practices in or affecting commerce. The FTC enforces other federal laws pertaining to consumer privacy and security in addition to the FTC Act (e.g., COPPA, GLBA and others) (Federal Trade Commission, 2018). Since 2020, according to publicly available information, the FTC has taken action against 20 organisations, including tech giants such as *Facebook*, *Zoom*, *Miniclip*, *Flo Health* and others. On the one hand, the possibility to assess privacy practice in terms of fair commercial practices allows the US to have at least a limited way to supervise

organisations for their data protection practices. On the other hand, in most cases, the approach to such supervision is through the prohibition of deceptive actions against customers and not through specific privacy rules. As a result, there is a lot of ambiguity and subjectivity in investigations as FTC each time assesses how well corporations kept their promises to their customers in terms of data protection. According to *DLA Piper's* research, many state attorneys have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states. The state attorneys general sometimes work together to enforce actions against companies for actions that broadly affect the consumers of multiple states (DLA Piper, 2022).

In the eyes of EU institutions, the US national security laws are considered a significant threat to personal data protection from the user's perspective. Under the US national security laws (FISA (Foreign Intelligence Surveillance Act) 702, Patriot Act and others), Internet service providers are required to supply the National Security Agency with all communications to and from a selected person of interest, some of which are also transmitted to the Federal Bureau of Investigation and the Central Intelligence Agency. In general, this means that any personal data may be disclosed to the US national security institutions if there is sufficient suspicion that such data and its holder threaten national security. According to the CJEU findings in the *Schrems II* judgment, the US authorities' intelligence activities undermine not only US citizens' privacy but also the data protection of EU citizens in cases where US organisations process data concerning Europeans. The CJEU held that neither of the assessed US national security laws correlates to the minimum safeguards under the EU law and that data subjects have no right to an effective remedy. As a result, no data may be transferred to the US-based entities without additional safeguards imposed by the data exporter (an organisation that is transferring data) and data importer (an organisation that is receiving data).

However, in March 2022, the US and EU announced the general agreement on the Trans-Atlantic Data Privacy Framework. This agreement is yet to be transferred to legal documents. Still, press releases ensure that the US has committed to implementing new safeguards to ensure that intelligence activities are necessary and proportionate in pursuing defined national security objectives, which will ensure the privacy of EU personal data (Fact Sheet, the United States and European Commission Announce Trans-Atlantic Data Privacy Framework, The White House, 2022). The agreed framework ensures that intelligence collection may be

undertaken only where necessary to advance legitimate national security objectives and must not disproportionately impact the protection of individual privacy and civil liberties. In addition, the U.S. intelligence agencies will be obliged to adopt procedures to ensure effective oversight of new privacy and civil rights standards. Under this new framework, it will be required to adhere to the Privacy Shield mechanism (which was undermined by the *Shrems II* judgment), and EU individuals will reserve the right to resolve complaints about organisations participating in the mechanism. The final legal documentation will provide more clarity regarding the renewed data protection framework; however, at first glance, the imposed changes do not seem revolutionary and provide more assurance only for intelligence-related data processing rather than the general level of data protection in the US.

There are opinions that Washington is miles behind Brussels because of the lack of federal data protection legislation. Several CJEU's judgments that the US is not secure enough to store European data helped reinforce this perception. However, this view is opposed by considering it false framing. The data on the sum of imposed fines for data protection violations and targeted big tech companies show a more rigorous approach in the US than the EU tends to consider. With a 5 billion dollars (around 4,4 billion euros) fine to *Facebook*, FTC surpassed the EU enforcement action, which does not reach 2 billion euros considering fines imposed by all Supervisory Authorities across Europe. In addition to the *Facebook* fine, *YouTube* was fined 170 million dollars (around 150 million euros) in 2019 for violating children's privacy. *Equifax*, the credit-reporting firm, was fined 575 million dollars (around 510 million euros) for a nationwide data breach in the same year. *TikTok*, a Chinese-owned video sharing app, was fined 5.7 million dollars (around 5 million euros) for illegally gathering children's online data (FTC, 2022). However, 2021, privacy-wise, was also not a very good year for big-tech companies in the EU. *Amazon* was fined 746 million euros in Luxembourg, *WhatsApp* was fined in Ireland (225 million euros), and France imposed a fine on *Google* (150 million euros) and *Facebook* (60 million euros) (GDPR Enforcement Tracker, 2022).

Taking the public opinion and changes in the international arena into account, the US comes back to discussions on whether one federal law to rule all sectoral laws shall be adopted. The academic discussion is divided into two camps – for and against the need to enact federal data protection legislation. Kessler suggests that the US should adopt a federal standard that would grant consumers equally strong protection as the GDPR or the CCPA. Large technology businesses are concerned about having to comply with a patchwork system of regulations,

which will likely be more expensive and burdensome than complying with a single state's law because other states are expected to follow California's lead and implement rules similar to the CCPA. Most businesses would reject legislation as harsh as the GDPR, and privacy activists claim that these businesses are just trying to pre-empt laws like the CCPA by establishing a diluted standard that is considerably less stringent than California's. Privacy activists reject this strategy and have stated that they would fight attempts to pass a watered-down federal law that pre-empts state laws (Kessler, 2019, p. 123). The disruption – pandemic-related issues like vaccine certificates, digital contact tracing, and mobile health apps – have helped put privacy and data security at the forefront of public debate, changing the public demand for the federal privacy law.

There are certain advantages whether the federal law is enacted. Rather than requiring consumers to parse through privacy policies and understand the nuances of various state laws, federal data privacy legislation would clarify which baseline rights they are entitled to when it comes to safeguarding their data and ensure there are appropriate enforcement mechanisms in place. Furthermore, comprehensive legislation at the federal level would benefit businesses in a certain way. Rather than monitoring fifty different state laws and sectoral federal legislation and attempting to assess, interpret, and design frameworks that comply with each, federal legislation would provide a simplified framework for company compliance and help the companies to understand better data privacy requirements and follow them. There are opinions that federal privacy legislation in the US would benefit the economy. Adopting federal data privacy legislation would promote data sharing with organisations subject to privacy standards, such as the GDPR, because data processed by US organisations would be more compatible with these standards.

A primary conceptual point of debate concerning federal data protection legislation is whether to utilise the so-called "prescriptive" method or an "outcome-based" approach to achieve the set law's objectives. Under the prescriptive approach, the government defines data protection rules and requires regulated individuals and entities to comply with those rules. An alternative methodology is an outcome-based approach whereby the government focuses on the outcomes of organisational practices rather than defining the practices themselves (Congressional Research Service, 2019, 55-56). The fact that the EU has already created the data protection framework could benefit the US if it adopts a GDPR-style data privacy law. Because many American companies do business in the EU, they are legally required to follow

the GDPR. If the US data privacy rules and regulations followed the GDPR's model closely, it would eliminate the necessity for organisations to develop a separate set of data protection measures for US customers.

The approach to federal data protection legislation largely depends on the US administration. The Obama administration attempted to introduce a Consumer Privacy Bill of Rights, but it was met with strong opposition and lost momentum. The Trump administration has refused to implement a national policy despite the EU's pressure. Furthermore, the FTC did not recognise the right to be forgotten under Trump's presidency, contradicting one of the GDPR's and the CCPA's core principles (Kessler, 2019, p. 124). Biden's administration has already drawn attention to privacy issues in the US – in July 2021, President Biden signed the Executive Order on Promoting Competition in the American Economy, which attempts to increase competition in the US and resolve issues related to monopolistic behaviours, including with respect to privacy and data protection. It is expected that Biden's administration will push forward the process of federal data protection legislation. There are opinions that the US big-tech companies have too much influence on the approach to federal privacy law. Many big-tech businesses have a vested economic interest in ensuring that any online privacy legislation is minimal and does not impose undue restrictions on their business models because data equals power in their view. On the other hand, public concern is that the US is falling behind its primary rival – China – without federal privacy legislation, as China adopted the Personal Information Protection Law in 2021.

Discussions on the federal privacy legislation emphasize that whatever law is passed, it must be flexible to avoid the outdated law in the next few years. The law should have meaningful protections for consumers, so it needs to require companies to be transparent in how they use data and what data is collected. It also means it needs to give consumers meaningful and not just check-the-box type choices. Businesses often raise concerns that any privacy legislation should have some kind of safe harbour provisions so that companies understand that if they take specific steps under such legislation, their activity is considered consistent with the law, and the risk of sanctions is minimal. This approach would reflect the need to balance the interests of businesses and the interests of consumers. Even while the US continues to negotiate federal legislation, some companies tend to keep aware and be proactive. Any legislation approved in the US will probably include elements of the GDPR, CCPA, other state laws, artificial intelligence, and other privacy and consumer protection areas. Compliance

with such standards at the moment will ensure a smoother transition when a complete law is finally implemented in the US.

