UNIWERSYTET WROCŁAWSKI

Wydział Prawa, Administracji i Ekonomii

Katedra Doktryn Politycznych i Prawnych

Małgorzata Sikora

Privacy protection through the right to be forgotten and data transfer rights under General Data Protection Regulation - implementation challenges in online-operating software.

Praca doktorska

Promotor pracy: dr hab. Łukasz Machaj prof. UWr

Promotor pomocniczy: dr Krzysztof Wygoda

Wrocław, 2023

Table of contents

Introduction

We are living in an era where data has become one of the most valuable resources, while at the same time, we are observing a moment when the law struggles with one of its most powerful challenges, namely, extreme technological growth. As the world changes and science and social contexts evolve, the law faces new challenges that were not foreseeable in the past. As one of the great thinkers, Roscoe Pound, put it, *The law must be stable, but it must not stand still*. This quote effectively summarizes certain challenges facing lawmakers set out and described in this thesis, namely, how best to interpret and understand privacy within the context of currently evolving technological growth and current use of data what implies the change in understanding of privacy, its relationship with data protection, and lastly, what technological challenges protection of privacy brings on the grounds of current jurisprudence and the rise of the General Data Protection Regulation.

Before one dives into the scope of data protection as a right, for purposes of context it would be important to first lay the groundwork of current data processing laws. It is widely recognized that data protection laws and definitions of processing activities arise from the right to privacy, and even though data protection laws and right to privacy shall not be used interchangeably, the underpinning values of data processing rights stand apart from the protection of privacy as such. In the online world, the will to shape the information about oneself and the aspiration to be able to manage one's image and private life information emerge from currently known laws on the processing of personal data. As such, at the beginning of this thesis, it is important to clarify the meaning of privacy from the perspective of doctrinal foundations. Chapter I focuses on the question of the meaning of privacy and how its meaning has evolved through the ages of legal doctrine development. The right to protect privacy, especially from the perspective of data processing law, emerged from the idea of why privacy should be protected at all and in the first place. The right to privacy is a fundamental human right that is recognized in various national and international laws and agreements. It also functions as a customary law. Right to privacy is the right to be free from unwanted intrusions or disturbances and to have control over one's personal information and how it is collected, used, and shared. Data protection is a related concept that refers to the measures and practices that are put into place to protect personal data from unauthorized access, use, or disclosure. It is a way of safeguarding an individual’s right to privacy by ensuring that their personal information is collected, used, and

shared in a responsible and transparent manner. At the moment, data protection and privacy laws become so globally recognized that both concepts are included and protected in almost every jurisdiction around the world.

As a consequence, the right to privacy and data protection are closely related to one another because the right to privacy is concerned with protecting individuals' personal information and their right to control how it is used, while data protection is a means of safeguarding this right by establishing rules and standards for the collection, use, and sharing of personal data. Right to privacy is qualified as a human right and further its understanding shall be viewed not inly through the perspective of legal rights but also moral underpinnings. The right to privacy itself, as an core value of data protection, is an essential aspect of human dignity and autonomy. It allows individuals to control their own lives, make their own choices, and express themselves freely without interference or coercion. Such trust in the protection of individual rights enables individuals to freely execute their rights within society. For example, protecting the right to privacy helps to promote trust, security, and confidence in society. When individuals feel that their privacy is respected and protected, they are more likely to feel secure and to share personal information and ideas, which, in a long-term perspective, affect the functioning of other rights such as, for example, freedom of speech. This can foster a sense of community and facilitate the free exchange of ideas and information, which is essential for a healthy and vibrant society. Moreover, protecting the right to privacy can also help to prevent abuses of power and ensure that individuals are treated with dignity and respect. Without the protection of privacy, individuals may be subject to invasions of their personal space and intrusions into their private lives, which can lead to feelings of vulnerability and powerlessness. Overall, protecting the right to privacy is essential for promoting human dignity, autonomy, trust, security, and confidence in society.

On the international level, the right to privacy is protected by several human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). These instruments recognize the right to privacy as a fundamental human right and provide protections against interference with an individual's privacy, including their home, family, correspondence, and personal data. At the national level, the right to privacy is protected by constitutional and statutory laws in many countries. In the United States, for example, the Fourth Amendment to the Constitution protects individuals from unreasonable searches and seizures by the United States government and further requires

the United States government to have a warrant before it can conduct a search or seizure[1]. The Privacy Act of 1974 also establishes rules for the collection, use, and disclosure of personal information by United States federal agencies.

In addition to these legal protections, there are also various regulatory frameworks and self-regulatory codes of practice across almost every jurisdiction including EU and USA that seek to protect the privacy of individuals in relation to the collection, use, and storage of personal data by businesses and other organizations. These include data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. Overall, the legal protection of the right to privacy is an important aspect of ensuring that individuals' privacy is respected and upheld in various contexts.

In the European Union, data protection is currently regulated by the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018. The GDPR applies to all organizations, including businesses, that process personal data of individuals in the EU, regardless of whether the organization is based inside or outside the EU, and has been the most powerful and recognized act that has come into force in modern legal history. The GDPR establishes a set of principles for the processing of personal data, including: lawfulness, fairness, transparency, data minimization, accuracy, storage limitation, integrity, and confidentiality. The GDPR also gives individuals certain rights in relation to their personal data, including the right to access their personal data, the right to rectification, the right to erasure (also known as the *right to be forgotten*), the right to restrict processing, and the right to data portability. In addition to the GDPR, there are also several other EU laws and regulations that relate to data protection, including the ePrivacy Directive (2002/58/EC) and the Network and Information Systems Directive (2016/1148/EU). These laws and regulations provide additional protections in relation to the processing of personal data in specific contexts, such as the use of cookies and the security of networks and information systems.

[1] U.S. Constitution, Amendment IV: *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

GDPR has been the most influential at least with respect to the aforementioned statues, but at the same time, it has brought a number of questions and uncertainty. As a regulation, GDPR functions at a certain level of abstraction. Chapter II of this thesis focuses on the *per se* rights expressed in the GDPR as a whole and their relationship with expectations towards the data controller as being the main actor that controls data processing. The main aim of Chapter II is to seek proportionality and define expectations towards the data controller. Chapter I of this thesis highlights the reliability of law and the background for privacy protection while at the same time questioning whether a law with no clarity to rely on or defined consequences qualifies as law. The concept of the *reliability of law* refers to the degree to which a legal system can be relied upon to provide consistent, predictable, and fair outcomes. A legal system that is reliable is one in which individuals can have confidence that the law will be applied consistently and fairly, and that they can rely on the legal system to resolve disputes and protect their rights. There are various factors that can impact the reliability of a legal system, including the quality of the laws themselves, the independence and impartiality of the judiciary, the ability of the legal system to adapt to changing circumstances, and the transparency and accountability of the legal process.

In the early 20th century, legal scholars Roscoe Pound and Oliver Wendell Holmes Jr. raised questions about the quality of law and the reliability of the legal system[2]. Pound argued that the legal system had become too complex and unmanageable and that it was failing to meet the needs of society. Holmes, on the other hand, argued that the law should be understood as a *prediction of the courts* and that the primary function of the legal system was to provide a predictable and stable framework for resolving disputes[3]. Overall, the reliability of the law and

[2] In "The Spirit of the Common Law" (1921), R. Pound stated that *The great criticism of the legal order of the present is that it is too complex, too technical, too unadapted to the needs of society. It is said that the law is so complicated that only lawyers can understand it, that it is too expensive for ordinary people to use, that it is too slow in meeting the needs of a rapidly changing world*. In this quote Pound argues that the law is too technical and difficult to understand for non-lawyers, and that it is too slow to adapt to changing circumstances. This complexity and lack of adaptability, according to Pound, constitutes the major criticisms of the legal system and contribute to its inability to effectively serve the needs of society.

[3] Oliver Wendell Holmes Jr.'s at his work titled *The Path of the Law* (1897) states *The prophecies of what the courts will do in fact, and nothing more pretentious, are what I mean by the law*. By such statement, Holmes is expressing his view that the law should be understood as a *prediction of what the courts will do*. Holmes argues that the primary function of the legal system is to provide a predictable and stable framework for resolving

the quality of the legal system are important considerations in ensuring that the law serves the needs of society and protects the rights and interests of individuals.

The main aim of such questioning is to highlight the fact that GDPR, as a legal act, places a number of requirements and pushes the vast majority of responsibilities and accountability towards the data controller. The act itself fails to respond to the factual situation of data controllers, who are mostly dependent on market monopolists such as Google, Atlassian, or Meta delivering the solutions used worldwide with hardly any alternatives. One of the technological challenges of implementing the GDPR is the need to ensure that personal data is processed in a secure and confidential manner. This includes implementing appropriate technical and organizational measures to protect personal data from unauthorized access, use, disclosure, or destruction. Another technological challenge of the GDPR is the requirement to implement systems and processes to enable organizations to comply with the data subject rights provisions of the GDPR. These provisions give individuals certain rights in relation to their personal data, including the right to access their personal data, the right to rectification, the right to erasure (also known as the *right to be forgotten*), the right to restrict processing, and the right to data portability. Implementing systems and processes to enable organizations to respond to these rights can be complex and require significant investments in technology. A further technological challenge of the GDPR is the need to ensure that personal data is processed in a manner that is consistent with the principles of data protection by design and data protection by default. This requires organizations to consider data protection issues at all stages of the data processing lifecycle, from the design of systems and processes to the collection and use of personal data. To conclude, implementing the GDPR involves a number of technological challenges that require organizations to invest in new systems and processes, and to ensure that they have the necessary technical and organizational measures in place to protect personal data and comply with the requirements of the GDPR. At the same time, one may currently observe how those technological challenges are further narrowed down and escalated to an even more orthodox interpretation by the Court of Justice of the European Union. On the one hand, EU Regulation provides a very narrow scope of support for controllers

disputes, and that the law itself should not be seen as a set of moral or ethical principles, but rather as a means of predicting the outcomes of legal disputes. Holmes's view of the law as a prediction of what the courts will do reflects his belief that the primary role of the legal system is to provide a stable and predictable framework for resolving disputes, rather than to serve as a source of moral or ethical guidance.

while at the same time assigning them all responsibility[4]. On the other hand, decisions of the CJEU in the Schrems cases are further narrowing down the possibility of data transfer and placing a responsibility on data controllers to exclude the access of foreign intelligence agencies to data transferred outside of the EU[5]. In the most foreseeable scenarios, the extensiveness of protection towards the right to privacy may seem justified nevertheless, once we take into consideration the balancing approach towards data controller's rights and data subjects rights the perspective changes. The fact that the GDPR went far with requirements towards data processing and further that the actions of the CJEU made such interpretation even more extreme leads us to the situation where reality and social need stand apart from the current interpretation of law and that the responsibility for such actions is aggregated on data controllers. In the last Chapter of this thesis, I summarize the difficulty arising from the orthodox interpretation of the GDPR that goes beyond the currently known scope and that further places the data controllers, also named as the *bad guy* from Holmes theories, in the disadvantageous position of a lack of reliability in law. It further questions the logical grounds that stand as the backbone of Schrems judgments as aspiring to regulate the scope of law that is outside of EU regulation and that is further directed towards the exempted matter of state security. One criticism of the Schrems judgment is that it has created uncertainty and confusion for organizations that rely on the transfer of personal data between the EU and the US. The invalidation of the EU-US Privacy Shield framework has left many organizations without a clear legal basis for transferring personal data to the US, and they have had to resort to alternative methods, such as standard contractual clauses (SCCs), to transfer personal data. Another criticism of the Schrems judgment is that it has raised questions about the ability of

[4] All risk-based assessments as well as transfer impact assessments as offered by the GDPR are based on assumptions that shall be done individually by data controllers. A DPIA may be based on assumptions about the likelihood and potential impact of risks to the rights and freedoms of individuals. These assumptions should be based on the best available information and should be regularly reviewed and updated as necessary. This level of certainty is the maximum available to data controllers to ground their processing decisions that are attached to a massive financial responsibility GDPR) provides for a number of different types of penalties that can be imposed on organizations that infringe the provisions of the GDPR. Under the GDPR, administrative fines can be imposed on organizations that infringe the provisions of the GDPR. These fines can be up to €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

[5] CJEU, Judgment (Grand Chamber), *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, Case C-311/18, July 2020. ECLI:EU:C:2020:559.

the EU to adequately protect the personal data of its citizens when it is transferred to countries outside the EU. The CJEU found that the US does not provide an adequate level of protection for personal data, and this has led to concerns about the ability of the EU to ensure that personal data is adequately protected when it is transferred to other countries outside the EU.

The main aim of this thesis is to build a bridge of understanding between privacy protection, data processing, and the modern challenges that we are currently facing with the implementation of the GDPR. The right to privacy has been tremendously exposed to the challenges of new technologies. The GDPR came with the answer to address such fears of abuse towards our privacy, but the excessive practical dimension of this law that tends to get fast and hash verification leads one to the question – is GDPR a law that we can be relied upon despite its flaws and lack of predictability?

Chapter I: Right to privacy and processing of personal data

A. Meaning of privacy in the light of doctrinal foundations, the 19th-century case law until today's understanding.

Understanding the right to privacy requires an extensive evaluation of the underpinning values that stand behind the development of such laws. Such a statement may seem very obvious and fitting to every type of law; nevertheless, at the current stage of world development, there are only a few areas of law as exposed to the growth and constantly evolving circumstances as privacy protection. Privacy protection growth or an extension of its scope can be viewed from numerous perspectives: a data subject, a person or entity in charge of information about an individual, or an individual of exceptional value. In a time where data remains the most valuable resource that we have and the shaping of information shared about us is the key goal of many legal acts, understanding privacy laws and their values is a fascinating subject of research. Is there a clear distinction between judicial practice, case law, and doctrine in this regard, and how does legal practice correspond with this constantly growing reality? To understand the rise of the right to privacy, we shall take into account both the philosophy of law and practice as non-distinctive fields. Privacy stands as a reason and further evolves into an underpinning value for data protection, limitations of data processing, and a risk-based approach. Consequently, to arrive at an understanding of the modern challenges of data processing in light of the GDPR, the right starting point would be to define the meaning of privacy, the need for it, and the reason for its protection.

The right to privacy is among the first generation of human rights, and the sphere of privacy in life as a separate legal good is protected in most of modern legal systems. There is no unified meaning of *privacy* neither in the doctrine itself nor in legal documents. Nevertheless, privacy was intuitively considered a valuable element and attribute of humanity. Early literature on privacy helps to distinguish the normative and descriptive character of this term - it can exist as the epitome of an interest or right[6]. The term is often used in ordinary language, but it is also

[6] J. DeCew, *Privacy*, The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (Eds.). Retrieved June 22, 2021 from https://plato.stanford.edu/archives/spr2018/entries/privacy/.

vividly presented in philosophical and legal discussions to denote an individual right belonging to each of us - the right to shape information shared about oneself along with the right to be entitled to know about such sharing. Of course, discussion about privacy is more complex than just a supportive approach. Indeed, in the doctrine, several skeptical and critical accounts of privacy are present and visible. Skepticism in this regard goes as far as to say that there is no right to privacy and there is nothing special about privacy because any interest protected as private can be equally well explained and protected by other interests or rights, most notably rights to property and bodily security[7].