Considering the US chosen data protection regulation model, there is no comprehensive set of rules in the US that apply to all consumers regardless of the services they receive or the state they are located in. The US's chosen restrained approach to a broad data protection regulation was one of the reasons that caused difficulties with unrestricted data flow with the EU. Following this and US-based companies' emerging use of data, discussions regarding the adoption of comprehensive federal law are relevant as ever. The author considers that further analysis through an economic lens may provide significant insights for harmonising the US preferred companies' freedom and consumers' rights to privacy.

3. TO REGULATE OR NOT TO REGULATE, THAT IS THE QUESTION: ECONOMIC ANALYSIS OF DATA PROTECTION REGULATION MODELS

The main features of the EU and US data protection regulation models show that these models differ in the fundamental approach to the right to data protection and who shall bear the responsibility to decide on the level of protection that is granted to individuals. Furthermore, the EU approach puts forward strict administrative regulation while the US has left more possibilities to resolve issues via tort liability in the data protection field.

These different approaches, among others, cause issues in cross-border data transfer cases resulting in extensive negotiations and discussions on the harmonisation of the approaches. Even though the EU and US agreed on the renewed framework, its solutions concern mainly intelligence-related data access but not the general privacy approach at the US federal level. The author considers that to prevent further clashes and achieve the most optimal result for both jurisdictions, the primary goal of data protection law must be reconsidered from its roots.

"Understanding costs is a critical step towards achieving privacy" (Chander et al., 2021, p. 42); therefore, one way to look at EU-US data protection models' harmonisation and their efficiency is to analyse the essence of the data protection law through the lens of social preference for strict regulation or liability if harm occurs. The author relies on the models of economic analysis of law to evaluate the data protection regulation models.

3.1. *Ex-Ante* Safety Regulation and *Ex-Post* Liability: Theoretical Concepts and How They Apply to Data Protection Field

Attempts to analyse legal solutions to certain issues through an economic approach are not new. Such approaches help to evaluate the practical efficiency of a chosen regulatory framework. In this part, the author provides an overview of the scholars' developed economic approach to a preference for either *ex-ante* regulation or *ex-post* liability in terms of data protection legislation. This analysis is largely based on notions and social preference models formulated by S. Shavell in "Liability for Harm Versus Regulation of Safety" (Shavell, 1984). The main ideas of S. Shavell are summarized below.

In his work, Shavell mainly analyses why society prefers to strictly regulate some fields or leave them unregulated with the possibility of tort liability. Shavell describes that tort liability (***ex-post* liability**) is private in nature and works not by social command but by the

effect of legal damage actions that may be brought once harm occurs. Standards, prohibitions, and other types of safety regulation (***ex-ante* regulation**), on the other hand, are public in nature and modify behaviour immediately through requirements imposed before, or at least independently of, the occurrence of harm (Shavell, 1984, p. 357).

Shavell indicates four determinants of the relative desirability of *ex-post* liability and *ex-ante* regulation. According to Shavell, to identify and assess the factors determining the social preference of liability and regulation, it is necessary to set out a measure of social welfare. He assumes that this measure equals the benefits parties derive from engaging in their activities, less the sum of the costs of precautions, the harms done, and the administrative expenses associated with the means of social control. According to him, the formal issue is to employ control mechanisms to maximise the welfare measure. Shavell outlines four factors that impact the solution to this issue (Shavell, 1984, p. 358-359) (Image 2).

Image 2. Shavell's Determinants Defining Social Preference for *Ex-Ante* Regulation and *Ex-Post* Liability

Source: Compiled by the author based on S. Shavell's article "Liability for Harm versus Regulation of Safety" The Journal of Legal Studies (1984).

The first determinant is "the possibility of a difference in knowledge about risky activities." Shavell considers that giving the regulator the power of control when private parties have complete information about risky behaviour about which the regulator has little knowledge will lead to a high probability of regulation errors. The regulator's standard will be excessively strict if it overestimates the possibility of harm caused by the risky activity. In the opposite case, if the regulator makes contrary errors, its requirements may be overly lenient (Shavell, 1984, p. 359). Shavell describes that because the private parties are the ones who are engaged in and benefit from their actions, they should have an inherent advantage in knowledge. Obtaining such information for a regulator would usually need nearly constant

surveillance of parties' conduct, which would be practically impossible. However, in some specific fields, information about risks may not be evident and will take effort or particular competence to analyse, which the regulator may supply in these situations by dedicating social resources to the task (one of the provided examples is the healthcare system) (Shavell, 1984, p. 360).

The second determinant for "the relative desirability of liability and regulation is that private parties might be incapable of paying for the full magnitude of harm done." In such cases, liability would not provide adequate incentives to reduce risk because private parties would treat losses that exceed their assets as an unproportionate burden. On the other hand, the capacity to pay for the harm caused would be irrelevant under regulation, assuming that parties would take steps to reduce risk as a precondition for engaging in their activities; therefore, any harm will be less likely to occur (Shavell, 1984, p. 360-361).

The third determinant is "the chance that parties would not face the threat of suit for harm done." This depends on the reasons why a lawsuit may not be filed. First, a defendant may avoid *ex-post* liability because the harms caused are widely dispersed, making it difficult for any single victim to pursue legal action. Second, there could be a significant period of time before any harm occurs; therefore, it could be impossible to gather the evidence needed for a successful suit. Third, it is challenging to assign guilt for harm to those actually accountable for it, as actual harm often may not be directly linked to certain actors (Shavell, 1984, p. 363).

The final determinant is "the magnitude of the administrative costs incurred by private parties and the public in using the tort system or direct regulation." The tort system's costs must be widely defined to cover private parties' time, effort, legal fees, and public expenses such as trial costs. Similarly, administrative costs of regulation encompass expenses of maintaining the regulatory establishment and the private costs of compliance. In this scenario, liability has the benefit because, in such cases, most administrative expenses are incurred only if harm occurs, while administrative costs are always incurred under regulation (Shavell, 1984, p. 363-364).

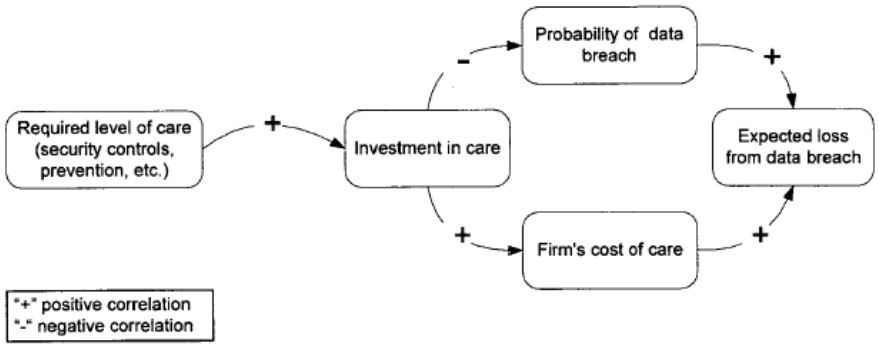
In conclusion, administrative expenses and differential in knowledge, according to Shavell, favour social preference for *ex-post* liability, but the inability to pay for the harm done and the opportunity to avoid lawsuits support *ex-ante* regulation. Shavell argues that these two approaches should not be seen as mutually exclusive. Instead, a comprehensive legal solution to any social problem should include *ex-post* liability and *ex-ante* regulation, with the balance

reflecting the significance of the determinants (Shavell, 1984, p. 365). The author applies the four determinants to compare the EU and US data protection regulation models in the analysis provided in section 3.2. below.

Shavell's and other authors' ideas on social preference for *ex-ante* regulation or *ex-post* liability are applied and expanded by other scholars specifically for the data protection field. A study by Romanosky & Acquisti examines the effectiveness of personal data protection legislation in the US through an economic analysis of law. These authors concentrate on consumer data breaches occurring due to the loss or theft of personal data stored by organisations. The authors provide an economic analysis of three legislative approaches for reducing the possibility for a company's activities to cause privacy harm: *ex-ante* safety regulation, *ex-post* liability, and information disclosure (Romanosky & Acquisti, 2009, p. 1065). Romanosky & Acquisti repeat the link between economics and law and how economic modelling can be used to evaluate the efficiency of various legislative methods.

Romanosky & Acquisti understand *ex-ante* safety regulation as a method of limiting or controlling an externality imposed by a company's harmful activity. This method intends to prevent harm by enforcing minimum standards or operating restrictions. In addition to Shavell's notion that *ex-ante* regulation is public, Romanovsky & Acquisti impose that businesses can establish safety standards through self-regulation. Romanovsky & Acquisti propose that companies must invest in a minimum degree of security controls to reduce the likelihood of a data breach and the associated harm (Romanosky & Acquisti, 2009, p. 1069) (Image 3).

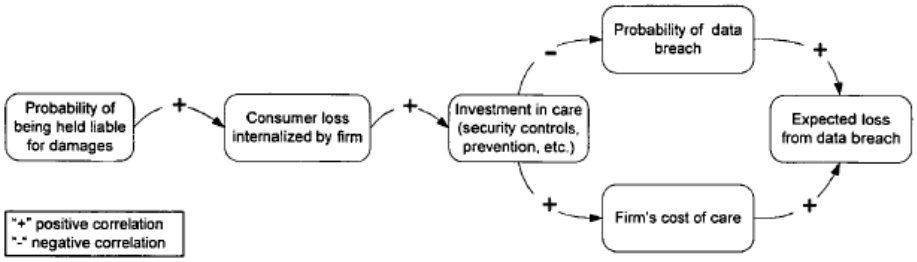
Image 3. Correlations of *Ex-Ante* Safety Regulation and Expected Loss Caused by Data Breaches



Source: Romanosky & Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1069.

In this study, *ex-post* liability is defined as a mechanism used after the damage occurs. This mechanism empowers victims to sue for damages, forcing businesses to internalise the part of the harm they cause. Suits in these cases are brought by private entities such as customers and businesses; hence it is private in nature (Romanosky & Acquisti, 2009, p. 1068). In the context of data breaches, victims who successfully demonstrate four conditions: (1) that an organisation had a duty of care to protect the plaintiff's data, (2) that organisation breached this duty, (3) that the actual harm was suffered, and (4) that this harm was a direct result of the organisation's breach of duty, are generally entitled to compensation (Romanosky & Acquisti, 2009, p. 1071). *Ex-post* liability is a deterrent for businesses by increasing the anticipated costs of engaging in a harmful activity and compensating affected parties (Romanosky & Acquisti, 2009, p. 1072) (Image 4).

Image 4. Correlations of *Ex-Post* Liability and Expected Loss Caused by Data Breaches



Source: Romanosky & Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1072.

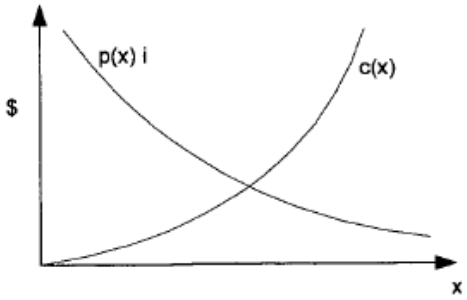
It is challenging to assess the impact of an *ex-post* liability approach. Romanosky & Acquisti indicate that the US courts frequently dismiss negligence claims because the plaintiff is unable to demonstrate actual damages, as required under negligence tort claims. (Romanosky & Acquisti, 2009, p. 1078). While it appears that customers may experience losses as a result of data breaches (whether financial, psychological, or expenses to prevent future harm), the judicial system has yet to acknowledge such harms properly (Romanosky & Acquisti, 2009, p. 1080-1081).

Romanosky & Acquisti introduces the information disclosure model, which requires businesses to provide information about the risks associated with their goods or services. However, in terms of this research, the author believes that information disclosure requirements are enshrined in the new generation data protection legislation (e.g., GDPR or

CCPA requirements); therefore, the author does not elaborate on the findings of Romanosky & Acquisti regarding this issue in further analysis.

Authors in the study indicate that it is not fully clear what criteria should be used to evaluate the impacts of various data protection regulation models. Even when the legislature's objective appears to be clear (i.e., to protect customers' privacy), the actual purpose of legislation may be more confusing. Is the goal of the privacy regulations to reduce the amount of harm that could be caused to individuals due to data breaches on average, improve business practices for each data processing operation, or both? While businesses and consumers would naturally advocate reducing their own private costs, the purpose of the social planner (regulator) is to reduce the sum of these costs (Romanosky & Acquisti, 2009, p. 1083).

Image 5. Basic Cost Functions



Source: Romanosky & Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1083.

To reflect how investment in privacy care correlates with the probability of data breaches, Romanosky & Acquisti provide a basic cost function (Image 5). Here x - some level of care; c(x) – the cost of this care; p(x) – the probability of the accident; p(x)i – expected harm (probability multiplied by the cost of investigating the cause of the accident) (Romanosky & Acquisti, 2009, p. 1084). In general, this basic cost function means that the higher investment (cost) in care, the lower probability of any data breach-related accident.

Table 2 provides how this basic cost function applies to a firm, consumer and general social loss.

Table 2. Basic Cost's Function Applicability to Different Actors

(1)	Firm loss = c(x) + p(x) i	x, c(x) and p(x), and i are as described above The firm's loss is equal to the sum of the cost of care and expected harm from the accident

(2)	Consumer loss = p(x) h	h is the total consumer harm The consumer's loss is equal to the probability of the accident multiplied by the total harm experienced by a consumer
(3)	Social loss = c(x) + p(x) [i + h]	Total social loss is composed of both consumer and firm loss

Source: Compiled by the author based on Romanosky & Acquisti "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1085.

Romanosky & Acquisti describes that the regulator's objective is to achieve a value of x (some level of care) that minimises equation (3) because social costs are lowest when the firm invests in the socially optimal level. To have the firm invest at this level, it must internalise the total amount of its harm. Nevertheless, firms are motivated by their own private costs; therefore, they invest in a level of care that minimises (1), not (3), which is always less than socially optimal (Romanosky & Acquisti, 2009, p. 1085).

Further authors provide formulas for basic cost functions' applicability to models of *ex-ante* regulation and *ex-post* liability (Table 3) (Romanosky & Acquisti, 2009, p. 1086-1088).

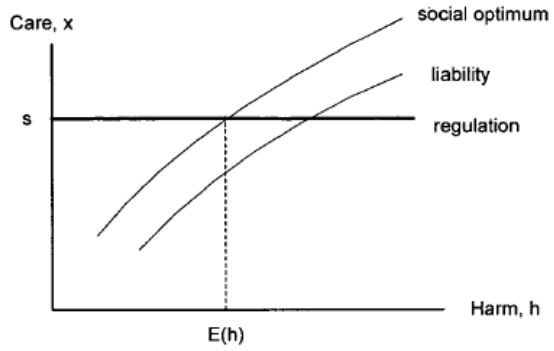
Table 3. Basic Cost's Function Applicability to Different Data Protection Regulation Models

Model	Formulas
***Ex-Ante* Safety Regulation** *Ex-ante* safety regulation requires the social planner to establish a standard level of care for all businesses, regardless of the harm they cause	Social loss = c(s) + p(s) [i + h] * *(s) is a mandated standard that holds the social cost constant with any change in care, (x)
	Firm loss = c(s) + p(s) i
	Consumer loss = p(s) h
***Ex-Post* Liability** *Ex-post* liability enables victims to be compensated for harm inflicted by businesses. As a result, the cost of the harm is transferred from the injurer to the injured	Firm loss = c(x) + p(x) [i + α h]* *Where α captures the probability of being held liable for damages and the portion of consumer harm internalised by the firm ($0 < \alpha < 1$)
	Consumer loss = p(x) [1 - α] h
	Social loss = c(x) + p(x) [i + h]

Source: Compiled by the author based on Romanosky & Acquisti "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1086-1088.

In summary of findings in Table 3, Romanosky & Acquisti declares that when social regulator imposes regulatory rules, part of the social loss will always be constant as the required investment in care will be the mandated standard. On the other hand, while applying *ex-post* liability, the social loss will always depend on the probability of being held liable for damages.

Image 6. Level of Care for Regulation, Liability and Social Optimum



Source: Romanosky & Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1089.

Image 6 shows *ex-ante* regulation and *ex-post* liability compared against the basic model regarding care as a function of harm. Given that the level of prevention (x) should reasonably increase with the probability and severity of harm, it is clear that the level of care taken by the firm under liability will always be less than is socially optimal for any given amount of harm, h, because of the probability of evading lawsuit. Regulation enforces a constant level of care that becomes socially optimal only at the average level of harm, E(h). It is considered inefficient because it enables high-risk firms (those more likely to cause harm) to underinvest in care and forces low-risk firms (those less likely to cause harm) to invest more than they should.

When companies do not bear the full cost of their misbehaviour, they will underinvest in care. The optimum level of care for the company will always be lower than the best level of care for society. The authors provide the table that shows how the company's losses are consistently lower than those of society (Romanosky & Acquisti, 2009, p. 1090) (Table 4).

Table 4. Basic Loss Equations

Policy Intervention	None	Regulation	Liability
Social loss	$c(x) + p(x)\,[i + h]$	$c(s) + p(s)\,[i + h]$	$c(x) + p(x)\,[i + h]$
Firm loss	$c(x) + p(x)\,i$	$c(s) + p(s)\,i$	$c(x) + p(x)\,[i + \alpha\, h]$
Consumer loss	$p(x)\,h$	$p(s)\,h$	$p(x)\,[1 - \alpha]\,h$

Source: Romanosky & Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1090.

The authors conclude that any of these policy approaches will only achieve the socially optimal outcome in rare and extreme scenarios (Romanosky & Acquisti, 2009, p. 1090). *Ex-*

ante regulation is efficient only for a single set of companies causing the average amount of harm; *ex-post* liability is efficient only when suits are always filed, and companies always pay for their harm (Romanosky & Acquisti, 2009, p. 1091). Following the limitations of these models, the authors provide extended loss equations (Table 5).