Regardless of what approach we take toward privacy, one element is certain: it remains a vital element of public discussion, and in the light of a growing data exchange that constitutes an element of private information, it will be present and affect our lives. Furthermore, as privacy is strongly related to personal information or information about individuals, big data or data minimization shall place new challenges on this long-standing right and will bring new standards towards the understanding of the extent and context individuals shall or shall not be able to affect information shared about them and information derived about them from their activities[8].

1. Early notions of privacy towards the rise of privacy rights in the XIX century.

The distinction between private and public life dates as far back as Aristotelian times, personified as the public *polis*, and the private or domestic sphere of the family, the *oikos*[9]. The ethically impregnated concept of political practice, paradigmatically formulated by Aristotle, is based on the strict separation of political and economic spheres: the economic differences

[7] The reductionist approach represented by Judith Jarvis Thomson, she claims that privacy is derivative; there is no need to find what is common in the cluster of privacy rights. J. J. Thomson, The right to Privacy. Philosophy & Public Affairs 1975, vol. 4, no. 4, pp. 295-314.

[8] Privacy shall be evaluated and understood in a broader context than just information about individuals. In fact, in the modern understanding of data processing, one should distinguish a situation where a combination of non-personal data becomes personal information due to the correlation between such data. For example, data profiling used in the case of the US election resulted in one of the most historically recognized processes of affecting targeted group choices through the use of information collected about the group on publicly shared social media during online activity (Cambridge Analytica case).

[9] The matter was raised in the famous writing of Aristotle "*Politics*".

between households have no impact on the political participation rights of citizens. The women who belong to the *oikos* and the slaves, who are ruled by a tyrant with power over life and death, are jointly not allowed in the polis. Obviously, this early distinction is in sharp contrast to how private life is understood today, and, as a result, so is the right to have this private right protected. But it demonstrates the long history of guarding what makes up our private sphere of existence. Intuitively, privacy refers to the notion of secrecy and autonomy inside society and is what shields our non-public sphere of existence from any intrusion[10]. Richard A. Posner rightly stated that *the concept of privacy is elusive and ill defined. Much ink has been spilled in trying to clarify its meaning*[11]. He further discusses the economic and social aspects of privacy and the fact that every individual possesses information about themselves or others that is of value to others or of a character that makes sharing such information unbeneficial. On the other hand, disseminating information risks exploiting people through false portrayal[12]. Consequently, it is rightly noted by the past legislators as something that should be under legislative control as freedom from infringement of bodily integrity.

Although the legal concept of privacy originated in Anglo-Saxon law, unlike other institutions, it originated on the American continent. The authors who first used the term *right to privacy* were American lawyers S. D. Warren and L. D. Brandeis. In 1890, they published a groundbreaking article in the Harvard Law Review titled *The right to privacy*. In the article,

[10] J. Hirshleifer, *Privacy: Its Origin, Function, and Future*, The Journal of Legal Studies 1980, vol. 9, no. 4, pp. 649-666.

[11] R. A. Posner, *The Right of Privacy*, Georgia Law Review 1977, vol. 12, p. 393. .

[12] Psychologists and sociologists have pointed out that even in everyday life, people try to manipulate by misrepresenting other people's opinions of them, and as the outcome of this - respect for privacy is somehow a personification of a desire to control others. This idea was discussed by Erving Goffma,n who develops this thought in a book titled *The Presentation of self in everyday life* in which he refers explicitly to *misrepresentation* but uses the term without any pejorative connotation. In this book, Goffman argues that individuals present themselves to others in various social situations in order to create a particular impression or identity. He called this process the *presentation of self*, and he argued that it is a fundamental aspect of social interaction. According to Goffman, the presentation of *self* involves the use of various strategies and tactics, such as language, gestures, and appearance, to create a desired impression on others. He argued that individuals are constantly engaged in this process, both consciously and unconsciously, and that the presentation of self is a crucial aspect of the way that we interact with others in society. Goffman's concept of the presentation of self has had a significant influence on sociological theory and has been widely studied and debated by sociologists and other scholars. It remains an important and influential concept in the field of sociology today.

Warren and Brandeis argued that protection of privacy is a fact and further implies a need for regulation in this area of life based upon the civil law of Torts (tortious interference)[13]. The authors argued, based on civil tort law literature and an analysis of selected U.S. court decisions, that there is a common ground, though not explicitly codified or expressed in *per se* terms, which is the right to privacy for the protection of inviolable characteristics. Gradually, U.S. courts have begun to recognize invasion of privacy as a tort under civil law - distinguishing four types thereof:

- violation of an individual's solitude, private affairs, and family life,
- publication of news ridiculing an individual's private life, hurting feelings or reputation,
- false publication that puts an individual in a false position in the eyes of the public, and
- use of an individual's likeness or name without his or her permission or consent.

According to a well-known paper by S. D. Warren and L. D. Brandeis *[...] the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society*[14]. The authors

[13] Tortious interference is a legal concept that refers to a wrongful act where one party intentionally interferes with another party's contractual or business relationships, causing harm or damage. It occurs when a third party disrupts or prevents the fulfillment of a contract or business arrangement between two other parties, without any lawful justification. Tortious interference can take different forms and further interact with the right to privacy. Tortious interference with contractual relations indirectly protects an individual's right to privacy. When a third party wrongfully interferes with a contract or business relationship, it can potentially expose private and confidential information, leading to a breach of privacy. For example, if an individual discloses confidential information about another person's medical records, thereby causing harm or damage to their contractual or business relationships, it may constitute tortious interference and a violation of privacy rights.

[14] The quote originates from the 1890 US Supreme Court case *S.D. Warren Co. v. Maine Board of Environmental Protection*. In this case, the Court considered the constitutionality of a state law that regulated the disposal of paper mill waste into a river. The Court ultimately held that the law was constitutional and that the state had the authority to regulate the disposal of waste in order to protect public health and the environment. The quote you provided is often referred to as the "Brandeis Brief," as it was written by Louis D. Brandeis, who later became a justice on the Supreme Court. In the quote, Brandeis argues that the principle of protecting the individual in person and in property is a long-standing one that has been recognized by the common law. He also notes that the common law has evolved over time to meet the changing needs of society, and that new rights may be recognized as a result of political, social, and economic changes. Overall, the quote you provided reflects the idea that the protection of

of the article from the Harvard Law Review claimed that the American legal system needed to differentiate the breach of the right to privacy as a distinct tort. The article's writers made a difference between torts and the growth of the protection of individual rights at the outset. It starts first with offenses against our property, as described above in the subchapter 1, being the understanding that individuals can be granted a remote ground for privacy rights recognition. The focus shifted to the right to life and physical integrity after it was realized that humans can own. This final step in the knowledge of individual rights led to the idea of privacy, which gained prominence during the 19th century. The aforementioned publication is remembered as a turning point in the history of the creation of the right to privacy, both in the American legal system and throughout those of Europe.

Consequently, the United States is considered to be the cradle of the right to privacy. A deeper analysis of this issue, however, leads to a slightly different reflection. Warren and Brandeis' concept was developed as a result of an in-depth analysis of not only the jurisprudence of American courts but also, perhaps most importantly, the literature and jurisprudence of British courts. Warren and Brandeis based their concept of the right to privacy as the *right to be left alone* itself based upon the theses of English Justice T. Cooley. In his famous *Treatise on the Law of Torts* of 1888, he classified personal rights[15]. Among them, he listed the right to personal immunity, defined as the right to *complete personal immunity* or the right to be left alone. He pointed out that an infringement of this right will involve not only the actual infliction of damage but also an attempt to cause damage, entailing psychological injury to the individual. Warren and Brandeis elaborated on this thesis by stating that not only property and integrity in the material sense but also the non-material sphere of informational and emotional autonomy of an individual should be protected. The case law arising from the analysis provided by Warren and Brandeis finds its implication not only on the right to be let alone as the element of the doctrine but also on shaping the meaning of privacy in the 19th-century case law which shall now be discussed hereinbelow.

The idea of privacy, as described in Chapter I, titled *Meaning of privacy and early definition*

individual rights is a fundamental principle of the legal system, and that the law must be able to adapt and evolve in response to the changing needs of society. Regenerate response

[15] T. M.Cooley, *Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*, Chicago, Callaghan and Company, 1879, pp. 24-44.

is the search for the earliest concept of the right to privacy over centuries. It clearly depicts that it is inherent in legal culture to attempt to define ownership, the non-public sphere of right, and concepts that arose out of such ideals. The right to privacy was not an obvious idea at the very beginning, and as consequence, it was necessary to find its roots in concepts such as ownership or confidentiality before a formal definition of privacy could emerge. The attempt to protect privacy as we know it now under the European legal order, including the GDPR, derives from the need to shape the information that is known about individuals and from the direct right to be left out of the discussion or disclosure of further information. Consequently, one could ask: *when does one begin to have such privacy as a right?* An obvious answer may be found in *The Right to Privacy* article published by the Harvard Law Review, authored by Samuel Warren and Louis Brandeis. It would be impossible to formulate the right to privacy as recognized today without first considering certain early case law as discussed below along with its progeny. A reason for the aforementioned may be because the right to privacy was not a phenomenon that was inherently always present but was discovered or arrived at as an outcome of evolving social needs.

In the early eighteenth-century case of *Entick v. Carrington* from 1765, the matter of improper search and seizure and the right to privacy occurred occasionally as an early indication of the right to privacy. The case originated with the plaintiff, John Entick, and was about the trespass of his house and the subsequent seizure of certain writing materials authored by him which he had drafted for magazine *The Monitor*. The King of England authorized two of the King's messengers to break into the house of the plaintiff and search for drafter with the purpose of *quieting clamor and sedition*. In some sources, the judgment in the case of *Entick v. Carrington* is viewed almost with the same approach as the *1789 Declaration.* It is worth mentioning that the case dealt with by Lord Camden as described above does not refer to privacy yet, but the judgment was delivered based on the trespass. Consequently, the approach was less positive than in the case of the above-mentioned declaration. Lord Camden, in his outstanding judgment, states:

> *What would the parliament say, if the judges should take upon themselves to mould an unlawful power into a convenient authority, by new restrictions? That would be, not judgment, but legislation*[16].

[16] *Ibid.*

Consequently, Lord refers to the inability to stand above the law, not the right to privacy itself[17]. Apart from the objective assessment as we see it now, the judgment of *Entick v. Carrington* was later quoted in another case of *Boyd v. United States.* The following US case highlighted that *Entick v. Carrington* was considered to be the case that stands in favor of the *sanctities of man's home and the privacies of life*, further recalling the first amendment of the US Constitution. In fact, what was laid down by the US Constitution is not a *per se* or explicit codification of an absolute or clearly defined right to privacy. Nevertheless, it serves as a preface of sorts to the right to privacy identified by Warren and Brandeis in 1890. Following case law, such as *Olmastead v. United States* from 1928 where Brandeis served as a supreme court judge, held that there is a need for protection against interference in personal conversations of an individual. *Olmastead v. United States* was a case that reviewed whether the use of wiretapped private telephone conversations, obtained by federal agents without judicial approval and subsequently used as evidence, constituted a violation of the defendant's rights provided by the Fourth and Fifth Amendments[18]. Similar tendencies to search for the legal ground of the right to privacy were also found in multiple jurisdictions across the world.[19]

On a number of different national grounds understanding of privacy has been shaped in a different way. As the definition of privacy have shaped through XIX century European case law it remains important to stated that codification of right to privacy was slower and more reluctant that recognition via case law. Importantly enough, the right to privacy was never directly translated to *the Right of Man and Citizen,* which rather focused on the freedom of speech or press and the meaning of those rights and guarantees from the perspective of

[17] A. A. M. Irvine, *Human Rights, Constitutional Law and the Development of the English Legal System*, Portland, 2003, pp. 278.

[18] U.S., Supreme Court, *Olmstead v. United States*, 277 U.S. 438, February 1928. Argued February 20, 21, 1928 Decided June 4, 1928 277 U.S. 438. Retrieved December 19, 2021 from Retrieved April 17, 2023 from https://supreme.justia.com/cases/federal/us/277/438/.

[19] For example, similar constitutional developments followed in France with the French Revolution. Nevertheless, constitutional protection was featured in the French Constitution no sooner than the 19th century. There were also early privacy cases, particularly referring to the use of personal images as, for example, *Felix c O'Connell* from 1858.

democracy[20]. Consequently, one of the most meaningful documents in shaping the modern understanding of citizens' rights did not include the right to privacy per se.

Prince Albert v. Strange is one of the instances from the early 19th century that best illustrates how privacy is understood today. The plaintiff was not consulted prior to the display and publication in the catalog of reproductions of etchings depicting the lives of Queen Victoria and her husband, which marked the commencement of confidential legislation. The theft and use of veterinary medicine formulations by an employee in the *Yovatt v. Winyard* case were further described as posing comparable legal issues to those raised in the earlier-cited *Prince Albert v. Strange* case. In all instances, it was adamantly asserted that, despite the fact that the studied judgments safeguard various values, like property, honor, or image, their unifying denominator is the right to privacy. It was only logical for Warren and Brandeis to reference British philosophy and legal precedent. Due to the common law foundation of the legal system, both legal systems are relatively similar to one another.

Early jurisprudence about privacy was mostly focused on the right to shape information about individuals. In simple terms, it means that an individual gains the right to define what information about himself or herself is further disclosed to the public or, otherwise speaking, to the information accessible by others. As an example of such an understanding of privacy rights, the case of *Southey v. Sherwood* may be recalled. The case concerned the right to withdraw the permit to publicize the piece of writing authored by the Poet Laureate Robert Southey; his piece of writing was titled *Wat Tyler*. The author claimed that the piece was written in his youth and that it was disclosed by him to his friends only in 1794 but was not intended to be generally accessible to the public.

As the complaint issued by Lancelot Shadewell states, the request is to *restrain them their servants and agents from printing, publishing and selling the said Poem*[21]. It was further discussed by the author that there was no copyright conveyed that may enable further

[20] The Rights of Man and Citizen (French: *Déclaration des Droits de l'Homme et du Citoyen*) is a fundamental document in the history of human rights and serves as a cornerstone of the French Revolution. It was adopted by the National Assembly of France on August 26, 1789, and is considered a fundamental document of the French legal system.

[21] *Ibid.*

distribution[22]. It is worth noticing that there is a very limited scope of privacy mentioned in general in the complaint issued. In fact, the core element regarding privacy in this case is the right to decide if one revealed the information purposefully to the public or to a limited number of people, and no further disclosure may happen without prior consent.