Table 5. Extended Loss Equations

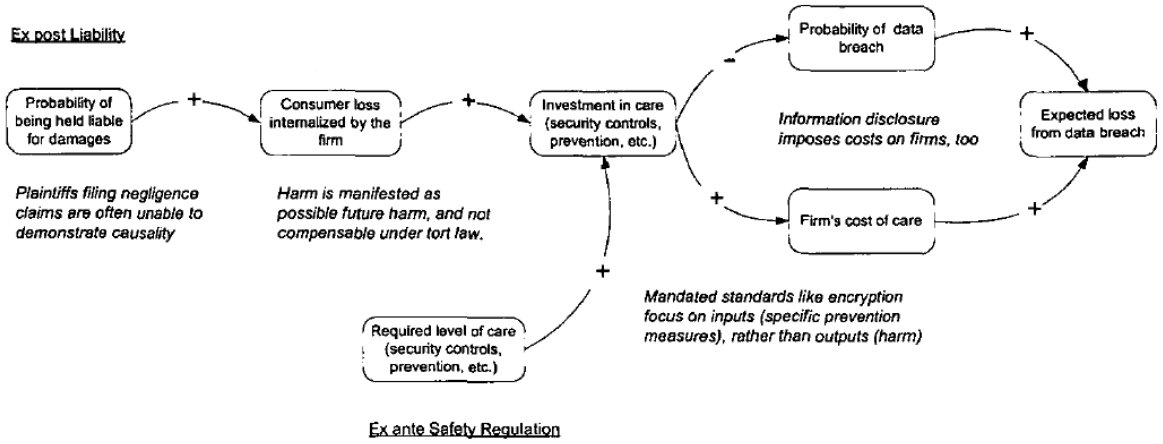
Policy Intervention	Regulation	Liability
Social Loss	$c(s) + \beta\, p(s)\, [i + h]$	$c(x) + p(x)\, [i + h]$
Firm Loss	$c(s) + \beta\, p(s)\, i$	$c(x) + p(x)\, [i + \alpha' h]$
Consumer Loss	$\beta\, p(s)\, h$	$p(x)\, [1 - \alpha']\, h$

Source: Romanosky & Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1098.

In these extended loss equations, authors claim that *ex-ante* regulation focuses on inputs (specific data protection and security-enhancing technologies) rather than outputs (the actual harm from data breaches). This implies that the firm's cost of care would remain unchanged, but now the probability of harm would be higher because care no longer perfectly corresponds to a lower probability of harm. $\beta\, p(s)$ represents the increase in the probability of harm, $\beta > 1$. As for the *ex-post* liability, it demonstrates inefficiencies because: (1) consumers incur direct and indirect costs from privacy invasions; (2) probabilistic harm is generally not compensable under tort law; and (3) plaintiffs filing negligence claims are often unable to demonstrate causality; therefore, a more accurate loss function would attenuate the value of α as α' where ($\alpha' < \alpha$) (Romanosky & Acquisti, 2009, p. 1097-1098).

The provided formulas by Romanovsky & Acquisti attempt to answer the question under which conditions would the firm's loss function approach the social loss; therefore, it results in the social optimum. The authors provide a compilation of policy mechanisms and their inefficiencies detected through the applicability of the set formulas. The image below illustrates the "causal relationships between the policy approaches, their intended effects on firm and consumer behaviour" (Image 7).

Image 7. Legal Mechanisms and Their Inefficiencies



Source: Romanosky & Acquisti. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." Berkeley Technology Law Journal, 2009, p. 1100.

The study of Romanosky & Acquisti proves that investment in care does not perfectly correspond to a lower probability of data protection related harm. Therefore, none of the chosen approaches are without shortcomings; hence, achieving the optimal social loss requires a combination of *ex-ante* regulation and *ex-post* liability. The study concludes that there is a difference between categories of costs associated with data breaches: firms respond naturally to private costs paid as a direct result of a data breach (through investigation, regulatory sanctions, etc.), causing them to increase their care. Evaluating consumer privacy harm, however, is more complex. The harm to them is probabilistic and manifested as direct and indirect, financial and psychological loss. Data breaches may cause loss that could be catastrophic for some while inconsequential for others.

The author does not apply the formulas of Romanovsky & Acquisti's study in further analysis but considers these findings illustrative in defining perception to a socially optimal level of data protection from different actors' points of view. The author describes this study to provide additional support to Shavell's notions that none of the approaches – *ex-ante* regulation or *ex-post liability* may be applied independently from the other in the data protection field as well. Additionally, Romanovsky & Acquisti's study points out important issues such as difficulties in evaluating possible harm and a lack of companies' willingness to invest in the socially optimal level of care.

3.2. Who is the Fairest One of All: Comparison of the EU and the US Data Protection Regulation Models Through the Lens of Economic Analysis

While the EU and US have different approaches to data protection, both of these jurisdictions attempt to combine *ex-ante* regulation and *ex-post* liability in their data protection regulation models. In this section, the author analyses the social costs of EU's and US's data protection regulation models and preference for either *ex-ante* regulation or *ex-post* liability based on the previously described Shavell's economic approach. The models are analysed by applying the four determinants that influence preference for *ex-ante* regulation and *ex-post* liability: (1) difference in knowledge about risky activities, (2) incapability of paying for the full harm done, (3) escaping the threat of suit for harm done, (4) administrative costs.

(1) Difference in knowledge about risky activities. This difference between private parties and state institutions is quite evident in the data protection field. In this context, Shavell refers to regulatory authorities, which, in the data protection field, in the author's opinion, shall include Supervisory Authorities. Supervisory Authorities interpret the data protection legislation, and *de facto* expand or narrow down the data protection rules. Technological neutrality of the data protection laws results in their equal applicability to big-tech companies and organisations that process data in a non-complexed manner. This presupposes that while it is not too difficult to have knowledge of basic operation principles and set standard rules for non-complexed cases, it is a different story for processing data using emerging technologies. The complicated technological solutions used for data processing may cause a significant difference in the information that companies and state actors possess. Additionally, the human rights lens taken by regulatory authorities could be considered a difference in knowledge because private parties in the data protection field often take the approach that consumers choose to give up their data to receive services or purchase goods; therefore, companies consider themselves the ones that should know better, how to serve the customers most efficiently.

The GDPR is constructed to be technologically neutral legislation; hence, the abstract provisions apply to different actors in various business fields. As a result, Supervisory Authorities possess different knowledge on the applicability of the GDPR depending on differences in data processing performed by various actors. Big-tech companies often process data in a complex way; for example, technical characteristics may not straightforwardly indicate whether particular data may be related to an identified or identifiable natural person

(e.g., data logs, encrypted data). These technical characteristics are an issue when Supervisory Authorities investigate organisations and apply GDPR principles to specific data processing operations. In such cases, Supervisory Authority may lack the expertise and resources to thoroughly analyse and understand the actual technical setting. This may result in fines that do not necessarily ensure the actual protection of personal data. Another factor proving the differential knowledge is the asymmetry of the burden that lies with the global corporations and small and medium enterprises. The latter are obliged to comply with the exact requirements imposed on the big companies. However, they often do not extensively process massive datasets or cause a significant threat to individuals. Such regulatory asymmetry may be considered what Shavell describes as a chance of regulatory error, where the EU overestimates the potential for harm in small and less intrusive data processing operations and sets too stringent standards.

The US model is based on the premise that private parties should generally enjoy an inherent advantage in knowledge of their risky activities. For a regulator to obtain the same information would often be practically impossible, especially when the information concerns complex technological solutions. This means that the general chosen US approach corresponds with the fact that regulators usually possess less information than private parties in the data protection field. In addition, due to the specifics of the jurisdiction, which allows separate states to adopt their legislation, it would be difficult for any federal regulator to possess a better knowledge of details of data protection than companies may have at a state level. However, the fragmented sectoral regulation is an example of what Shavell describes as better knowledge possessed by the regulator due to the specifics of the field that require special protection. For example, children's privacy protection under COPPA or health data protection under HIPAA shall be considered areas where private parties do not enjoy the same knowledge as the regulator. Following Shavell's notions in these areas, substantial regulation is not a coincidence but rather is needed, both because liability alone would not adequately reduce risks and because the usual disadvantages of regulation are not as severe as in the tort context (Shavell, 1984, p. 369).

As for the determinant concerning differential knowledge possessed by private parties and state actors, it is fair to state that the US model reflects such difference better than the EU model as it leaves a majority of data protection related decisions to organisations. In addition, the chosen US fragmentary approach to federal regulation reflects specific fields that require a

higher standard of protection and provides examples where the regulator possesses more knowledge than private parties. On the other hand, with technological neutrality, GDPR obliges Supervisory Authorities to possess more information than private parties on technological aspects to enforce the regulation. This often is impossible due to limited resources and expertise. At the same time, with the introduction of the GDPR, the regulator is often considered to have created too stringent rules for organisations that usually do not possess significant threats to individuals regarding their data.