Shortly after *Southey v. Sherwood,* the court decided on the *Gee v. Pritchard* case, where the court directly referred to privacy, which makes it a landmark case in this regard. Plaintiff attempted to get protection for the privacy of letters sent to her husband's son when they were friends. In her request to the court, plaintiff Mrs. Gee asked for an injunction restraining Pritchard from publishing letters of a private and confidential nature. Her statement included the fact that she had never consented to any further disclosure, stating that publication of such letters would be a violation of privacy[23]. The case not only raised the question of equity as a doctrine of British law but also referred directly to wounded feelings and the welfare of society when it came to the ownership and privacy of correspondence such as letters[24].

The reasoning included in the above listed cases focuses mostly on the lack of prior consent for the disclosure of the information. Additionally, it is important to highlight that there is a need to be able to cancel the consent given as an element of privacy rights. This scenario was discussed in the *Wyatt v Wilson* case[25]. In this case, the artist Matthew Cotes Wyatt expected an injunction against the bookseller E. Wilson, who was in charge of the printing and

[22] In a global understanding, copyright protection attaches to the written word as soon as the work is created in a fixed and tangible form. In other words, as soon as the words are written down or typed, they are automatically protected by copyright law. This applies to various written, or otherwise expressed, forms, including books, articles, poems, essays, letters, and other literary works.

[23] UK, Judgement, *Gee v. Pritchard,* [1818] EngR 605, (1818) 2 Swans 402, (1818) 36 ER 670, July 1818. Retrieved December 27, 2021 from http://www.commonlii.org/uk/cases/EngR/1818/605.pdf.

[24] When it comes to the equity doctrine, Lord Eldon stated what follows in the *Gee v. Pritchard judgment the doctrine of these courts ought to be as well settled and made as uniform almost as those of the common law laying down fixed principles but taking care that they are to be applied according to the circumstances of each case. I cannot agree that the doctrines of this court are to be changed with every succeeding judge. Nothing would inflict on me greater pain in quitting this place than the recollection that I had done anything to justify the reproach that the equity of this court varies like the chancellor's foot.*

[25] U.S., Supreme Court, North Carolina, *Cora E. Wyatt And L. R. Wyatt v. W. S. Wilson And A. H. Martin (Wyatt v. Wilson),* 67 S.E. 501 (N.C. 1910) 152 N.C. 276, March 1910.

distribution of prints of the King George III. The plaintiff claimed that those prints were based on his drawings, which were eventually withdrawn from any publication[26]. Here the Lord Chancellor reported that such an image had originated from the diary kept by King's physician and that *this Court would not in the King's lifetime, have permitted him to print or publish*[27]. The judgments of Lord Eldon paved the way for the further development of privacy case law and its growing importance. Apart from the quoted landmark case of *Prince Albert v. Strange*, *Abernethy v. Hutchinson* remains one of the crucial cases on the discussed subject[28]. The *Abernethy v. Hutchinson* case concerns the professional interests of the plaintiff when it comes to the publication of his lectures. The case grew into not only a copyright landmark case but also a confidential law case that further eased the way for privacy rights recognition[29]. Further developments in case law regarding privacy were also supported by the doctrine, which undoubtedly shaped the approach to privacy law afterwards[30].

In fact, the discussion about early XIX-century case law stands only as a beginning of the discussion, and neither *Prince Albert v. Strange* nor any publication, including *On Liberty,* stands as the end of the privacy-shaping story. To fully depict the approach to privacy development, it is worth taking an overview of the later case law regarding the right to privacy and its understanding. In the early case law about privacy, one can visibly see that the focus was strongly on the matter of shaping revealed information with regard to very day-to-day things such as letters. In the latter development, we can observe how recognition of privacy grows into an aspect related to, among other things, dignity. Such recognition was definitely supported by the technological transformation (even if it was in these early times) as well as growing portrait trends[31]. The discussed trend was even named *portraituromania* and played a

[26] Plaintiff replied on the Engraving Copyright Acts (1735 to 1766).

[27] Quoted in another privacy related early case, namely *Prince Albert v Strange*, 1849b, para. 25.

[28] UK, Judgment, *Abernethy v Hutchinson*, 1 HandTw 28, [1825] EngR 653, (1824-1825) 1 H and Tw 28, (1825) 47 ER 1313, June 1825.

[29] This approach was already highlighted by Lord Eldon in *Gee v Pritchard* case discussed above.

[30] For example, the opinion shared by a friend of Jeremy Bentham, Samuel Romilly, who made an argument about the welfare of society in *Gee v Pritchard*, may be considered an element of the liveral-utalitarian approach to thinking about privacy. Another landmark view may be J. S. Mill's statement of privacy in the articulation of the liberal/utalitarian approach in his *On Liberty*. Listed thinkers, among others, shaped the understanding of privacy in the early XIX century.

[31] Q. Bajac, *The Invention of Photography: The First Fifty Years*, London, Thames & Hudson, 2002, pp. 56.

vital role in shaping privacy due to the fact that creating a portrait can be equalized with currently known personal image processing and, as a consequence, may raise some objections towards such processing.[32]

It is important to remember that, at the time discussed in this chapter, there was not yet a settled meaning of privacy as such. Of course, early case law as well as the finalization of the meaning given by Warren and Brandeis in the article on privacy gives us an outline of the meaning of the word *privacy*. Nevertheless, we are still at the stage where the world is seeking the right place for privacy within its legal order, with the pioneers in case law being England and France. At the time of *Pollard v. Photographic Company*, it was clearly discernible that case law had undergone a shift when it came to the role of privacy. Initially, the case was argued as a breach of contract; nevertheless, in the judgment itself, additional elements were used to support the plaintiff's position.[33] At the beginning, the focus of the case was on the fact that the photographer was in breach of contract when he used the image of a photographed person on a Christmas card in his window. In the comments to the judgment in this case, one can find an argument based on the sentimental grievances of the plaintiff. This argument goes beyond classic contract infringement and goes in the direction of dignity recognition, the right to privacy, and the right to decide in what way our image is further disclosed. This dignity-based approach finds support not only in case law but also in legal doctrine[34].

Growing access to data and the popularization of photography led to the point where the public's appetite to know more about other people's lives was growing[35]. Knowledge of information that was defined as personal by the owner of such information was always considered very influential and powerful. As a consequence, thoughts on privacy are becoming more valuable and changing from being a fatuous expectation of the upper classes to a right

[32] *Ibid.*

[33] UK, Judgment, *Pollard v Photographic Co*, 1888, 40 Ch Div 345, June 1888.

[34] J. S. Mill, in his *On Liberty* states that the *duty to onself, when it means anything more than prudence, means self-respect or self-developement, and for none of these is any one accountable to his fellow-creatures because for none of them is it for the good of mankind that he be held accountable to them.* This approach, that law should mirror dignitarian values, was further visible in both Kant's and Mill's writings and finds strong support in German doctrine as well. This approach paves the way for privacy to be understood as being close to dignity protection. For example, Rudolf von Jhering and his approach expressed in *Der Kamph ums Recht* from 1872.

[35] The emerging importance of image as an object covered by the right to privacy was discussed in the *Marion Manola v Stevens & Mayers* case concerning an actress who wanted to limit the scope of distribution of her image taken during her performance.

that belongs to every individual. Warren and Brandeis, in their article, opened a discussion that went further to a point that was probably not foreseen by the originators of privacy thought such as Bentham, Mill, or von Jhering. They have added an extra factor of modern approach that opened up a discussion for future thinkers but also judges as the right to privacy became more and more legally grounded. The approach of early case law and, in general, XIX-century case law on privacy differs vastly from the up-to-date challenges. Nevertheless, it proves from the perspective of current legislation, including GDPR, that the need for protection of the right to privacy will change due to technological growth. By analogy, the rise of online internet intermediaries' may pose for all today a substantially similar challenge to the growing portrait fashion of the XIX century.

Meaning of the right to privacy has reached a turning point in our view of what is private because of the continued growth of the right to privacy. What is the most private aspect that has to be preserved, especially in the age of technological advancement when data continues to be one of the most potent instruments available to our society? As a result, the idea of personal data - data that directly relates to an individual - and sharing such data might result in the violation of personal rights emerged. The concept of personally identifiable information and the right to privacy were explored by great thinkers such as Pound and Freund, who defined privacy in terms of an extension of personality or personhood[36]. Consequently, the notion of information that identifies an individual was traced back to the idea of personality, or, speaking otherwise, to the idea of personal characteristics of the individual. In 1960, William Prosser published an article in which privacy was divided into four dimensions based on tort law, namely intrusion: intruding (physically or otherwise) upon the solitude of another in a highly offensive manner. Private facts: publicizing highly offensive private information about someone that is not of legitimate concern to the public. False light: publicizing a highly offensive and false impression of another. Appropriation: using another's name or likeness for some advantage without the other's consent[37]. One of the key moments that definitively established the legal existence of the right to privacy was the Supreme Court's decision in

[36] R. Pound, *Interests in Personality*, Harvard Law Review 1915, vol. 28, p. 343 and P. A. Freund, *Privacy: One Concept or Many?* [In:] *Privacy: Nomos XIII*, J. Roland Pennock, John W. Chapman (Eds.), New York 1971, pp. 182.

[37] D. W. Prosser, *Privacy*, California Law Review 1960, vol. 48, cited as E. Alderman, C. Kennedy, *The Right to Privacy*, New York 1995, pp. 155–156.

Zacchini v. Scripps-Howard Broadcasting Co., which referred to the right to commercial publicity.

The acknowledgment of the right to privacy as a constitutionally protected right was the apex of the process by which it evolved into one of the common law systems. The definition and significance of privacy as a legal phenomenon served as the foundation for early attempts to codify the right to privacy. What is more, the growth of technology and big data brings new challenges to jurisdictions around the world as well as new questions on how to understand legal standards that were developed through years of legal practice. The recently enacted General Data Protection Regulation (GDPR) serves as a great example of how a law attempts to face modern challenges created by technological development. The origin of the regulation, namely Article 16 of the Treaty on the Functioning of the European Union along with Article 8 of the Charter of Fundamental Rights of the EU, implies that before analyzing the question of what rights are protected under the Act, it shall be addressed how privacy may be understood. To reveal this meaning and provide a ground for the creation of the regulation, one must explain the complexity of the term *privacy*. The protection of the sphere of private life is a first-generation human right, and as a fundamental right, it is protected in most modern legal systems[38]. At the same time, privacy as a term is used more and more often, in different contexts and dimensions. As an introduction to any analysis of privacy, it needs to be mentioned that the term is associated with multiple meanings, such as a right, claim, situation, value, and autonomy[39]. It serves as a vital point of interest for multiple thinkers, and the characteristics of privacy remain a matter of discussion when it comes to their scope and meaning. The right to privacy protection is guaranteed by international law, European law, and national jurisdictions .[40] Privacy in normative terms assumes the individual's right to shape the sphere of private life so that it is free from interference and inaccessible to others[41]. Contemporary states are developing legal instruments to a significant extent to protect privacy, but at the same time, they find reasons to strongly interfere. What is more, the development of technology creates more and more risks and potential spheres of infringement for privacy protection. That is why

[38]A. Neier, *The International Human Rights Movement: A History*, Princeton 2012, p. 77.

[39] C. S. Gal, P. B. Kantor, M. E. Lesk, *Protecting Persons While Protecting the People: Second Annual Workshop on Information Privacy and National Security ISIPS 2008*, New Brunswick 2008, p. 59.

[40] G. Ulrich, I. Ziemele, *How International Law Works in Times of Crisis*, Oxford 2019, p. 118.

[41] M. Timmons, *Oxford Studies in Normative Ethics*, vol. 9, Oxford 2019, p. 16.

multiple countries, supranational organizations, or international documents attempt to catch up with technological growth and secure legal obligations regarding privacy in the age of the Internet. From an external perspective, the right to privacy secures one of the most important aspects of human life, which is tightly connected with values such as dignity or freedom of expression. In the formal doctrine, it is possible to find a whole group of terms referring to the analyzed issues of privacy: the personal sphere of man, the legal-personal sphere, the sphere of intimacy, or the area of secrecy, the area protected by non-disclosure[42]. The idea of the law on the protection of private life has changed depending on the state, the legal system, and the concepts put forward in science or on cultural and religious grounds. This leads to the conclusion that there is no one universal privacy system and that the scope and perspective on what shall be protected will differ depending on the jurisdiction.

Although the concept of *privacy* arguably originated in the United States, and was further affected by the English case law, it should not be forgotten that in the German-speaking area and in the Roman countries, the doctrine of the right to personhood arose in the 19th century. Since the beginning of the nineteenth century in German jurisprudence, the term *Individualrechte* was understood to mean a series of rights such as the right to a good name, to a surname, to organize one's life as one wishes. to organize one's life as one sees fit[43]. French law also created the idea of *droits de la personnalité* towards the end of the 19th century to protect a person's identity, name, and appearance[44]. Both of these concepts can be considered parallel to those developed in American law. From the perspective of political and legal thought, the doctrine concerning the right to privacy emerged during the XIX century, but its origins can be found as early as the Bible. After more detailed analysis, the basic concept of privacy can be found multiple times through the history of political and legal thought, such as by Grotius, Hobbes, Locke, Montesquieu, and J.J. Rousseau[45].

---

[42] I. Kerr, I. R. Kerr, V. M. Steeves, [et al.], *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York 2009, p. 162.

[43] Z. Szente, K. Lachmayer *The Principle of Effective Legal Protection in Administrative Law: A European Perspective*, Routledge, New York, pp. 348.

[44] H. Beverley-Smith, A. Ohly, A. Lucas-Schloetter, *Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation*, Cambridge 2005, p. 150.

[45] Annual Institute on Privacy Law: Strategies for Legal Compliance in a High Tech and Changing Regulatory Environment, vol. 1, Practicing Law Institute, Indiana 2011, p. 27.

Apart from the complexity and variety of political and legal doctrines relating to this issue as set out beforehand, it should be noted that the early characteristics of the right to privacy as we have come to appreciate it today, first appeared, as introduced above, in 1890 as the outcome of the work of the American law professors V. Brandeis and E. Warren, who defined it as a right to exclusivity combined with the idea of privacy under the formulation of *a right to be let alone*[46]. Consequently, there is a strong presumption that the early stages of the formulation and development of privacy rights were based on Anglo-Saxon law. Another researcher who has dealt with the issue of *privacy* is Joseph Kohler, who in 1907 defined this concept as freedom of information disposal about yourself, but with regard to the confidentiality of correspondence. Since then, we have observed an increase in interest in this legal issue, which is caused by a great many factors. As mentioned before, there is no one unified definition of the right to privacy; each piece of legislation attempts to define it in its own way in line with constitutional standards.

2. The modernized XX-century understanding of the right to privacy; arriving at the current understanding.

As written by R. Williams in Keywords: A Vocabulary of Culture and Society, ***Private**, that is, in its positive sense, is a record of the legitimation of a bourgeois view of life: the ultimate generalized privilege, however abstract in practice, of selection and protection from others (the public); of lack of accountability to 'them'; and of related gains in closeness and comfort of these general kinds. As such, and especially in the sense of the rights of the individual (to **his private life** or, from a quite different tradition, to his civil liberties) and valued intimacy of family and friends, it has been widely adopted outside the strict bourgeois viewpoint. This is the real reason for its current complexity*[47] (emphasis added). The quote as presented above touches upon two important aspects clarified in the XX century once compared to the XIX emerging understanding. First of all, the XX century's understanding of privacy, both when it comes to legislation as well as doctrine, is to name privacy in a straight-forward manner. The XIX century was a time of emerging understanding of privacy, while earlier understanding of the right to privacy was grounded more in the confidentiality of property rights. Consequently,

[46] B. R. Ruis, *Privacy in Telecommunications: A European and an American Approach*, Kluwer Law International, Hague 1999, p. 24.

[47] R. Williams, *Keywords: A Vocabulary of Culture and Society*, London 1988, p. 248.

the former background prepared by early doctrine understanding brought us to the place in history where we officially recognize privacy as standing alone, as named in the quote above. Instead of justifying the existence of privacy protection by other rights, the world views privacy protection as an alone-standing value that will shortly find its place in the codified international and national legal systems.

Thanks to the wider recognition of the right to privacy, we will not only observe its impact on society but also the growing amount of interpretation of what privacy actually means. Discussion about privacy shall focus not only on codified elements of law as international conventions or pure doctrine but also on elements of assessment towards a normative and descriptive understanding of privacy that emerges.

The distinction between descriptive and normative theories is usually the starting point in the construction of theoretical concepts concerning the interpretation of the law, including the analysis of the right to privacy. The essential feature of normative theories is the orientation of interpretation according to values (goals), which should be realized according to these theories. Hence, the basic groups of normative theories of interpretation were characterized by the opposing values of a reduced form: the constancy (certainty) of law and the adequacy of law and life. Accordingly, these theories were called static (subjective) and dynamic (objective) theories. The choice between static and dynamic theories of interpretation entailed the choice of a particular set of interpretative directives at the level of resolving inconsistencies between linguistic, systematic, and functional (second-level interpretation directives). From a descriptive perspective, it has not. From a descriptive perspective, it was not possible to reconstruct universally accepted conflict directives because the practice of interpretation has shaped preferences that are most domain-specific. This also applies to the normative perspective, which is reflected in the nomenclature used by the author, because in later works he writes about the *ideology of interpretation* as an alternative to the *normative theory of interpretation*. Early codifications on privacy appeared with the development of privacy protection in American law from the 1890s onward, and privacy protection was justified largely on moral grounds; in fact, its function was mostly descriptive and presented a person's affiliations sifted through the lens of what is morally ordered. In the doctrine, the division between normative and descriptive understandings of privacy is present, and in fact, it helps to distinguish descriptive accounts of privacy while describing what is in fact protected as private, contrary to the broader approach as defined by normative understanding. A limited perspective

on privacy centers on the idea of personal information that has been made public. Warren and Brandeis, William Prosser, and more modern authors like Charles Fried (1970) and A. W. Parent (1983) all backed this viewpoint that places emphasis on information management. In fact, A. W. Parent stated his own definition in the 1983 publication titled *Privacy, Morality, and the Law*, where he claims that privacy is *a condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is diminished exactly to the degree that the others possess the kind of knowledge about him*[48]. Of course, the approach presented by Parent has some vulnerabilities that were discussed in the doctrine, among others, by Scanlon; nevertheless, it is worth mentioning that Parent's statement essentially summarizes the understanding of a limited scope of descriptive privacy understanding. Normative privacy is about what privacy ought to have, while natural privacy is descriptive. Normative understanding is about whether an individual in fact has exclusive control over the information about him or her. The issue of privacy involves the self-interest of the individual, his or her well-being, and the actions taken by the individual to protect that value. Privacy also refers to the sphere of an individual's activity that is not subject to external control. Thus, we can define this concept as a space of free movement, a domain of autonomous activity that is free from the control of other entities. It includes physical space, objects, and structures to which others do not have access. Depending on the socio-cultural system in which an individual functions, the sphere of privacy is defined differently in terms of interactions, degree of distance, and level of isolation[49]. As a consequence, privacy in the normative sense implies the power of the individual to shape the private sphere of life so that it is free from interference and inaccessible to others. This right includes the ability to establish and maintain relationships with others for, among other things, the purpose of developing one's own personality.

The link between two aspects of privacy as presented above is the subject of the legal notion of a reasonable expectation of privacy. The value of individuals living in a community and engaging in social ties was highlighted in Aristotle's philosophical framework. He felt that people are political creatures that thrive in well-ordered societies. The focus on communal life and the common good by Aristotle may imply that he valued public life and the interdependence of people within a society. Aristotle, on the other hand, acknowledged the

[48] W. A. Parent, *Privacy, Morality, and the Law*, Philosophy & Public Affairs Vol. 12, No. 4 (Autumn, 1983), pp. 269-288. Retrieved August 7, 2021 from www.jstor.org/stable/2265374.

[49] J. Braciak, *Prawo do prywatności*. [In:] *Prawa i wolności obywatelskie w Konstytucji RP*, B. Banaszak, A. Preisner (Eds.), Warszawa 2002, p. 278.

importance of personal space and the need for individuals to have some degree of solitude. He introduced the concept of eudaimonia in his work *Nicomachean Ethics*, which is typically rendered as *flourishing* or *human flourishing*. This idea relates to the ultimate good or objective of human life. Individuals, according to Aristotle, require a certain amount of isolation and introspection in order to grow their virtues and pursue personal well-being. This notion of privacy as dualistic and a discussion generated by Aristotle on the idea of core and peripheral situations in talking about *friendship* may be seen to have a little resemblance. However, as can be seen from this thought, it remains peripheral as to its own understanding. As Aristotle wrote *[. . .] so they are not able to do justice to all the phenomena of friendship; since one definition will not suit all, they think there are no other friendships; but the others are friendships[. . .].* Similar complexity may be perceived towards privacy - some of the core features of the central cases may not be present in the outlying cases. One of the ways a conception is illuminated is to trace the similarities and differences between these examples[50]. The most recent examination of privacy and data protection actually reveals similarities between the two, but it is still crucial to maintain those two ideas independently. There is a significant teleological difference, as noted by De Hert and Gutwirth, even if the principle of supporting privacy may, in certain cases, necessitate data protection and may even serve as an underlying value for such. The author describes privacy as a tool of opacity that draws the line between the government's intrusion into an individual's life and freedom as a result of imposing normative limits on it, while data protection is a tool of transparency that regulates and channels the superior power[51].

An understanding of privacy from the XX century until today was not only shaped by the constant growth of science in this field of technology but also by the growing recognition of the right to privacy in law. Since the XX century, the question of the right to privacy has gained even more attention due to the trauma of the Second World War and the strong invigilation, censorship, and atrocities of war in general. The Second World War had a significant impact on the understanding and recognition of the right to privacy. During this period, widespread human rights abuses and violations, including intrusive surveillance, propaganda, and the violation of personal freedoms, were perpetrated by authoritarian regimes. The atrocities

[50] A. D. Moore, *Defining Privacy*, Journal of Social Philosophy 2008, vol. 39, no. 3, pp. 411-428,. Retrieved July 11, 2021 from https://ssrn.com/abstract=1980849.

[51] P. de Hert, S. Gutwirth, *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power* [In:] *Privacy and the criminal law*, E. Claes, A. Duff, S. Gutwirth (Eds.), Antwerp 2006, pp. 61-104 .

committed during World War II led to a global recognition of the need to protect individual rights and freedoms. In response, international efforts were made to codify and protect human rights, including the right to privacy. Notable developments include Universal Declaration of Human Rights or European Convention on Human Rights (ECHR). The war's experiences highlighted the potential hazards of unfettered governmental authority and monitoring, leading to a greater appreciation for privacy as a basic right. The post-World War II era led to a developing idea that individuals should have a safe space where they may freely express themselves, create connections, and preserve control over their personal information. During the conflict, technical breakthroughs and monitoring capabilities had a part in developing privacy rights. The use of wiretapping, secret monitoring, and communication interception prompted worries about the possibility of misuse and intrusions of privacy. As a result, legislative frameworks were created to limit governmental monitoring while still protecting people' privacy.

Currently, interest in stable and effective protection of privacy is supported by the challenges of technology, common access to the Internet, and the value of information as a means of exchange. Authors who address this issue focus primarily on identifying the areas that need to be protected by the right to privacy. Another approach accentuates and defines a list of activities that violate an individual's private life. The right to privacy is a very complex and broad concept, including family life, home life, human personal rights, human integrity, the protection of personal data, the secrecy of correspondence, the content of communications, the intimate sphere of the human person, and personal identity.[52] Identity goes far beyond physical appearance and leads up to personal history and all other collections of data about one's self.[53] Once we list elements like integrity, personal rights, and confidentiality, it seems to imply that the discussed issue is also within the scope of constitutional law. During times when numerous countries use data surveillance techniques and big data, as well as profiling, are more advanced, the right to privacy shall serve as a fragile and important value to protect.

As mentioned before, the doctrine defines privacy and its origins in multiple ways. For example, J. Thomson defines the law of privacy as a derivative of other rights, such as property rights and personal integrity, highlighting that the area is still being explored and undefined. In

[52]A. Patterson, *A Companion to Philosophy of Law and Legal Theory*, Oxford 2010, p. 146.

[53] N. Dorsen, M. Rosenfeld, A. Sajo [et al.], *Comparative Constitutionalism. Cases and Materials*, Saint Paul 2003, p. 651.

The Right to Privacy, Thomson states that *Perhaps the most striking thing about the right to privacy is that nobody seems to have a very clear idea of what it is*[54]. According to a different set of academics, who restrict privacy to an individual's personal identity, the most serious kind of privacy infringement is when an individual's sexual autonomy is violated. Further concepts are to identify privacy with control over information about one's personal life. The right to privacy is defined here as the power of an individual to determine when, how, and in what way the scope of the information concerning it may be shared with others. R. Gavison constructs his definition of perfect privacy, making its existence subject to three factors:

- when no one has access to any information about the individual,
- no one has physical access to it; and
- no one pays attention to her[55].

This interesting idea seems impossible to implement in practice in the modern state. Furthermore, R. Gavison in *Privacy and limits of Law* refers to the idea of what we assume to be covered by the idea of privacy:

> *First, we must have a neutral concept of privacy that will enable us to identify when a loss of privacy has occurred so that discussions of privacy and claims of privacy can be intelligible. Second, privacy must have coherence as a value, for claims of the legal protection of privacy are compelling only if losses of privacy are sometimes undesirable, and if those losses are undesirable for similar reasons. Third, privacy must be a concept useful in legal contexts, a concept that enables us to identify those occasions calling for legal protection, because the law does not interfere to protect against every undesirable event.*[56]

Consequently, Gavison points out elements necessary to define the scope of privacy as it is, namely: neutrality as a concept, coherence as a value, usefulness in legal contexts.

The literature on the subject further emphasizes that the protection of privacy, which assumes the right of the person's exclusive control over a particular sphere of life, shall be understood

---

[54] J. J. Thomson, *The Right to Privacy*. Philosophy and Public Affairs 1975, vol. 4, no. 4., p. 295. p. 295. Retrieved April 18, 2020 from https://www.jstor.org/stable/2265075.

[55] W. Sokolewicz, *Prawo do prywatności [Right to Privacy]* . [In:] *Prawa człowieka w Stanach Zjednoczonych*, L. Pastusiak (Ed.), Warszawa 1985, p. 253

[56] R. Gavison, *Privacy and the Limits of Law*, The Yale Law Journal 1980, vol. 89, no. 3, p. 424. Retrieved April 19, 2020 from http://www.jstor.org/stable/795891.

in a twofold manner: concerning the individual's relations with other individuals as a horizontal arrangement and in relations between an entity and public authority as a vertical arrangement[57].

It is a challenge to build a narrow and precise definition of privacy because of the very broad meaning of the right to respect for private life[58]. This complexity finds its practical application in the case law of international bodies, the protection of human rights, and above all, the extensive case law of the European Court of Human Rights, referring to Article 8 of the European Convention of Human Rights. Based on that Article, the Court examines and formulates general claims that determine the essence of the protected values, which undoubtedly allows the concept of *private life* to be defined. An example is the case of *Pretty* (*Pretty v. the United Kingdom*, 2346/02), in which the Court states that this concept consists of physical and psychological elements, the psychological integrity of the person, and may also refer to the physical and social identity of the individual[59]. In a different case, Van Oosterwijck v. Belgium, the court defined the right to privacy as the right to live in accordance with one's own wishes and without public scrutiny. Respect for private life also includes the right to make and develop contacts with other people. The case law on this issue is very rich and is an important reference in protecting the rights to private life. What is more, Article 8 opens a group of four regulations of the Convention that formulate the classical rights and freedoms of an individual[60]. Consistency and uniformity in the formulation of four freedoms and rights from Articles 8-11 of the Convention go far enough to apply a uniform methodology for the interpretation of all four provisions. This is subject to three general rules settled by the ECHR in *Handyside v United Kingdom* (5493/72), namely: (1) rights as the right to privacy are fundamental to the functioning of a democratic society and therefore need to be protected particularly intensively, (2) the limitation of these rights, although permissible and unavoidable, is exceptional and always subject to a strict interpretation (*Klass and Others v. Germany*, 5029/71), and (3) the limits of those rights may not be applied for any purpose other

[57] M. Elliott, R. Thomas, *Public Law*, 4th Edition, Oxford 2020, p. 801.

[58] The concept of right as described hereto may be also interpreted as the basic human need for a meaningful or happy existence.

[59] B. Rainey, P. McCormick, C. Ovey, *Jacobs, White, and Ovey: the European Convention on Human Rights*, 8th Edition, Oxford 2021, p. 407.

[60] The four rights and freedoms of an individual are: respect for private and family life (Article 8), of thought, conscience and religion (Article 9), freedom of expression (Article 10), and freedom of assembly and association (Article 11).

than that for which they were introduced, following Article 18 of the Convention[61]. On a national level, for the first time, the principle of individual information privacy and autonomy has been formulated and developed by the German Federal Constitutional Court in its case-law of December 15, 1983, 1BvR 209/83. The Court stated that *under conditions of modern data processing*, the Constitution of the Federal Republic of Germany protects an individual against *the unrestricted collection, use, and transfer of his personal data*. The Constitution also guarantees *the right of the individual to establish himself in principle on the disclosure and use of its personal data*[62]. What is more, on the level of the Federal Court, there is also the possibility of limiting the right to informational self-determination. However, restrictions on this right are only acceptable if the general interest prevails while respecting the principle of proportionality. At the same time, as the Court has stressed, *the law to informational self-determination* is not provided without borders.

When it comes to the international standards of the right to privacy protection, from a chronological perspective, the Universal Declaration of Human Rights is the first example. Article 12 of this Act stipulates that anyone's private and family life or correspondence may not be interfered with arbitrarily, offended, or infringed by the actions of another[63]. Furthermore, every person is guaranteed the right to legal protection against such interference or misrepresentation. In fact, Internet development poses new challenges to the protection of

[61]*Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom 1. Komentarz do artykułów 1–18*, L. Garlicki (Ed.), Warszawa 2010, p. 483.