(2) Incapability of paying for the full harm done. This Shavell's determinant shall be adjusted for a data protection field as data actors often measure risks relating to imminent administrative fines and not the harm-related costs. Shavell states that the party's assets are crucial in establishing whether this determinant favours more regulation or liability – the greater the likelihood of harm much larger than assets, the greater the appeal of regulation. However, such presumption shall be altered considering the importance of fines in the data protection field.

In terms of understanding harm, it has to be assessed how such harm is understood under the data protection legislation. As was also indicated by Romanovsky & Aquisti, while it is relatively easy to determine harm in cases of data breaches when a financial loss occurs (e.g., cases of identity theft), there are difficulties in measuring such harm when the loss is intangible (e.g., mere disclosure of personal data) or not related to data breaches (e.g., refusal to grant access to personal data held by an organisation). In addition to this, one could say that if the occurred harm is not tangible, could there be harm as such if consumers are the ones who give up their data in exchange for services or goods?

Inability to pay relates more to the failure to pay a fine than to pay for the harm done in the context of the GDPR. Usually, when organisations to whom the GDPR applies assess the risk, they consider the possibility of being fined and not the amount of damages that could be required to pay for the harm caused. However, the GDPR allows a Supervisory Authority to impose a fine for up to 20 million euros or 4 % of the annual turnover, whichever is higher. The second limit proved useful for fining major corporations – the top 10 GDPR imposed fines exceed the 20 million limit, with 746 million the highest fine imposed. Until 2022 more than 1000 fines reaching more than 1.6 billion euros overall were imposed by Supervisory Authorities across Europe (GDPR Enforcement Tracker, 2022). Some national jurisdictions in the EU may be considered stricter than the others, but close cooperation between the

Supervisory Authorities allows to, in general, keep the fine practice unified. While some of the fines do not cause a significant burden, there are examples when even a small administrative fine under the GDPR is too hefty for small organisations. For example, the Lithuanian division of the International Council of Monuments and Sites (ICOMOS) was fined 3000 euros fine for lack of legal basis for data processing under the GDPR. However, the court reduced the fine to 1500 euros considering the annual budget and the ICOMOS activity in the cultural heritage field (Judgment of the Vilnius Regional Administrative Court in case no. EI2-1249-789 / 2020). The possibility for courts to reduce fines is a safeguard for organisations to receive fair sanctions. However, the GDPR imposed approach of rigorous fines could generally propose that Shavell's determinant – incapability to pay – favours the liability more than the regulation.

Contrary to the EU's model, the incapability to pay for the harm done or pay a fine is not straightforward to assess in the US model. *De facto* FTC is empowered to fine organisations if they violate business practices. However, until 2022 the number of such actions does not exceed 20 on a federal level, according to the publicly available information. Other institutions are authorized to fine organisations under sectoral federal legislation; however, due to the very limited number of actions brought before organisations, a more significant concern in the US is the amount that would be entitled to pay if the lawsuit for privacy violations is successful. This is also related to the different litigation culture in the US compared to the one in the EU. Shavell argues that companies may use self-regulation to take precautionary measures and reduce possible harm to avoid large liabilities. However, available information shows that in the US, targets for hefty fines are usually big tech companies which also are at higher risk of facing a class action. Therefore, there is no pressing need for small and medium enterprises to assess the risk of the inability to pay a fine or face a lawsuit in the US.

While the general Shavell approach is that incapability to pay for the harm done favours *ex-ante* regulation, such presumption is not as simple in the field of data protection. This field is closely related to imposing fines; therefore, organisations assess not only the sum of possible damages but also possible fines in different jurisdictions. While the US jurisdiction is more abstract in terms of the possibility of fines, the EU has established a more or less unified practice of imposing fines across the EU Member States that does not seem to slow down. In addition, assessing the inability to pay for the harm done in both jurisdictions correlates with the understanding of harm related to data protection, which is not simple to define.

(3) Escaping the threat of suit for harm done. The possibility of escaping the threat of a suit for harm done is very likely in the data protection field. As explained in section 3.1., Shavell indicates that the importance of this aspect is partly determined by why a lawsuit may not be filed. First, the harm that may occur in the data protection field is hardly measured; therefore, the possibility of escaping suit is relatively high. Second, usually, in cases of massive data breaches, the harms a company generates are widely dispersed, making it unattractive for any victim individually to initiate legal action, especially against big-tech companies. This may be overcome by the possibility of maintaining class actions, whose application, however, may be problematic. In terms of this thesis, the author focuses on the possibility of class actions rather than individual claims. Third, difficulties for suing may occur due to a long period of time before actual harm related to a data breach occurs, meaning that the necessary evidence can be ineffective by the time the lawsuit is filed. Fourth, it could be challenging to attribute harm to certain parties responsible for it if, for example, malicious action that causes harm is performed by a third party that accessed data online and not by an organisation that was in possession of the data.

GDPR sets not only a fines mechanism but the right to claim damages for anyone who has suffered material or non-material harm due to a violation of the GDPR (Article 82(1) of the GDPR). In other words, this means that a breach under the GDPR may have consequences under both private and public law. Data subjects can seek compensation before national courts for material or non-material damage that results from the infringement of their rights under the GDPR. The regulation also sets the principle of full compensation for the plaintiffs, which is very protective of data subjects' rights. Some of the potential damages, such as costs incurred due to fraudulent spending, credit card charges, and so on, are straightforward to identify (and for companies to reimburse individuals for). In contrast, "non-material damage" is a more abstract concept under the data protection legislation.

While filing individual actions before corporations for causing harm may not look very promising, the GDPR provides for the possibility of class actions. According to Article 80 of the GDPR, a data subject has the right to appoint a non-profit entity, organisation, or association with statutory objectives in the public interest and activity in the field of data protection to file a complaint on their behalf. Spreading the cost of litigation across many plaintiffs creates a greater likelihood of challenges being brought in court. However, the situation of bringing collective action is not uniform across the EU. Even though the GDPR

states that the data subject "shall have the right to" initiate actions, it does not provide the data subject with an actionable tool; instead, EU Member States are responsible for this. In other words, because the GDPR does not cover the procedural elements of a data subject's claim, a reference to national procedural legislation should be made. This raises the issue that there could be as many personal data collective action procedures as the EU Member States, contrary to the GDPR's objective of consistency across Europe.

There are already class action cases in European jurisdictions under the GDPR. For example, Dutch courts awarded damages from *TikTok* for the GDPR infringements. Three organisations brought class actions that included declaratory relief and significant claims for damages relating to the validity of *TikTok's* general conditions and the use of personal data (Loyens et al., 2021). The Dutch and other courts abroad struggle with pinning a number to GDPR infringements or the question of when a GDPR infringement results in actual damages for data subjects. For example, because the plaintiffs attempted to adopt an abstract "lowest common denominator" approach to the damages, the UK Supreme Court rejected a lawsuit brought against *Google* for breach of UK data regulations. The UK Supreme Court disagreed with this procedure, ruling that a claimant must show that each individual member of the represented class suffered sufficiently substantial harm (Lloyd v. Google LLC, 2021).

Significant developments in the right to damages under GDPR infringement are expected in the near future. Currently, a case before the CJEU challenges whether compensating a claimant requires, in addition to a GDPR violation, that the claimant has experienced damage or if the infringement of GDPR provisions is sufficient itself (referral for a preliminary ruling by the Supreme Court of Justice of the Republic of Austria) (Global Privacy & Security Compliance Law Blog, 2021). If the CJEU decides that a mere GDPR violation is sufficient to claim damages from the data processor or data controller, this may result in unfair data subjects' positions before organisations that process data. Such development would raise the European data framework and protection of individuals' right to data protection to a level where any organisation violating the GDPR could face an administrative fine and lawsuits for harm on the mere infringement of the GDPR.

One of the examples of how fines and the possibility of damages may become a headache to companies is the *British Airways* case. The airline processed a significant amount of personal data without ensuring adequate security measures as required by Article 32 of the GDPR. Therefore, it failed to protect the personal and financial details from a data breach in 2018 that

resulted in the exposure of datasets of more than 400,000 of its customers. UK Supervisory Authority (**ICO**) originally served a notice of intent to impose a 218.51 million euros fine on *British Airways* but later reduced the imposed fine to 22.046 million euros (ICO, 2020). The *British Airways* example is good proof of incompliance with data security requirements that resulted in tangible harm for individuals. While the original fine was reduced significantly, more than 16,000 people have joined a class action seeking compensation from the airline related to the data breach. In 2021, *British Airways* settled the data breach class action. While the terms are confidential, due to a number of claimants, the group settlement may be just under – or equal to – the fine the ICO issued.

In addition to the challenges of showing the incurred harm, there are examples of other privacy class actions' difficulties in the EU. For instance, two tech giants – software companies *Oracle* and *Salesforce* faced class actions for not obtaining consent and misusing third party cookies used to track, monitor and collect the personal data of Internet users. Lawsuits were parallelly brought in the UK and the Netherlands, reaching 10 billion pounds and 15 billion euros accordingly. However, the Dutch GDPR class action against *Oracle* and *Salesforce* was inadmissible. The organisation that brought the class action (the *Privacy Collective*) argued that in view of its statutory objective, its constituency is formed by (in principle) all natural persons in the Netherlands who use the Internet. The *Privacy Collective* argued that it had met the representation requirement by collecting 75,000 "likes", obtained by clicking a "support button" on its website. The Court of Amsterdam in the Netherlands ruled that this was not sufficient, showing that not just any class action has a chance of succeeding (International Network of Privacy Law Professionals, 2022).