[62] BVerfG, Decision of Bundesverfassungsgericht on the constitutionality of the 1983 Census Act, 1BvR 209/83, May 1985. Retrieved April 19, 2020 from https://www.bundesverfassungsgericht.de/Shared Docs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.

[63] The Universal Declaration of Human Rights (UDHR) makes no specific mention of the right to privacy. While the UDHR contains several provisions concerning personal freedoms and rights, such as the right to life, liberty, and security of person (Article 3) and the prohibition on arbitrary interference with privacy, family, home, or correspondence (Article 12), it does not specifically mention the "right to privacy" as a standalone provision. As it concerns the protection against arbitrary interference with private life, family, home, and communication, the terminology employed in Article 12 of the UDHR is frequently understood as including characteristics of privacy. It is crucial to highlight, however, that the UDHR does not give a clear and full articulation of the right to privacy in current legal and cultural situations.

The right to privacy has been recognized in subsequent international and regional human rights instruments, such as the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR), which provide more detailed and explicit protections for the right to privacy.

individual rights. Transnational processing and global access to the Internet make cross-country responsibility even more challenging for the idea protected by Article 12[64]. The right to privacy outlined in line with this interpretation has been an inspiration for the authors of successive international laws. Attention should certainly be paid to the International Covenant on Civil and Political Rights and subsequent international laws. Attention should certainly be paid to the International Covenant on Civil and Political Rights of December 19, 1966, where the right to privacy is enshrined in Article 17 of the act. It was decided that no one can be exposed to arbitrary or unlawful interference with his private or family life, and correspondence shall be protected against infringements. Everyone is also guaranteed the right to legal protection against such interference and assaults. The literature indicates that the Covenant protects two types of personal rights: private life, family, and correspondence can be counted among the first, and reputation and a good name shall be included in the latter category. The above-mentioned provisions of universal human rights systems strongly influenced the creators of national or supranational legal systems[65]. The right to privacy has found its place in almost every such system. The next point to note is the American Convention on Human Rights, signed in San José, Costa Rica, on November 22, 1969. It affects the territory of South American countries and the Caribbean islands; hence, the Convention is sometimes called the Latin-Caribbean. The right to privacy in the Latin-Caribbean is regulated in Article 11, which states that everyone is entitled to respect for honor, and to acknowledge dignity. Furthermore, no one shall be subjected to arbitrary or improper treatment when it comes to the private sphere of life. The above-mentioned example of regional initiatives serves only as an example, and different countries or regions around the world decided to create initiatives dedicated to protecting privacy[66]. On a more global or supranational scale, it is important to mention the European Convention on Human Rights from 1950, where the right to privacy was included as a non-absolute, basic right. The Convention's regulation is the most concise one, which concerns the method of formulation of its normative text and the precision of standards through the case-law of the Court. The regulation distinguishes between the sphere of privacy *sensu*

[64] T. Mendel, A. Puddephatt, B. Wagner [et al.], *Global Survey on Internet Privacy and Freedom of Expression*, Paris 2012, p. 22.

[65] T. Craig, M. E. Ludloff, *Privacy and Big Data: The Players, Regulators, and Stakeholders*, Sebastopol 2011, p. 35.

[66] Other examples of the right to privacy protection on an international level are the African Charter on Human and Peoples' Rights from 1986 or the Cairo Declaration on Human Rights in Islam from 1990.

stricto and the sphere of privacy relating to family relationships, housing, and correspondence. Every aspect of this right that is recognized in the Convention from the individual's standpoint is, therefore explicitly specified[67]. Details of the limits of privacy as an individual right are discussed above. What is shared as an element from the perspective of an international act preview concerning privacy is that in all cases, the scope of the protection of privacy is non-absolute and provides a detailed definition of what privacy means. On the level of international law, privacy can be traced back to elements such as protection of family life, protection of correspondence, the right to be left alone, and the guarantee of receiving no obligation to share your personal data. Nevertheless, the catalog of what shall be included under the term privacy seems to be dynamic and flexible depending on the individual context of a case, remaining applicable to different situations and dimensions of privacy protection.

Privacy is treated as an important element of rights to be protected by the European Union, as is often highlighted by the Commission and Parliament[68]. One of the foundations of this system is the Charter of Fundamental Rights of the European Union. It is important to note that, under Article 6(1) of the Treaty on European Union, the Charter is considered to have the same legal value as binding European Union treaties. Above mentioned article reads as follows:

> *The Union recognizes the rights, freedoms, and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties. The rights, freedoms, and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.*[69]

Consequently, the Charter can directly implement protection for individual rights and freedoms, among them the protection of privacy enshrined in Articles 7 and 8.[70] Article 7

[67] L. Leszczyński, B. Liżewski, *Ochrona praw człowieka w Europie – szkic zagadnień podstawowych*, Lublin 2008, p. 88.

[68] D. Kelleher, K. Murray, *IT Law in the European Union*, London 1999, p. 271.

[69] Consolidated version of the Treaty on European Union, Article 6(1), (ex Article 6 TEU).

[70] Article 7 of the Charter refers to respect for private and family life, and Article 8 of the Charter refers to the protection of personal data.

presents a broad statement that everyone shall have a right to private and family life and free communication. This formulation remains similar to previously presented international acts referring to the right to privacy. Following Article 8, there is a more complex statement related to privacy and of vital interest in the up-to-date issue related to data processing and data safety, namely the protection of personal data. The article reads as follows:

1. Everyone has the right to the protection of personal data concerning him or herself.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.[71]

The formulation is less common and has more modern characteristics than the universally used right to privacy mentioned in numerous examples of international legislation. Article 8 of the Charter implies that everyone has the right to the protection of their personal data. It further stipulates that data must be processed fairly for specified purposes with the consent of the person concerned or on any other justifiable basis provided by law. Everyone has the right to access data that has been collected concerning him or her and the right to have data concerning them corrected. Finally, it was established that compliance with these rules is subject to oversight by an independent body. Both on an international and national level, the rise in recognition of the right to privacy has led to further recognition of the right to privacy.

Moreover, in the system operating under the auspices of the Council of Europe, there is a Convention for the Protection of Individuals concerning the Automatic Processing of Personal Data[72]. It is worth emphasizing that although it is a relatively new regulation (at least against the background of the above-mentioned), it is considered to be the most basic and one of the oldest instruments of international personal data protection. It discusses in quite a detailed manner the category of data, its quality, and the safeguards necessary to deliver the right

[71] The Charter of Fundamental Rights of the European Union, (2000/C 364/01), Article 8.

[72] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981, European Treaty Series - No. 108.

security measures towards the rights of the data subject[73]. On top of all guarantees and restrictions provided by this Convention, it shall be remembered to whom and how this Convention grants protection, because Article 1 is an assurance to every natural person, regardless of nationality or place of residence, out of respect for his or her rights and fundamental freedoms in the territory of each Party to the Convention, and in particular its right to privacy in connection with the automatic processing of personal data concerning an individual. Given that it only applies to natural persons, the range of entities covered by this law is limited. Only Article 3 paragraph 2(b) makes it clear that information pertaining to other legal entities may be included in the Convention's purview, but only after a declaration to that effect has been made by a state party to the Convention. The personal range of the right to privacy appears distinct and comprehensible. All natural individuals have the right to privacy protection since only they may live a private, family life and benefit from it, according to international law and some examples of state laws.

It should be noted that data processing does not necessarily infringe on a person's right to privacy of information because the term has a broader and more agnostic definition. However, the European Court of Human Rights recently ruled that any processing of personal data should be interpreted as falling under the scope of Article 8 and, as a result, as being protected by the privacy rights promised by the mentioned Article[74]. Consequently, as presented above, the right to privacy remains a strong backbone for the development of data protection regulations. Purposively, the definition of the right to privacy remains an open question in a non-exhaustive catalog presented in different jurisdictions both on a national and international level. The right to privacy has evolved over the years to include in its scope a field addressing guarantees challenged by mass data flow, big data, and extensive processing. This field remains a fascinating scope of research, showing how the law faces and attempts to cover multilayer technological growth.

There is an equivocal discussion about meaning and reason for the right to privacy exist among today's challenges, and the state of today’s affair was summarized by the James B. Rule by stating that a*ware if or not, we are all heirs to potent Enlightenment ideas in matters relating to control. If knowledge is good and informed actions preferable to the alternative, why should*

[73] Article 5 of the Convention refers to the quality of data; Article 6 explains special categories of data, Articles 8–11 address measures, restrictions, and sanctions related to data safety.

[74] *Ibid*.

we expect institutions of all kinds to maximize their grip on the lives of those they deal with?[75]. This quote perfectly summarizes the philosophical nature of reasons to protect an individual's right to privacy, leaving it as an open question.

One of the cornerstones upon which the data protection legislation is based is the idea of personal data. Threats to a person's private zone, which includes his or her personal data, have increased as a result of economic development and the creation of new technologies, particularly information technology. Along with the development and spreading of the role of information technologies, the scope of the notion of personal data has also been changing. As quoted previously, data protection differs as a term from the normative perspective from privacy itself but may be directed towards a similar higher protected value. In the area of terms developed around privacy and new technologies, the idea of personally identifiable information (PII) emerges. Therefore, it is worthwhile to have a look at the legal definition of the notion of *personal data* and the new categories of data distinguished in the General Data Protection Regulation.

To be able to navigate through new technologies and privacy, it may be necessary to set up a context for the terminology used in this field of science, and PII remains one of the most vital ones. The concept of personally identifiable information, or in general, data that can be assumed to be personal, leads to a discussion about when we can talk about privacy law violations and go further about data protection applications. The definition created for the purposes of personal data protection focuses on the element of personal, so the corresponding definitions can be found in almost all legal acts in this field[76]. They are comparable to one another since they were both made using the same plan. According to the most often used definition, personal data refers to any information pertaining to a named or distinguishable natural person. During the period when the above definition was in effect, an extensive doctrinal interpretation arose, with the aim of trying to clarify the terms contained therein and translate them into practice[77]. One of the first challenges that the definition encounters is the traceability of personal data, or simply speaking, what is the benchmark for stating that the data

[75]J. B. Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, Oxford 2007, p. 192.

[76] One of the exceptions to this rule comes from United Nations guidelines from 1990, where there is no definition of personal data as such. Nevertheless, this approach remains unique compared to other national and international acts.

[77]

are considered to be personal? The question remains even more important in the light of new technologies, where we can assume that almost every piece of data, after a certain amount of analysis, may become a personal one, pointing at individuals[78]. In the case of traceability, the characteristic is the ability to identify a specific personal data subject, the ability to distinguish a person from others on the basis of the data processed. An exemplary model for this characteristic is, *inter alia*, Article 2 of Directive 95/46, which indicates that an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to that person[79]. Another issue under consideration concerns so-called inputs.

As mentioned earlier, especially in the case of the processing of personal data by modern media, the question arises of how to separate the real possibility of obtaining data from the one burdened with an impossible real effect. It is definitely a fact that the effort put into data acquisition cannot be ignored, and indeed, some data will lose the characteristics of personal data if the effort is disproportionate to the effect of the acquisition. However, the problem arises here as to the criteria for such acquisition and defining the limit.

The report explaining the position of Council of Europe Convention 108 proposes to solve this problem by defining the notion of an identifiable person. According to the report, it defines a person as one whom we can easily identify and does not include identification by means of very complex methods (these methods are defined in the report as sophisticated)[80]. A number of legal acts refer to the scope of work that should be applied to an individual; nevertheless, there will always be a small field of discretion in this regard as none of the definitions provides

[78] The above interpretation of traceability is well established not only in EU law but also in the jurisprudence of the European Court of Human Rights. See, for example ECtHR, Decision, *Lundvall v. Sweden*, no. 10473/83, December 1985 or ECtHR, Application, *Klass and Others v. Germany*, nos. 5029/71, 5485/72, and 6234/73, September 1978.

[79]According to the definition stated by article 2 of the GDPR *'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*.

[80]Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981 defines as follows: *'Identifiable persons' means a person who can be easily identified: it does not cover identification of persons by means of very sophisticated methods.*

clear details[81]. This approach ended up in the GDPR broad definition of personal data as presented by Article 4 of the Act which states as follows: *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*. Even though previously quoted legal acts were created with a significant time lag from the GDPR, the approach of a definition remains similar - it states that everything that enables us to identify an individual is personal data and, as a consequence, shall be covered by privacy guarantees and data protection laws.

The question of personally identifiable information remains a vital one not only from the perspective of the GDPR but also from the perspective of every legal act that regulates privacy protection and processing of personal data because this defines the scope of applicability of a particular act. On the grounds of the GDPR, recital 26 recalls that principles relating to personal data processing should apply to any information that enables the identification of a natural person. It also further discusses that if the data are pseudonymized but can still be attributed to a natural person with the use of additional information, they shall be treated as personal data as well. It is important to note that the GDPR has a fairly broad definition of what is personally identifiable information. Both the reference in Recital 30 to the online identifiers and the direct reference in Recital 34 to genetic information as RNA are to be considered as personal data. Numerous cases on a national and international level have brought up the issue of personally identifiable information. As the outcome of years of development, the Article 29 Data Protection Working Party came up with a suggestion to ground the definition on four chief constituent elements, namely:

1. *any information* that points out that there is no catalog of types of data that may be considered personal. It also reflects the aim of the European Union to apply a broad

[81] For example, Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment defines personal data in a similar manner, namely any information relating to an identified or identifiable individual ("data subject").

scope to the concept that is not limited by the definition of sensitive or private information[82].

2. *relating to* is referred to by the CJEU again, taking a broad approach. In the case of Nowak, the court repeated that the type of relationship doesn't matter; what matters is the effect. The Court stated that the requirement *is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person*[83]. In the quoted judgment, the Court seems to take the approach that corresponds to the position previously taken by the Article 29 Data Protection Working Party in the opinion from 2007[84]. Nevertheless, the approach of the Court was not always consistent on the matter and in joined cases of *YS* the Court held that access to data in a dossier about asylum seekers does not constitute access to personal data[85]. The case of *YS* is also a rare example of a restrictive interpretation of the law in this regard.
3. *identified or identifiable* this shall be understood broadly, as signaled by the wording of both article 4(1) and recital 26 of the GDPR. The CJEU took a broad approach, stating that data is considered to be personal even if the controller itself cannot make a link to a particular person without help from other sources[86]. It is, nevertheless, important to mention that this approach is limited by Recital 26 which mentions proportionate and reasonable effort.
4. *natural person* the requirement in the definition of personally identifiable information seems to be the most obvious one. This initially implies that the data of corporations, partnerships, and other legal persons is not protected under GDPR. In Joint Cases of Schecke, the CJEU held that *in so far as the official title of the legal person identifies*

[82] CJEU, Judgement, *Peter Nowak v Data Protection Commissioner*, Case C-434/16, December 2017. ECLI:EU:C:2017:994, para. 34.

[83] *Ibid*., para 35.