US tech giants are also not immune from class actions, and the possibility of evading a lawsuit in case of massive data-protection relation issues is relatively low. For example, video conferencing platform *Zoom* faced a class action for allegedly sharing users' data without their consent and providing false information about their software being end-to-end encrypted. *Inc. Privacy Litigation* sued *Zoom* claiming that such alleged conduct violated California state and federal laws. *Zoom* denies these allegations of any liability whatsoever. However, the parties agreed to the settlement. The court has decided that everyone who fits the set description is a settlement class member and can submit a claim form and receive payment. *Zoom* has agreed to pay 85 million dollars to settle the action (Zoom Meetings Class Action, 2022). The same situation happened with the video-sharing app *TikTok* which faced a lawsuit for using and

collecting users' data in connection with their use of the app without the proper notice or consent, a violation of state and federal law. *TikTok* has agreed to pay 92 million dollars to eligible claimants to settle the action (TikTok Data Privacy Settlement, 2022).

Recent case law confirmed difficulties faced by privacy class actions brought in the US. The US Supreme Court judgment in *TransUnion LLC v. Ramirez* case (TransUnion LLC v. Ramirez, 2021) confirmed that there is no standing without concrete harm in federal court. The issue stemmed from the FCRA, which mandates that credit reporting agencies follow reasonable processes to ensure that customer records are as accurate as possible. According to the FCRA, any individual who willfully fails to comply with the rules "is liable to that customer" for damages. Due to database errors, *TransUnion* has wrongly identified thousands of law-abiding Americans on the government's list of terrorists, drug traffickers, and serious criminals in their credit reports which made (or could have made) obtaining financial services impossible or very hard to achieve. In this case, the court held that only 30 per cent of the class action members experienced an actual injury from the errors. The remaining 70 per cent lacked standing because the mere presence of inaccuracy in an internal data file, if it was not disclosed to a third party, caused no concrete harm. As a result, the US Supreme Court remanded the case, stating that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm."

Dempsey argues that, in reality, the *TransUnion* case leaves a more complex picture. For example, some federal courts have found ways to avoid *TransUnion's* holding and read the judgment narrowly to still find standing for future harm. In reality, ransomware does not harm customers. If the threat of future harm is ever enough, there must be credible allegations that the data obtained will almost certainly be used for identity theft or other forms of fraud. Short of alleging that at least some of the victims' data has already been misused, the best way to do so is to claim that the attack was carried out by criminals looking to get personal data that might be used for identity theft or other forms of fraud. That might not be possible in a typical ransomware attack when the data is taken and held for ransom, but the thieves do not do anything else with it (Dempsey, 2022).

There are certain differences between the litigation cultures in Europe and the US. While there has yet to be a wave of GDPR-related class actions in Europe, the long-tail of these kinds of cases makes it impossible to establish if this is because they do not exist or because they are still making their way through the system. However, the risks of facing a class action are

relatively low in the data protection field due to the nature of the activity that could cause harm. Courts both – in the EU and US – put forward a general tendency that future harm that may occur as a result of a violation of data protection is not enough, and incurred harms shall usually be tangible. Having this in mind, the data protection field under Shavell's determinants does not necessarily prefer regulation to liability as risks of facing class actions that could exceed the fine are relatively low because courts tend to critically evaluate harm under data protection regimes.

(4) Administrative costs. Understanding administrative costs is crucial for estimating efficiency and social preference for the EU or US data protection models. The cost of the liability system must be broadly defined to include the time, effort, legal expenses borne by private parties in the course of litigation or settlements and public expenses for trials. Correspondingly, the administrative costs of regulation include the expense of maintaining state institutions performing regulatory functions and the private costs for compliance. The main difference is that, unlike under liability, administrative costs are incurred under regulation regardless of whether or not harm is caused.

Litigation costs in the EU and US differ significantly according to the International Comparisons of Litigation Costs report by *NERA Economic Consulting* (US Chamber Institute for Legal Reform, 2013). Under this report, the US has the highest liability costs as a percentage of the gross domestic product of the countries surveyed, with liability costs at 2.6 times the average level of the Eurozone economies. In addition, US liability costs are four times higher than those of the least costly European countries in the performed study – Belgium, the Netherlands and Portugal. Considering this, it is fair to admit that the EU seems to be a more favourable jurisdiction under litigation costs in the data protection field. However, as litigation costs depend on a number of factors outside of the scope of this thesis, the further analysis focuses on the administrative costs of the data protection regulation models.

As indicated in the background paper by Chander et al., "the cost for complying with privacy laws varies dramatically – from the baker managing a relatively small database of her regular customers' orders to the 1,000-person company supplying information services to a variety of clients across multiple jurisdictions" (Chander et al., 2021, p. 9). In the background paper, the authors summarise a number of studies regarding the costs of compliance with data protection frameworks in the EU and US. Their principal findings are listed below (Chander et al., 2021, p. 10).

Average yearly GDPR compliance expenses vary greatly based on the size and industry of the company, types of activities, geography, perceived risks, risk tolerance and other criteria. The annual estimates for major corporations are regularly in the millions of dollars (Chander et al., 2021, p. 11). Management services, personnel, and technologies continue to receive the greatest amount of funding (Chander et al., 2021, p. 14). Hiring privacy compliance personnel accounts for a significant portion of the expenses (between 20 and 50 per cent, depending on the research). Technology also accounts for a considerable percentage of GDPR compliance costs (between 12 and 17 per cent, depending on the study). Another 19 to 24 per cent, depending on the research, went to outside consultants and attorneys. Despite these investments, most respondents said their privacy budget was insufficient to satisfy their data protection obligations under the GDPR (Chander et al., 2021, p. 12). Salaries for privacy compliance professionals represent a significant part of privacy-related costs (Chander et al., 2021, p. 15). Studies suggest many organisations have followed the GDPR's encouragement to appoint a DPO even when not required (Chander et al., 2021, p. 18).

Compliance with US privacy legislation has a wide range of estimates, although it is typically lower than compliance with the GDPR (Chander et al., 2021, p. 10). According to studies conducted over the last two decades, the health industry spends billions of dollars on HIPAA compliance measures (Chander et al., 2021, p. 21). Compliance with the COPPA appears to be less costly than those associated with HIPAA or GLBA (Chander et al., 2021, p. 24). Instead of taking steps to comply with COPPA, some businesses have tried to avoid it entirely by eliminating minors under the age of 13 from their customer base (Chander et al., 2021, p. 25).

In addition to compliance costs, regulation enforcement costs also have to be considered. For example, on average, the then-28 European Union member states allocated 12.1 million euros to their Supervisory Authorities in 2020. Each EU Member State is required under the GDPR to establish Supervisory Authorities with adequate financial resources to operate. Supervisory Authorities are responsible for enforcing the GDPR, raising awareness, providing guidelines, responding to complaints, and conducting investigations. Dissatisfaction regarding the insufficient level of resourcing originates from a combination of the following: (1) significant increases in data privacy complaints, particularly those involving large tech companies or cross-border elements, (2) the complex system in which cross-border complaints are handled, and (3) a lack of resources to match complaint growth (Chander et al., 2021, p.

28). For regulators, even individual cases might be highly costly. For example, the ICO's investigation into *Cambridge Analytica* cost 2.4 million pounds and took more than three years (Chander et al., 2021, p. 32).

Enforcement costs differ in the US as no single Supervisory Authority exists. Instead, multiple federal agencies enforce separate privacy laws. The HIPAA is primarily enforced by the Department of Health and Human Services' Office for Civil Rights. The GLBA is administered in the financial industry by a number of banks, other authorities and the FTC. The US federal government independently funds each of these regulators, so there is no need to assign specific funds for overseeing the enforcement of federal sectoral privacy laws (Chander et al., 2021, p. 34).

The background paper of Chander et al. shows that the amount of incurred administrative costs favours *ex-post* liability to *ex-ante* regulation as administrative costs under compliance are always incurred while under liability incurred only when the harm is done. Furthermore, compared to the EU, the US chosen sectoral approach creates less overall administrative costs in terms of compliance; however, for actors in specific sectors (e.g. healthcare or finance), these costs are significantly higher than for actors in other fields in the US. Enforcement costs in the EU also supersede the costs in the US due to mandatory funding for Supervisory Authorities and excessive workload due to complaints and investigations under the GDPR.

The author concludes that Shavell's provided model of preference for *ex-ante* regulation and *ex-post* liability is applicable to compare the EU and US chosen data protection frameworks. However, following Shavell's provided conclusions, the four determinants may not be applied blindly and have to be adjusted for each legal issue to benefit the evaluation of social preference. In terms of this research, the author adjusted the general contents of Shavell's determinants and compared how each of them is reflected in the EU and US data protection regulation models.