[84] Article 29 Data Protection Working Party, 2007WP 135, Revised and Updated Policy to promote the transparency of the activities of the Working Party established by Article 29 of Directive 95/46/EC from 15 February 2007, pp. 9-12.

[85] CJEU, Judgement (Third Chambre), *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, joined cases C-141/12 and C-372/12, July 2014. ECLI:EU:C:2014:2081, para. 48.

[86] CJEU, Judgment (Second Chamber), *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, October 2016. ECLI:EU:C:2016:779, para. 43.

> *one or more natural persons*, the natural person may claim protection under articles 7 and 9 of the Charter of Rights of the European Union[87].

Regardless of case law inconsistencies, the underpinning value behind the definition of personally identifiable information remains clear: the aim is to cover, by this definition, all data that may lead to an individual, in particular a natural person. Similarly, the right to privacy, which in the modern era remains inseparable from the concept of personally identifiable information, does possess a plurality of understandings and dimensions; nevertheless, the high-level purpose and aim remain coherent: protection of the individual rights of data subjects and minimization of possible misconduct via the use of personal data.

[87] CJEU, Judgment (Grand Chamber), *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, joined cases C-92/09 and C-93/09, November 2010. ECLI:EU:C:2010:662, para. 53.

B. Effects of the inability to meet the requirements of the law and the concept of the *bad guy,* according to Pound, Fuller, Llewellyn, and Postner.

1. Pound's understanding of law in books and law in action

The following part of this dissertation aims to discuss the perspectives on the law as actively applied or viewed only from the perspective of the legal norm as written down in the codes. Perspectives on formal, realist, pragmatic, and positivistic aspects of law shall remain vital in the discussion about the applicability of the General Data Protection Regulation as well as the right to be forgotten and data transfer rights under said regulation, taking into account implementation challenges, as the responsibilities of the data controller remain strongly discussed when it comes to the scope of responsibility. While analyzing the doctrine on what should be considered applicable from a legal perspective and how the law should be shaped, the following part of the dissertation shall recall names such as K. Llewellyn, O. W. Holmes, and R. Postner to evaluate the contemporary aspects of law in books and law in action doctrine.

The essence of law can be viewed from two distinct perspectives, namely: historical and contemporary. It is crucial to address the question of whether the legislation written in books can be applied in practice before moving on to the following sections of the debate. Longer than the debate over privacy and data protection, the term *law* has been used to refer to the restricted, textual application of the law. However, it matters because, particularly in light of technology, the issue of how to apply the law represents the real conflict that will result either in the successful defense of individual rights or in the creation of legal fiction. Even though the law aspires to be as precise as possible it does not mean that every written rule is of a quality of applicable law. As rightly stated by Prof. Freund, courts have the tendency to invalidate the rules considered by them as not wise.[88] As a consequence, the applicability of the law as written extends as far as its consideration to be within the scope of acceptance. The appeals court in the state of New York, United States, ruled on the matter of regulating working hours on projects that are financially supported by the state or city budget. The same subject matter was

[88] P. A. Freund, *On Law and Justice*, Cambridge, 1968. p. 259.

touched upon by the Supreme Court of the United States. The first court directly stated that there is no option to regulate the mentioned working hours, but there is a possibility to regulate the working time of personnel working in bakeries. The first court mentioned that there is no such possibility of working hours regulation in the first case, but it is possible in the latter subject matter. Then the Supreme Court published a judgment that reversed the first subject matter beforehand, and then in the latter judgment, it underscored the latter subject matter as well[89]. This practice backs up Dr. Freunden's point of view on the selectiveness of the legislation. This method gradually takes us to Pound's position and the topic of law in books vs. law in practice. In the first case, we focus on the diversity of accepted visions of law while exposing the evolution of views on it. In the second case, when we adopt the contemporary perspective, we notice first of all that our understanding of what the law is and consequently the conception of law that we formulate have a significant impact on detailed solutions: on the principles of creating law, ways of interpreting it, adjudicating in courts of law, and applying it in various areas of social life by the judiciary and in various areas of social life by public administration bodies. Similarly, the perspective of law may be viewed from a purely formal or realistic perspective. The question of the relation between law and social facts remains a vital question as to the nature of law. It also applies to the discussion of data protection in practice. The meaning of law in books and law in practice is not only a pure reflection of the struggle encountered by the legal scholars while evaluating the applicability of law but also by the addresses of the regulation, namely data controllers, while assessing the risks of potential data infringement.

The need for differentiation between law applied in books and law applied in practice may have been stretched to some extent in earlier times by the idea of law as a creation of humans and fully under people's control, with the implication of effectiveness and achieving goals. In fact, the question of what law we should apply and how is a very old one and refers to concepts such as natural law vs. positive law, the source of truth, and how much law can be adjusted in practice by its application. The Sophists in the fifth century B.C.E. (before Plato and Aristotle) explained these ideals in terms of human reason, claiming that social systems and justice are exclusively the products of human beings. For example, Protagoras observed the difference in

[89] The cases described in U.S., Court of Appeals, New York, *The People Of The State Of New York Ex Rel. William J. Rodgers v. Coler*, 59 N.E. 716,166 N.Y. 1, February 1901.

justice across cities and, as a consequence, observed the impact of humans as creators of the social system in its diversity; this approach was later followed by the late Sophists. They insisted that laws made by rulers should not reject the idea of justice, but they were not, by their very nature, reflections of the natural order. In extreme cases, such as the one illustrated by Sophocles' tragedy Antigone, the two orders may even come into conflict. In this way, the separation of law created by rulers from other forms of social order gave it a special character: state law became a means of influencing people's behavior and an instrument for achieving the set goals. The centuries that followed saw a further strengthening of the concept of the autonomy of the law as produced (or at least acknowledged) and defended by those in power. It was known as positive law, or a law that was in effect here and now as a result of establishment or recognition by legitimate governmental power. The process of increasing the importance of state law was capped by two phenomena: the conviction of the need to write down the basic principles of the state system and citizens' rights in fundamental laws, commonly known as constitutions, and the regulation of selected broad areas of social and economic life in laws known as codes. Going further in the history of the doctrine, realists accuse the former of having an unjustified faith in the causal power of legal texts (law in books, official law). Legal-naturalist concepts criticize the authors for following legal positivism as a speculative search for patterns of law, replacing a theorist, study of the practice of social life[90]. Legal realists naturally oppose the approach of the law in books and its binding power since legal realism on how the law functions in practice.

The second approach, primarily represented by American legal realism, relates to sociological achievements and sees the core of law in human conduct. Representatives of this notion are interested in how the law operates; they want to see the law in action. The substance of the law is communicated in several forms. Despite the fact that realism is acknowledged, one might draw attention to the similarities between realism and positivism. It is essential to acknowledge Oliver W. Holmes while considering American legal realism; one of his publications, *The Common Law*, is considered an originator of the idea of American legal realism and has had a significant effect on legal thinking. Of course, while pointing out similarities between

[90] The matter of legal realism and how it corresponds to the law in books is still widely discussed in modern doctrine. For example, E. Mertz referred to the matter of how the *real world* affects and shapes legal practice and law itself in her writing titled Realism then and now: using the real world to inform formal law, published in: *Research Handbook on Modern Legal Realism*, S. Talesh, E. Mertz, H. Klug (Eds.), Northampton, 2021, pp. 21-36.

American legal realism and positivism, we are not talking about legal positivism, represented by John Austin, but about the positivism of August Comte, assuming that only true knowledge is scientific knowledge, and such knowledge may be acquired only through positive verification theory by means of the empirical scientific method[91]. Of course, pragmatists, including members of Holmes' scientific community, struggled against a number of Comte and his supporters' notions, particularly those that absolutized the truth. Nonetheless, it should be noted that some methodological similarities can be found. Most often, the essence of law is considered to be patterns of behavior revealed in mass, repetitive behavior of people, or decisions of certain individuals, which are considered to have legal significance. Oliver W. Holmes, considered the precursor of this thought, understood law as a prediction of judicial decisions made from the perspective of a *bad guy*, interested in the likelihood of being sanctioned and the amount of the sanction. *Law is what officials, judges, or lawyers do with their affairs*, wrote another American theorist Karl Llewellyn[92]. Holmes, in one of his most prominent works, namely *The Common Law*, he emphasis on the practical and evolving nature of the law. He argued that the law should be understood as a social institution that adapts to the changing needs and values of society. According to Holmes, the law is not a fixed and unchanging set of rules but rather a product of societal forces, customs, and the collective consciousness of the community[93]. A particular variation of it called *social engineering* was formulated by an American, Roscoe Pound, who over 100 years ago wrote his famous piece on law in books and law in action [94]. The politics of law does not explain legal phenomena but is supposed to lead primarily towards proven and effective means of achieving intended ethical or political goals. The idea that stands behind the theory developed by R. Pound is that law should not be seen solely as a collection of abstract rules or principles but rather as a means to bring about social change and promote social welfare. He believed that law should adapt to the changing needs and values of society and be responsive to social, economic, and cultural

[91] These positivistic accents, however, should not obscure the whole picture of The Common Law as a work imbued with the spirit of pragmatism. Holmes was convinced that for centuries, law was a creation arising in practice.

[92] S.N. Verdun-Jones, *The Jurisprudence of Karl Llewellyn*, Dalhousie Law Journal, vol. 1, issue 3, 1973-1974. Retrieved November 11, 2021 from https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1019&context=dlj.

[93] O. W. Holmes, *Common Law*, New York, 1991, pp. 169-170.

[94] R. Pound, *Law in Books and Law in Action*. American Law Review, vol. 44, no. 1, January-February 1910, pp. 12-36.

factors. Every legal act is followed by its practical implementation by the courts and this idea of looking *backward* to see practical examples of how the law was used is the core element distinguishing the perspective concerning just law in books as written down in statutory acts and law in practice as applied by courts. According to R. Pound, society can be controlled by the law. In this way, it succeeds in promoting and protecting the various social interests that surface in society and demand due consideration. The owners of things can be protected from infringement of their property, accident victims can count on adequate compensation, and drivers will know the rules of the road on public roads with, for example, the least risk of collision. The ultimate effect of the work of judges and other public officials will be a reduction in social conflict and increased safety for citizens.

The question of what is the difference between law in books and law in action was finally fully formulated by R. Pound. In 1910, in the *American Law Review,* Pound published an article entitled *The Spirit of the Common Law*. In a footnote to the article, he included the note *Chicago, Illinois,* which referred to the fact that the article was drafted during his career at the University of Chicago. In the theories of R. Pound, the reader can obviously see the dichotomy of legal perspectives as divided into law in books and law in practice. To better understand the meaning of the article, it is worth asking the question: what part of legal science does Pound attempt to improve? In this article, Pound directly referred to the theories of Ronald Dworkin and the understanding of law as a novel that is written by many book writers and then interpreted by others according to the need[95]. To identify the other chapter of law that Pound alluded to and strove to enhance, we must go back to 1887 and the theories of C.C. Langdell, who expressed two major ideas that Pound further recalled, namely that:

- law is a science,
- all materials and sources of this science can be found in the printed books[96].

Based on this approach, Langdell formulated his famous theory that the library is the same for legal students as the laboratory is for students of chemistry or physics.[97] Pound agrees with C.C. Langdell when it comes to the first remark about the law as a science; nevertheless, the part of legal doctrine where Pound is looking for adjustments is related to the second claim

[95] R. Dworkin, *Imperium Prawa,* Warszawa, 2006, p. 231.

[96] W. Twinning, *Karl Llewellyn and the Realist Movement,* Second Edition, Cambridge, 2012, p. 11.

[97] *Ibid*., p. 12.

made by Langdell. According to Pound, students cannot focus only on the law in books, as real legal science requires them to see the law in action as well. To show how incomplete the picture of law in books is without law in action, Pound quotes Mark Twain's infamous book regarding the adventures of Huckleberry Finn. In particular, Pound made reference to the part of the book relating how Thomas and Huck assisted Jim, who was captured by the judge, to escape to the states where slavery was no longer legal. The judge, as presented by Twain, was going to give the boy who escaped from slavery to the slaves' hunters. Pound's quote at the beginning of his article is an allegory of the law that, under the cover of right interests, brings a result that is different from the true word, evil and unjust. Sawyer represents an individual who is educated and civilized but also strongly attached to the written law and order. He applies what can be found in books directly, and this leads him to the idea of digging the escape road in the least efficient way but also in the way known from the books he appreciated so much. Consequently, instead of modifying the rules as presented in books, Sawyer decides to blindly follow what is written down. This metaphor mirrors the experience of Pound with the US judges[98]. According to Pound's beliefs, this reluctance to amend the law stems from lawmakers and judges' unwillingness to accept a mistake or the necessity to reform anything.

Pound was deeply touched by coincidences he saw in the approach to thinking characteristics of illiterate tribes and modern works of legal scholars as well as judges. He believed that the resistance to any changes in the law was mostly rooted in the conservatism that is visible in both the education system and legal reasoning. Pound also referred to the fact that literature regarding the legal doctrine and applicability of law is mostly of an analytic and historic character, while the merits and interpretation of law begin and ended with Anglo-American jurisdiction. The phenomenon observed by Pound is the resistance of judges to be more progressive and modern and, as a consequence, to at least delay the speed of any legal changes. A similar approach was represented by A. de Tocqueville, also quoted by Pound[99]. At the time, lawyers were mostly belonging to social classes directly interested in maintaining the *status quo,* and thanks to the XIV Amendment to the US Constitution, lawyers gained the most influential legal ground in the history of US jurisprudence in order to defend their otherwise

[98] An example from the life of Pound that is similar to the approach taken by Sawyer comes from the Supreme Court of the State Nebraska. According to his experience, judges prefer to manipulate the law than change it.

[99] R. Pound, *op. cit.*, p. 25.

conservative approach.[100] Pound's approach to legal conservatism was clear: the law needs to change to fit its purpose and serve its purpose. The law should be changed to fit reality, and going in the direction of covering potential gaps in application or outdated legal regulations is harmful and should not take place. He also often refers to the matter of social justice and the chasm between social justice and legal rules[101]. The bridge to cross this chasm is the rational law drafting and its application through the prism of a need for social, economic, and political reasons.[102] To the list as presented by Pound, I would suggest adding technology, which, to some extent, dictates the rationale behind both economic and social order today. In his earlier speeches, Pound referred to a direct manner to extend the role of judges, he also highlighted that, in his opinion, the role of the jury was not fully serving its aim[103]. Pound often referred to his disappointment with how slow the law is when it comes to the changes that happen in real life, and, to some extent, he sees the cure for this clash in the independence of judges and a non-conservative approach. Pound raises a very important matter of how the law may catch up, how it will react to the implementation difficulties, and most importantly, who will be responsible for adjusting the law towards reality.

To some extent, the dichotomy between acts and practical implementation, or the impact on how legal acts are being interpreted in practice, was also discussed by H. Kelsen or H. L. A. Hart when it comes to the matter of law and facts. For Kelsen, positive law is the only true law; as a consequence of this assumption, Kelsen believed that all other versions of the law are imagined and therefore either pure ideology or nonsense.[104] In general, Kelsen, in his legal writings, referred to the concept of normativity and the legality of the law as the biggest challenge to achieve. As a consequence of his research, he came to the conclusion that legal rules are not essential principles to be found by reasoning about a natural order but are instead

[100] G. Wierczyński, *Pound*, Sopot, 2018, p. 100.