The original model provides that differential knowledge and administrative costs favour *ex-post* liability while an incapability to pay for the harm done and the possibility to escape suit favour *ex-ante* regulation. In practice, differential knowledge in the data protection field is better addressed in the US as it is chosen to leave the general approach to data regulation for the self-regulation of organisations, except for the cases of sectoral federal legislation. At the same time, the EU's approach may be considered to result in more rigorous regulation than desired in the market and not necessarily ensure individuals' protection most efficiently.

Administrative costs are proven to be way higher in cases of adopted regulation and way higher in the EU than in the US because organisations are obliged to comply with the number of the GDPR requirements to avoid fines imposable by the EU Supervisory Authorities.

Determinants of the inability to pay for the harm done and the possibility to escape suit are not as straightforward in the data protection field. This is primarily related to the challenges of identifying the incurred harm in case of data protection violations. First, harm caused by data breaches is easy to define only in cases where it results in financial losses or similar situations. Second, there is still a dispute about whether harm is possible where no data breach occurs, but the organisation infringes the legislative requirements. Having this in mind, the incapability to pay for the harm done and the possibility to escape a lawsuit do not favour regulation as strongly as Shavell indicated because the threat of liability is not considered very significant. However, in this context, the EU chosen approach greatly differs from the one chosen in the US. The EU has a strict fine and enforcement framework that forces organisations to consider more the possibility of being fined than the possibility of being sued. As for the US, this jurisdiction does not possess a well-established framework of data privacy rules enforcement; therefore, the litigation culture still leaves more room for *ex-ante* regulation preference.

This research proves that theoretical models of economic analysis of law may provide the beneficial guidelines to determine social preference for the chosen approach to data protection in terms of efficiency. However, it is evident that no policy framework prefers one approach, *ex-ante* regulation or *ex-post* liability. The possibility of achieving the socially optimal standard can be reached only with the combination of both approaches. Due to its nature, data protection regulation differs in both analysed jurisdictions mainly because the EU has chosen a clear preference for *ex-ante* regulation with the non-comprehensive possibility to claim for damages which is also supported by the practice of enforcement of Supervisory Authorities. In general, the US data protection framework leaves for organisations to decide on their standard business practices and consumers to bring actions to claim damages rather than regulating, except for certain cases of sectoral federal legislation or comprehensive legislation in separate states. Shifting from the conventional human rights perspective and applying Shavell's model, the socially optimal approach in the data protection field would be closer to the US model mainly due to fewer social costs incurred by companies and a non-defined concept of harm that data protection violations could cause.

CONCLUSIONS

1. The GDPR is the cornerstone of the EU data protection framework, which emphasizes the human rights approach and puts the data subject at the centre of the EU data protection regulation model. The GDPR contains a comprehensive set of rules varying from the list of data subjects' rights to the uniformed administrative fines mechanism. Some of the disputed GDPR features include its extraterritorial applicability and cross-border data transfer requirements. The EU has a well-established network of national Supervisory Authorities that take a proactive approach toward strict GDPR enforcement. The GDPR is often considered the global "golden" standard for privacy rights protection. However, the regulation does not escape criticism for being an excessive burden, especially to small and medium enterprises, and not reflecting the needs of businesses and consumers that willingly provide their data to receive services or purchase goods.
2. The US data protection framework is considered a polar opposite of the one chosen by the EU. Instead of having one comprehensive data protection legislation at a federal level, the US has adopted a number of sectoral laws that concern only the specific type of data or specific data actors. The US also does not have one Supervisory Authority – *de facto,* part of this power is granted to the FTC. The US's fundamental approach to data protection is that companies are the ones who know better how to protect consumers' data as they are the ones to provide them with goods and services. Organisations welcome the US chosen approach as it generally permits the broad use of personal data; however, privacy activists challenge this approach by putting forward the human rights perspective. Therefore, companies more often choose privacy self-regulation as a matter of brand reputation. In recent years, discussions on the adoption of broad federal privacy laws have been as active as ever, especially with the rise of the adoption of state-level data protection legislation.
3. Repeated clashes between EU and US jurisdictions concerning cross-border data transfers suggest the need to compare the EU and US data protection regulation models. While it is generally undisputed that looking from the human rights perspective, the GDPR is the standard to be achieved; this research proves a different outcome when comparing the EU and US data protection regulation models using the lens of economic analysis of law. This thesis relies on S. Shavell's model, which defines a social preference for *ex-ante* regulation and *ex-post* liability. Shavell's distinguished determinants can also be applied to the data protection field and help compare the EU and the US approaches in terms of social

preference. Application of these determinants indicated that society should generally prefer the US chosen approach, providing more economic efficiency. However, none of the approaches – *ex-ante* regulation and *ex-post* liability – can be isolated from the other; therefore, both – EU and US – chosen data protection regulation frameworks aim to balance these two approaches to achieve the socially optimal result.

LIST OF SOURCES

STATUTORY LEGISLATION

European Union Statutory Legislation

1. 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). Official Journal L 119, 4.5.2016, p. 1–88
2. Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016). Official Journal L 119, 4.5.2016, p. 89–131
3. Charter of Fundamental Rights of the European Union (2012). Official Journal C 326, 26.10.2012, p. 391–407
4. Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002). Official Journal L 201, 31.7.2002, p. 37–47
5. 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). Official Journal L 281, 23/11/1995 P. 0031 - 0050
6. Single European Act (1986). Official Journal L 169, 29.6.1987, p. 1–28

United States Statutory Legislation

1. California Consumer Privacy Act (2018), California Civil Code, Section 1798.100
2. USA Patriot Act (2001), Pub. L. No. 107-56, 115 Stat. 272
3. Gramm-Leach-Bliley Act (1999), Pub. L. No. 106-102, S. 900
4. Children's Online Privacy Protection Act (1998), Pub. L. 105–277

5. Health Insurance Portability and Accountability Act (1996), Pub. L. No. 104-191, S. 264
6. Video Privacy Protection Act (1988), 18 U.S.C. § 2710
7. Electronic Communications Privacy Act (1986), 18 U.S.C. §§ 2510-2523
8. Computer Fraud and Abuse Act (1986), Pub. L. No. 99-474, 100 Stat. 1213
9. Foreign Intelligence Surveillance Act (1978), Pub. L. No. 95-511, 92 Stat. 1783, p. 1783 - 1798
10. Family Educational Rights and Privacy Act (1974), 20 U.S.C. § 1232g; 34 CFR Part 99
11. Fair Credit Reporting Act (1970), Pub. Law No. 91-508
12. Federal Trade Commission Act (1914), 15 U.S.C. §§ 41-58

Other Legislation

13. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), ETS No. 108
14. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
15. European Convention of Human Rights (1950)

SPECIAL LITERATURE

16. Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D. and Yu, I. (2021). *Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation*. SSRN Electronic Journal.
17. Citron, D. and Solove, D. (2022). *Privacy Harms*. GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, Boston University Law Review, Vol. 102.
18. Frankenreiter, J. (2021). *The Missing "California Effect" in Data Privacy Law*. SSRN Electronic Journal.
19. Goldsmith, J. & Wu, T. (2006). *Who controls the internet? Illusions of a Borderless World*. Oxford University Press.
20. Greenleaf, G. (2013). *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*. SSRN Electronic Journal.

21. Heiman, Matthew R. A. (2020). *The GDPR and the Consequences of Big Regulatio*n. Pepperdine Law Review, vol. 47, no. 4, p. 945-954.
22. Hilliard, E. (2009), *The GDPR: A Restrospective and Prospective Look at the First Two Years*. Berkeley Technology Law Journal [Vol. 35:1245 2021].
23. Kessler, J. (2019). *Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource*". Southern California Law Review 93, no. 1, p. 99-128.
24. Layton, R. (2019). *The 10 Problems of the GDPR. The US can learn from the EU's mistakes and leapfrog its policy*. Statement before the Senate Judiciary Committee On the General Data Protection Regulation and California Consumer Privacy Act: Optins, Consumer Control, and the Impact on Competition and Innovation, American Enterprise Institute.
25. Maldoff, G., and Omer T. (2019). *Born in the USA: The GDPR and the Case for Transatlantic Privacy Convergence*. Colorado Technology Law Journal, vol. 17, no. 2, p. 295-310.
26. Newman, M., Swift, M., and Gladicheva, V. (2020). *GDPR and CCPA Start to Bare Teeth as Privacy Protection Goes Global*. Business Law International Vol 21.
27. Romanosky, S. and Acquisti, A (2009). *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*. Berkeley Technology Law Journal, vol. 24, no. 3, p. 1061-1102.
28. Ryngaert, C., and Mistale T. (2020). *The GDPR as Global Data Protection Regulation*. AJIL Unbound, 114, 2020, p. 5-9.
29. Schwartz, P. and Peifer, K. (2017). *Transatlantic Data Privacy*. Georgetown Law Journal 115, UC Berkeley Public Law Research Paper.
30. Shavell, S. (1984). *Liability for Harm versus Regulation of Safety*. The Journal of Legal Studies, 13(2), p. 357-374.
31. Wilson, C. (2021). *Exploring Options Overcoming Barriers to Comprehensive Federal Privacy Legislation United States of America Federal Trade Commission*. Available at: https://www.ftc.gov/system/files/documents/public_statements/1596632/wilsonspeechovercomingbarriersprivacy.pdf [Accessed 17 Mar. 2022].

CASE LAW

Case Law of Court of Justice of the European Union

32. *Shrems II* [CJEU], C-311/18, [2020-07-16], ECLI:EU:C:2020:559
33. *Rīgas satiksme* [CJEU], C-13/16, [2017-05-04], ECLI:EU:C:2017:336
34. *Manni* [CJEU], C-398/15, [2017-03-09], ECLI:EU:C:2017:197
35. *Breyer* [CJEU], C-582/14, [2016-10-19], ECLI:EU:C:2016:779
36. *Google Spain and Google* [CJEU], C-131/12, [2014-05-13], ECLI:EU:C:2014:317
37. *Bodil Lindqvist* [CJEU], C-101/01, [2003-11-06], ECLI:EU:C:2003:596
38. *Commission v. Hungary* [CJEU], C-288/12, [2014-04-08], ECLI:EU:C:2014:237
39. *Commission v. Austria* [CJEU], C-614/10, [2012-10-16], ECLI:EU:C:2012:631
40. *Commission v. Germany* [CJEU], C-518/07, [2010-03-09], ECLI:EU:C:2010:125

Case Law of European Court of Human Rights

41. *Antović and Mirković v. Montenegro* [ECtHR], No. 70838/13, [2017-11-28], ECLI:CE:ECHR:2017:1128JUD007083813
42. *Uzun v. Germany* [ECtHR], No. 35623/05, [2010-09-02], ECLI:CE:ECHR:2010:0902JUD003562305
43. *S. and Marper v. the United Kingdom* [ECtHR], No. 30562/04 and 30566/04, [2008-12-04], ECLI:CE:ECHR:2008:1204JUD003056204
44. *Niemietz v. Germany* [ECtHR], No. 13710/88, [1992-12-16], ECLI:CE:ECHR:1992:1216JUD001371088
45. *Leander v. Sweden* [1987], No. 9248/81, [1987-03-26], ECLI:CE:ECHR:1987:0326JUD000924881

Other Case Law

46. *TransUnion LLC v. Ramirez* [Supreme Court of the United States], No. 20–297, 2021-06-25
47. *Lloyd v. Google LLC* [UK Supreme Court] [2021-11-10]
48. *ICOMOS* case [Judgment of the Vilnius Regional Administrative Court], No. EI2-1249-789/2020, [2020-04-08]

OTHER SOURCES

49. Cambridge Dictionary (2019). *Cambridge English Dictionary*. [online] Cambridge.org. [online] Available at:

https://dictionary.cambridge.org/dictionary/english/compliance. [Accessed 22 April 2022]

50. Canadian Marketing Association (CMA) (2022). *Privacy Law Pitfalls. Lessons Learned from the European Union*.
51. CNIL. *Lobbying file: penalty of 400,000 euros against MONSANTO*. [online] Available at: https://www.cnil.fr/fr/node/121570 [Accessed 10 Mar. 2022].
52. Congressional Research Service (2019). *Data Protection Law: An Overview*. [online] Available at: https://sgp.fas.org/crs/misc/R45631.pdf [Accessed 23 April 2022].
53. Court of Justice of the European Union, Research and Documentation Directorate (2020). *Protection of Personal Data, Fact Sheet*.
54. Data Guidance. *Italy Garante Fines Deliveroo for Unlawful Processing*. [online] Available at: https://www.dataguidance.com/news/italy-garante-fines-deliveroo-%E2%82%AC25m-unlawful-processing [Accessed 10 Mar. 2022].
55. Dempsey, J. (2022). *US courts mixed on letting data breach suits go forward*. [online] Iapp.org. Available at: https://iapp.org/news/a/u-s-courts-mixed-on-letting-data-breach-suits-go-forward/ [Accessed 18 March 2022].
56. DLA Piper (2022). *DLA Piper Global Data Protection Laws of the World - World Map*. [online] Available at: https://www.dlapiperdataprotection.com/ [Accessed 12 Mar. 2022].
57. EDPB. *Lithuanian DPA: Fine Imposed on a Sports Club for Infringements of the GDPR in Processing of Fingerprints of the Customers and Employees*. [online] Available at: https://edpb.europa.eu/news/national-news/2021/lithuanian-dpa-fine-imposed-sports-club-infringements-gdpr-processing_en [Accessed 10 Mar. 2022]
58. Federal Trade Commission. *Privacy and Security Enforcement*. [online] Available at: https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement [Accessed 16 Mar. 2022].
59. Forbes. *Booking.com Hit With €475,000 GDPR Fine for Late Reporting of Data Breach*. [online] Available at: https://www.forbes.com/sites/carlypage/2021/04/02/bookingcom-hit-with-475000-gdpr-fine-for-late-reporting-of-data-breach/?sh=1ecb1f3552bd [Accessed 10 Mar. 2022].

60. GDPR Enforcement Tracker. *List of GDPR fines*. [online] Available at: https://www.enforcementtracker.com/?insights.
61. Global Privacy & Security Compliance Law Blog (2021). *Austrian Court Submits Questions on GDPR Civil Damages Claims to CJEU*. [online] Available at: https://www.globalprivacyblog.com/gdpr/austrian-court-submits-questions-on-gdpr-civil-damages-claims-to-cjeu/ [Accessed 20 April 2022].
62. IAPP (2022). *US State Comprehensive Privacy Law Comparison*. [online] Available at: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [Accessed 15 April 2022].
63. ICO. *ICO fines British Airways £20m for data breach affecting more than 400,000 customers*. [online] Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers [Accessed 15 April 2022].
64. International Network of Privacy Law Professionals. *Dutch GDPR class action against Oracle and Salesforce declared inadmissible*. [online] Available at: https://inplp.com/latest-news/article/dutch-gdpr-class-action-against-oracle-and-salesforce-declared-inadmissible/ [Accessed 27 Mar. 2022].
65. Loyens, Damsté, L.-M.S., Lucassen, K., Bosselaar, M. and Orlić, N. (2021). *Privacy, GDPR and class actions: recent developments in the Netherlands*. [online] Lexology. Available at: https://www.lexology.com/library/detail.aspx?g=940ef820-c0ec-4ea3-9d38-323fa33f5909 [Accessed 27 Mar. 2022].
66. Perrin, A (2020). *Half of Americans have decided not to use a product or service because of privacy concerns*. [online] Pew Research Center. Available at: https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/ [Accessed 25 Mar. 2022].
67. Rainie, L. and Maeve Duggan (2016). *Privacy and Information Sharing*. [online] Pew Research Center: Internet, Science & Tech. [online] Available at: https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/ [Accessed 25 Mar. 2022].
68. The White House. *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*. [online] Available at:

https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ [Accessed 14 April 2022].

69. TikTok Data Privacy Settlement. *Musical.ly and/or TikTok Class Action*. [online] Available at: https://www.tiktokdataprivacysettlement.com/ [Accessed 27 Mar. 2022]
70. Zoom Meetings Class Action. *Zoom Video Communications Litigation*. [online] Available at: https://www.zoommeetingsclassaction.com/ [Accessed 27 Mar. 2022]

SUMMARY

Comparing Data Protection Regulation Models of the EU and the US: Which One Is More Preferred by the Society?

Raminta Matulytė

This master thesis analyses and compares the data protection regulation models in the European Union and the United States. The comparison of these models is performed by indicating their main features and assessing their social costs and efficiency through the lens of economic analysis of law.

The EU's model is based on the General Data Protection Regulation (GDPR), which contains a comprehensive set of rules varying from the data subjects' rights to administrative fines mechanism. The well-established network of national supervisory authorities and their proactive action toward the GDPR enforcement makes the GDPR a working tool and not a dead letter. However, while it is undisputed that the GDPR is the highest standard to be achieved from the human rights perspective, it does not escape criticism for being an excessive burden. The US chosen approach is the opposite of the EU's comprehensive data protection regulation. Instead of having one comprehensive data protection legislation at a federal level, the US has adopted a number of sectoral laws that concern only the specific type of data or specific data actors. However, in recent years, discussions on the adoption of broad privacy laws are as active as ever.

The importance of comparing the EU and US data protection regulation models results from the repeated clashes between these jurisdictions concerning cross-border data transfers. One way to look at these models is through the economic analysis of law. This master thesis relies on S. Shavell's model establishing determinants that help define the social preference for each data protection regulation model in terms of *ex-ante* regulation and *ex-post* liability. It is almost undisputed that looking closely from the human rights perspective, society will prefer the GDPR. However, this work proves that looking strictly from the economic perspective, the society shall prefer more the US approach because of its economic efficiency and balance of data actors' interests.