[101] R. Pound, *opt. cit*., p. 26.

[102] *Ibid*., p. 35.

[103] Pound reflected this view in, among others in: R. Pound, *Mechanical Jurisprudence*, Columbia Law Review, vol. 8, no. 8, 1908, pp. 605–623. Retrieved April 17, 2023 from https://www.jstor.org/stable/1108954 .

[104] J. L. Halperin, *Law in Books and Law in Action: The Problem of Legal Change*, Meine Law Review vol. 64, no. 1, 2011, pp. 48, Retrieved November 21, 2021 from https://digitalcommons.mainelaw.maine.edu/mlr/vol64/iss1/4.

human artifacts imposed by human actions.[105] At the same time, Kelsen considered the law to be a construction made of rules conceived as hypothetical norms. He often referred to the higher value norms and implied presumption of primacy of the Constitution as the ultimate and the most important legal norms. According to the *basic norm principle*, there is always a norm that validates the prior one, as a consequence, Kelsen believed in the system of authorization that logically needs to expire because there is a norm that is not validated by any other means. This phenomenon of the final, not authorized norm was famously argued by Kelsen in regard to the presupposed legal validity of the basic norm.[106] When it comes to the *living law* perspective as observed by Pound, Kelsen views the practice as strongly political[107]. In general, the matter of an historical approach to law and the impact of what is called in Europe a *doctrine* was difficult for Kelsen. Of course, Kelsen does not deny the social dimension of law, but he believes that the law in its pure and right manner shall be understood as a normative set of rules that arise from the legal reasoning and not from custom or socially affected practice. From the 1920s to

[105] H. Kelsen, *General Theory of Law and State*, A. Wedberg (Transl.), Clark 2011. Originally published: Harvard University Press, 1945.

[106] *Ibid*., pp. 110-111.

[107] Both Roscoe Pound and Hans Kelsen, influential legal theorists of their time, had distinct perspectives on the concept of living law. Pound's notion of living law emphasized the dynamic and evolving nature of the legal system. He argued that law should adapt to social changes and address the needs of society to maintain social order and justice. According to Pound, law is not static or fixed but rather a reflection of social forces and the changing conditions of human life. He advocated for the study of the social impact of legal rules and institutions to ensure that the law effectively serves the interests of the community. Pound's living law perspective aligns with his broader concept of sociological jurisprudence, which emphasizes the social function and purpose of law. Pound's notion of *living law* differs from Hans Kelsen's.

Kelsen was more concerned with the legal system's internal coherence and consistency than with its adaptability to societal developments. The "living" feature of law, according to Kelsen, refers to its continued validity and applicability within a legal system. He contended that the law is a hierarchical structure of norms, with each standard derived from a higher norm. Legal norms' validity is determined by their conformity with higher standards in the legal hierarchy. *Living law* develops from the continual application and interpretation of legal standards by courts and legal institutions, assuring the legal system's ongoing functionality and stability. While both Pound and Kelsen understood the necessity of the law's flexibility, their approaches and focus differed. Pound stressed the social influence of the law and its response to society requirements, whereas Kelsen emphasized the internal consistency and continuing validity of legal principles within a hierarchical framework.

the beginning of the 1960s (at the time of the second edition of *Reine Rechtslehre*[108]), Kelsen considered that *norms created and applied within the framework of a legal system have the character of legal norms only if legal science ascribes this character to them*[109]. Consequently, legal norms as described by Kelsen are constructions of legal science, and law can be captured only in books. Thus, it remains important to notice that there is the dichotomy of law in books and law in action through the recognition of the preferred and right form of law, namely law in books. In Kelsen's *General Theory of Law and State*, the author repeats that *the contents of positive law can be uniquely ascertained by an objective method*. The existence of the value of law is conditioned by objectively verifiable facts.[110]

In opposition to the perspective that the correctness of law relies fully on books, one need look no further than the teachings of Richard Posner, a federal appeals court judge and a professor at the University of Chicago who initiated research related to the economic analysis of law. In his famous exit interview, he stated that *[...] a case is just a dispute. The first thing you do is ask yourself — forget about the law — what is a sensible resolution of this dispute?*.[111] This approach clearly shows that, according to Posner's perspective, what matters is a practical evaluation and individual application of law and from a context of its role in the real actual world in habited by the actual matter at issue before the court. Consequently, one would be forgiven to conclude a potentially harsh clash of opinion(s) between the previously presented Kelsen and latter noted Posner, especially when it comes to the source of legal regulation *that*

[108] Pure legal theory (*Reine Rechtslehre)* is a variation of legal positivism developed by Hans Kelsen. It is a theory of positive law of an absolute character, i.e. positive law. In other words, it claims that it can be applied to any (positive) legal system ever established by humans, and therefore constitutes a *general theory of law*.

[109] H. Kelsen, *opt.cit.*, p. 49.

[110] In H. Kelsen, *Pure Theory of Law*, M. Knight (Transl.), 2nd print., Berkeley 1970, pp. 217-218, Kelsen states that: *The Pure Theory describes the positive law as an* ***objectively valid order*** *and states that this interpretation is possible only under the condition that a basic norm is presupposed…. The Pure Theory, thereby characterizes this interpretation as possible, not necessary, and presents the objective validity of positive law only as conditional—namely conditioned by the presupposed basic norm.* It is clearly visible that Kelsen referred to the possibility of interpretation and viewing the normative law through the lenses of practice, but such an approach is optional, not mandatory.

[111] Quote by Judge R. Posner in the New York Times article where he discussed his perspective on codified rules of law from the perspective of his career. A. Liptak, *An Exit Interview With Richard Posner, Judicial Provocateur*, New York Times 2017, vol. 11, September 12, p. A18. Retrieved November 28, 2021 from https://www.nytimes.com/2017/09/11/us/politics/judge-richard-posner-retirement.html.

matters. A reliably constant is change and in order to maintain its relevance, the law must keep pace with the constant change. The world changes, in the area of social science as well as technology and the reality to which the law shall be applied changes as well; this statement is objective. Today, we live in an era of unforeseeable change arising largely out of pure technological growth along with its knock-off effects on modern societies. New technologies often bring into question the validity of the most powerful ideas upon which humankind has stood upon and otherwise known until now.[112] Consequently and arguably, the issues raised by discussed thinkers have never been more relevant and current as they are today.

2. Lon Fuller and the idea of the morality of law.

[A] law which a man cannot obey, nor act accordingly to it, is void and no law: and this is impossible to obey contradictions or act according to them – Fuller's chapter *The morality that makes law possible* in the *Morality of Law* starts with this quote.[113] This quote simply and purely indicates that the law shall be considered operating as long as it stands in line with what Fuller defines as *morality*. Where legislation stands far away from the practical execution of rules, legislation may nonetheless bring up an impossibility of observance of law as and within the context of a challenge for and to its citizens. Technological growth was always one of the factors that affected consequences in law and society, and in fact, in almost every area of law, in up-to-date internet development, it seems obvious that the impact on privacy caused by the technology will emerge.[114] The development of the Internet of Things (IoT), growth of computer-based and communication technology, and the associated importance of data exchange which has resulted therefrom, has led legislative history of the European Union to the Commission's GDPR proposal. On May 15, 2003, the inquiry of the Directorate General of

[112] One of the real use cases of such challenges is the privacy among internet intermediaries and the growth of the General Data Protection Regulation.

[113] L. L. Fuller, *The morality of Law.* Revised edition, London, 1963, p. 33.

[114] It is worth noticing that In the late 90s Manuel Castells (Spanish sociologist, writer and academic) analyzed a shift from industrial, modern, societies to informational societies, which, according to his analysis, began in the 1970s. In Castells trilogy named *The Information Age: Economy, Society, and Culture* (published 1996, 1997, 1998), he describes current societies as being centered around networks instead of individual actors and as working through a constant flow of information through technology.

the Commission for the Internal Market was published in the form of a first report on the implementation of the Data Protection Directive 95/46/EC. Nevertheless, beforehand, there were a number of national legislation attempts referring to the matter of privacy, such as, for example, the legislative movement in Hesse, Germany, where the first modern data privacy law came into being in reaction to concerns about computing advancements and privacy in the processing of personal data. Afterward, Swedish jurisprudence decided to enact the first national privacy law called the Data Act, which criminalized data theft and granted those subject to data freedom to access their respective data records. In 1978, the German Federal Data Protection Act established basic data protection standards, such as the requirement of consent for the processing of personal data. As an outcome, during the late 1970s, many EU member states incorporated data protection laws as fundamental rights into their legislation. As a consequence of legislative growth at the time, the General Data Protection Regulation (GDPR) came into force.

Legislative growth in the area of privacy of personal data may be compared, to some extent, to an explosion that created a massive number of legal instruments to race against technological growth. In this regard, the question that should be asked refers to the idea of the effectiveness of the law, taking into account the growth of legal documents regulating this area. In fact, the question was already asked in the past by Lon Fuller, who questioned the morality of law.[115] The word *morality* itself may be misleading in how we understand it now. The key element to which Fuller referred to was asking about how a legislator can guide society? In his book, *The Morality of Law*, Fuller focuses on the legislative perspective and shares the story of a fictitious King Rex who failed to produce any laws despite eight serious attempts at doing the same. The author uses the figure of King Rex as an illustration to show how a legislator can fail in at least eight ways to arrive a law production via, for example, producing no general laws at all,

[115] Fuller was well known for his discussion with L.A Hart, as Fuller represents the non-positivist approach towards law. In fact, his approach may seem counterintuitive to the civil law lawyers as he focuses on how the law is made not on the final product, namely legal act. His wide discussion with Hart finds its depiction among others in the following pieces of writing H.L.A. Hart, *Positivism and the Separation of Law and Morals* (1958) 71 Harvard Law Review 593; Fuller's reply in the same issue *Positivism and Fidelity to Law. A Reply to Professor Hart* (1958) 71 Harvard Law Review 630; the publication of Hart's book The Concept of Law (Oxford: Clarendon 1961, 3rd edition 2012); Fuller's book The Morality of Law in 1964; Hart's book review of The Morality of Law in (1965) 78 Harvard Law Review 1281; it was concluded with Fuller's "Reply to Critics" added to The Morality of Law in 1969. On this debate, see *The Hart-Fuller Debate in the Twenty-First Century*, P. Cane (Ed.), Oxford 2010.

keeping laws secret, or making unclear and inconsistent laws. From such failures, Fuller derives an internal morality of law, consisting of eight principles or demands that legislators should meet in order to produce law at all, namely:

- law should be general,
- law should be published,
- law should be non-retroactive,
- law should be clear,
- law should be non-contradictory,
- law should not require the impossible,
- law should be constant through time (stability), and
- there should be congruence between official action and the declared rules. [116]

King Rex, as a ruler, came with the reformer's approach and was considered one of the biggest failures of his successors in the area of law. The list presented above in fact refers to the list of failures faced by King Rex, where he personally experienced his limitations that affected him as a lawgiver or judge[117]. Awareness of the law, its predictability, and its clear function remain within the scope of what King Rex experienced[118]. According to Fuller, the lawgiver must respect these principles. In order to make a law that can act as guidance to those subject to it, the lawgiver must respect the eight principles of legality; otherwise, the lawgiver will simply fail to draft a law that can effective guide behavior and as such be an effective law.

What happens once there is a failure at the stage of any of the above-listed eight elements of law? In fact, Fuller addresses this question by stating that: *[A] total failure in any one of these eight directions does not simply result in a bad system of law; it result in something that is not properly called a legal system at all, except perhaps in the Pickwickian sense in which void contract can still be said to be one kind of contract. Certainly there can be no rational ground*

[116] L. L. Fuller, *opt. cit.*, pp. 39-94.

[117] *Ibid.* p.33-34.

[118] As Fuller describes *To Rex's surprise this sensible plan was deeply resented by his subjects. They declared it was very unpleasant to have one's case decided by rules when there was no way of knowing what those rules were*. As the outcome of multiple experiences of Rex, Fuller conveys an important message – law shall be reliable, and subjects of such law shall have the possibility to rely on it; L. L. Fuller, *op.cit.*, p. 34.

for asserting that a man can have a moral obligation to obey a legal rule that does not exist […].[119]

Fuller dedicates its morality of law to defining what stands as a right law to obey. Of course, his concept of morality remains complex, and in his writing, he refers to the idea of what is good and moral, and what is possible for the legislator to distinguish.[120]. He seeks perfection in legality and finds a solid basis for such perfection in the clarity and reliability of the law. Of course, there are a lot of high expectations in the perspective on law taken by Fuller; nevertheless, similarly to Pound, he seeks out what can be executed in practice and what may remain only in the formal state of law due to its weaknesses and flaws. In fact, Fuller raises a question that should be currently asked in light of new data protection legislation, namely, is it possible to rely on such a law? Is it actually possible for the data controller to relay and foresee his or her obligations regarding data processing? Would it be practically possible to execute the data controller's obligation while functioning in the world of market monopolists that own essential parts of network access, infrastructure, and/or software solutions? Indeed, the analysis made by Fuller refers to the subject as being distinct in its practical scope but for the questions asked by him being still present and not to be forgotten with the purpose of making law reliable for the subject of the regulation.[121] Fuller pays much attention to the practical elements of law; for example, he quotes Prof. Friedmann, who attempted to offer a neutral definition of law with no substantive justice idea included. Fuller to some extent understands this approach but points to the situation where society is ruled by lawless terror and that, in fact, it may be ruled according to legal regulations as well, what means that sometimes the rulings that seem not to fulfil the standard of what is law may be formally implemented in a proper way.[122] Consequently, what is important for each and every legal system to be moral and, going even

[119] L. L. Fuller, *opt.cit.,* p. 39.

[120] L. L. Fuller, *opt.cit.,* p. 7. Fuller refers to the concept of distinguishing whether gambling shall be prohibited by law and morally wrong and how the lawmaker shall distinguish between harmful form of gambling and innocent actions. How to draw a line between the game that is partially dependent on skills and partially on luck against the game that harmfully overuses the player's faith in happy ending.

[121] Fuller offers what he concluded to be *the only formula that may be called a definition of law offered [in this chapter]*. In the *Morality of Law*, chapter *The concept of law* he states that *law is the enterprise of subjecting human conduct to the governance of rules. Unlike most modern theories of law, this view treats law as an activity and regards a legal system as the product of sustained purposive effort*.

[122] L. L. Fuller, *opt.cit,* p.106-107.

further, functioning and justified, is for the legal system to work in practice and otherwise carry with it a practical legal effect.

3. The concept of the *bad guy* envisaged Karl Llewellyn.

As an outcome of technological growth is the instigation of an ever faster and more responsive build-up of legal norms, there is no doubt that, by the inclusion of non-normative instruments in the domain of jurisprudence, the classic understanding of how law works slightly switches. In fact, this approach is a move towards the idea of law as an instrument of channeling human actions. Supporting a shift in focus from *law* to *regulation* might encounter potential obstacles, but, at least, mainstream regulatory theorists conceive of regulation as starting with the setting of standards and, thus, as normative. If the *regulatory environment* adopted this conception of *regulation*, it would still be limited to normative signals, and as a consequence, many jurists might find comfort with the aforementioned[123]. However, the comfort of jurists is not the fundamental element in question or a desired or expected outcome. Rather, our cognitive interest is directed towards the practical outcome of what effect particular elements of law bring in a practical dimension. In fact, this approach is quite different from the traditional legal approach and legal mentality, but the function of channeling human conduct in the field of law theory which was introduced by Karl Llewellyn in his theory about *law jobs*[124]. Llewellyn, as a representative of legal realism, claims that the law is a means to a social goal. The law is what officials, judges, or lawyers decide in their cases, but it is not limited to this when it comes to the purpose of its existence. Consequently, laws are any norms regulating group and/or societal behavior. Such norms are not limited just to the codified written language but also possess their own sociological and psychological approach to law. Llewellyn studied what is the law and not what it should be in an ideal world. He further examines how the law is implemented. Social interest theory holds that the purpose of the law is to achieve a balance between conflicting interests in society. It examines how the law works from the perspective of predetermined goals. According to the representatives of the school of thoughts where Llewellyn belongs, the

[123] R. Brownsword, *Law, Technology and Society. Re-imagining the regulatory environment*, New York, 2019, p. 26.

[124] K. N. Llewellyn, *The Normative, the Legal, and the Law-Jobs: The Problem of Juristic Method*. The Yale Law Journal 1940, vol. 49, no. 8, pp. 1355. Retrieved April 17, 2023 from https://www.jstor.org/stable/792545.

lawyer plays the role of a social engineer, namely, that of leading to a compromising and practical implementation of the law.

Most often, the essence of law is considered to be patterns of behavior revealed in mass, repetitive behavior of people, or decisions of certain individuals, which are considered to have legal significance. Oliver W. Holmes, considered the precursor of this thought, understood law as a prediction of judicial decisions made from the perspective of a *bad guy* interested in the likelihood of being sanctioned and the amount of the sanction. In *The Path of the Law,* O. W. Holmes depicted the idea of a *bad guy* that was further used by Llewellyn as follows:

> *But if we take the view of our friend, the bad man, we shall find that he does not care two straws for the axioms or deductions, but that he does want to know what the Massachusetts or English courts are likely to do in fact. I am much of his mind. The prophecies of what the courts will do in fact, and nothing more pretentious, are what I mean by the law.*[125]

This quote puts an important emphasis on a crucial element of the law, namely predictability. The bad guy or bad man, as referred to by Holmes, wishes to be able to foresee the outcome of his actions. There is no place in law for unpredictable holdings, outcomes and/or repercussions to the bad guy or bad man behavior. The above quote neatly provides an incredibly important dynamic into the movement and thinking of legal realists by placing a spotlight on the fact that one needs to actually analyze the behaviors and decisions of courts instead of theorizing about the ultimate source of law. This initial approach, as presented by Holmes, was taken a step further by Llewellyn, who, as detailed above, further developed the theory of the *bad man:*

> *The people who have the doing in charge, whether they be judges or sheriffs or clerks or jailers or lawyers, are officials of the law. What these officials do about disputes is, to my mind, the law itself.*[126]

Here Llewellyn extends the ideas previously quoted by Holmes into the practice and application of law, not only by judges, but also by others tasked with such things, so that the aforementioned may truly stand for what is understood to be the law. Consequently, law may be thought of as a living organism, a being that must be observed to be understood, such

[125] *Ead., op.cit.,* pp. 172-173.

[126] K. N. Llewellyn, *The Bramble Bush: some lectures on law and its study*. New York, [1930], 1951. As cited in A. K.Mehrotra, *Law and the "Other": Karl N. Llewellyn, cultural anthropology, and the legacy of The Cheyenne Way*. Law & Social Inquiry 2001, vol. 26, no. 3, p. 749.

requiring analysis of practical application. A focus of Llewellyn was to distinguish the real rules from the paper rules.[127] An approach that focuses on the practical rules instead of formal constructions was also highlighted by other thinkers such as Felix Cohen. Nonetheless, the focus of Llewellyn remains remarkably on point to the subject being discussed.[128] The idea of a *bad man* both in the case of Llewellyn and Holmes goes to the trust in the understanding of what is law that the law should stand as the last-resort decision upon which to rely. On the other hand, the idea of the *bad man* cynically highlights that in practice we are all mostly interested in the actual and predictable result and consequence of violating a law – this approach was obvious even for someone who, as a judge, was in the position to affect the law himself. This question was further developed into the idea of the accountability of judges by Aranio and Peczenik as within the theory of legal argumentation. In their view, the binding character of the law comes from the potential accountability of breaking the rules that stands upon a judge presiding over a case[129]. At the end, all people engaged in the process of legal decision-making should be interested in the scope and reliability of the law itself.

The idea of being able to rely on the law, foresee its course, and stand in a position of a person only interested in consequences, remains important for modern data protection laws. One can firmly state that an ordinary data controller will stand in the shoes of the *bad guy* focusing only on the consequences. It is mostly due to the subject matter being regulated by data protection and privacy laws. The GDPR focused on the regulation of the processing of personal data, and that happened at a time when data exchange is one of the most powerful tools known in the world. It is also necessary to run any business activity, and with the current Internet intermediary's services, data about individuals stands as powerful marketing leverage. Consequently, in the beginning, we may assume that the data controller, mostly in need of

[127] H. D. Lasswell, M. Macdougal, *Jurisprudence for a Free Society: Studies in Law, Science, and Policy*, New Haven, 1992, p. 60.

[128] Cohen discussed the functional approach to the law and its ethical dimension. According to his thought, when we recognize legal rules as the equivalent of formulas describing the uniformity of judicial decisions, the legal concepts become more similar to any other patterns. With such an approach, it becomes visible that judicial decisions are not the product of logic thanks to pre-existing norms and rules but are social events more directed towards the standard of human values. This perspective contrasts with the idea of the *prediction theory of law* as developed by Llewellyn and Holmes.

[129] R. Siltala, *Law, Truth, and Reason: A Treatise on Legal Argumentation*, 11th Edition. Dordrecht ; New York 2011, pp. 102-104.

shaping his or her responsibilities and conducting risk assessments, will be the person evaluating what, in practice, will be held by the court. In the scope of law, attempting to regulate one of the most growing branches of market foreseeability and looking at its practical implementation is, in fact, what is the law.

Gray, in his much-publicized work *The Nature and Sources of the Law*, drew a distinction between law in the strict sense, which he understood to mean the actual actions of courts, and sources of law, which can serve as the basis for decisions.[130] In the latter category, he included both statutes and precedents, legal custom, expert opinion, and morality, under which he also understood the principles of policy.[131] In this regard, Gray rejected the positions formulated by some legal theoreticians, according to which common law is characterized by a lower level of legal certainty than civil law and definitions arising from case law are not very precise.[132] He pointed out that the decisions formulated on the basis of state law are, as a rule, not completely accurate and only take on a fully clear dimension in the context of subsequent judicial decisions. Gray's theories and views find further support and evaluation in the works of Justice Holmes, who is believed to be the first great critic of US jurisprudence formalism[133]. The views presented by Holmes that find relevance to the below-mentioned Judge Posner may be summarized in the following highlights:

- Criticism of the deductive model of law application: according to his views, the main and crucial value of law is not logic but practical experience and application in real life.

- Law as a prediction about the court's behavior, also known as the prediction theory of law, refers to the predictability of law and the understanding of law as a prophecy of what shall happen. The obligation to act in a certain way was, according to Holmes,

[130] J. C. Gray, The Nature and Sources of the Law, ed. R. Gray, New York, 1948, pp. 123-125. Retrieved April 17, 2023 from https://ia600207.us.archive.org/2/items/cu31924017092846/cu31924017092846.pdf.

[131] In one part of his work great work titled "The Nature and Sources of the Law", Gray clearly outlined the boundary between the judge and the discoverer in the field of natural sciences. While the former identifies laws whose content is independent of him, the judge, by simply making a decision, influences the content of the law.

[132] J. C. Gray, *opt.cit.*, pp. 3-4.

[133] Despite Justice Holmes' clear inspiration from the philosophy of pragmatism and his rather clear-cut break from the tradition of American formalism of the laws of nothing and the model of legal certainty based on infallible logical reasoning, there is no consensus in the American literature about which current in jurisprudence Holmes was closest to as a judge.

nothing more than a prophecy of how the person could act, and the *bad guy* focuses only on the consequence.

- A model of empirical legal science: the basis for formulating predictions Holmes formulated a postulate for the reconstruction of the science of law, which, in his opinion, should undergo a process similar to that of other fields of science and be based on empirical premises.

- Case method model: Holmes defines precedence and case-based law as crucial elements of law in general. He further refers to the stability of the law and the associated predictability of judicial decisions as values that judges should take into account in their decision-making process.

The idea of predictability in the law and how a person should be able to rely on it was also discussed by Judge Posner. The question of how the law is made and the fact that law is not logic but experience are two of the key elements of discussion about the role and meaning of law among pragmatics. Judge Posner has, at least in some places, given a clear articulation of the instrumentalist view and a further pragmatic approach to the understanding of what is the law. Posner has stressed, for instance, a comparison of the relative futility of reasoning about *ends* as compared to a means. Posner sees the law as a tool grounded in science and, further, as a *tool for copying*. According to Posner, judges escape from difficult questions and legal matters in a variety of ways. The main way is to escape into formalism or so-called instrumentalism, that is, to pretend that cases can be resolved on a semantic and logical level. By resorting to formalism, judges themselves complicate the law in an unnecessary way. Expansive arguments full of legal terms and quotations only mask the intellectual deficiencies of lawyers. Of course, this doesn't apply to all judges. In addition to the formalist judges, there are also realist judges. A realist judge tries to understand the context of each case and the purpose of the rules. Posner also grounds his instrumentalist view on the same sorts of considerations that motivate the explanatory critique. He embraces a naturalistic, Darwinian picture of the world, in which human nature is the product of homo sapiens' success in the process of natural selection.[134] In his book *How Judges Think*, Posner raises two matters of judges' presence in jurisprudence, namely:

[134] C. L. Barzun, *Three forms of Legal Pragmatism*, Washington University Law Review 2018, vol. 95, no. 5, pp. 1023. Retrieved April 17, 2023 from https://openscholarship.wustl.edu/law_lawreview/vol95/iss5/5/.

- judges as labor-market participants, and
- judges as occasional legislators.

Both of those critical statements, as quoted above, view judges as non-objective, privileged participants in the legal process. In his writing, Posner depicts the idea of the role of judges nowadays: their work remains a demanded competence on the market as well as an important political tool that is used and played by a country's governing administrations.[135] According to Posner, there is a hypothesis of mystically motivated judge who always attempts to be only a good worker who imposes a challenge on the whole construction of the system itself [136]. Posner, in a rather dissatisfied tone, insists on the regularity of legal needs. Similar to the idea of judges as sometime legislators, Posner addresses the topic of when judges can and cannot decide, and comes to the conclusion that even their mandatory obligation to decide is constrained by legislative constraints that limit the scope of decision making.[137]. In general, R. A. Posner, as a judge, focuses on the question of how day-to-day judicial decision-making should be constructed. In his retirement speech, he firmly stated that he was proud to be a supporter of legal pragmatism. In fact, what remains most important for Posner is that political and judicial decisions should be guided by social needs and respond to the day-to-day issues that need to be managed. From his perspective, it was more about being pragmatic in everyday life than worrying about abstract issues that may or may not arise. In his opinion, judicial decisions should be a combination of pragmatism and the observance of a limited understanding of democracy rather than sticking closely to formalist theories of adjudication. The theories of Judge Posner were also criticized as being too narrow and, at the same time, too broad.[138]

[135] R. A. Posner, *How Judges Think*, Cambridge, 2008, p. 40.

[136] *Ibid*. p. 42.

[137] In *How Judges Think*, Posner refers to the obligation of judges to almost always be in a position of decision-makers with only an exclusion of political question doctrine and some administrative decisions that are taken away from the scope of judges' decision-making; *ibid*., pp. 53-55.

[138] Among others a criticism of *Law, Pragmatism and Democracy* wrote by Posner to which R.A Posner further responded was made by Ilya Somin. At the Washington Post in the article *Thoughts on Judge Richard Posner's legal pragmatism* Somin refers to the *too broad and too narrow* perspective of Posner on pragmatism. (The Washington Post, September 2, 2017. Retrieved April 17, 2023 from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/09/02/thoughts-on-judge-richard-posners-legal-pragmatism/).

Currently, with respect to the fallacies of predictions, this author respectfully submits that there is no one discovered and confirmed way of managing privacy issues and data protection laws that will survive the technological growth and pressure made by market monopolists in the various fields encompassed by the overarching term *technolog*. The idea standing behind the GDPR seems to be right, but at the same time, it seems to be what Judge Posner would qualify as formalistic. On both sides, the challenge of individuals to control their data as well as on the side of data controllers to meet the requirements, from which, time to time, seem to be designed to only spot the narrow issue empathized by the presence of big market players, is, in fact, what seems to have been missing since the 2018 GDPR implementation of what Judge Posner would call observing real-life, every-day problems and solving them by judges or by law. In his response to Somin's criticism, Posner wrote:

> *While pragmatism cannot resolve deep normative disagreements, it can, as a technique of judicial reasoning, at once resolve satisfactorily the majority of cases that do not involve such disagreements, while protecting democracy from overweening judicial assertiveness.*[139]

As quoted above, Posner firmly states that pragmatism is not a ready-to-use solution for every issue with which modern democracies struggle. It nevertheless remains an important tool to guide a judge through the decision-making process and assess how the law is to be applied in practice.

[139] R. A. Posner, *Law, pragmatism, and democracy: Reply to Somin*, Critical Review, vol. 16, no. 4, 2008, pp. 465-471. Retrieved June 5, 2022 from https://doi.org/10.1080/08913810408443620.

Chapter II: Individual rights derived from the General Data Protection Regulation.

A. Rights included in the General Data Protection Regulation.

The enactment of the General Data Protection Regulation (GDPR) remains one of the most important events in the recent history of data safety. Indeed, the European Parliament offered a solution that introduces a procedure to apply in all individual cases according to the consistency of European mechanisms[140]. It was obvious that access to information in the global age of technological growth, data mining, and AI big data is beyond the control of legal instruments. The world's legal systems are facing some serious challenges as a result of the rapid advancement of technology, and the right to be forgotten is one such right that has received particular attention.[141] Since 2010, regulating data security within the EU has been one of the most important priorities and needs for the EU, and growing tensions around mass data processing have only increased the need.[142] Contrary to the notice-and-consent model present under US jurisdiction, European law focused on individual rights and the accessibility of legal remedies in the case of data safety breach.[143] The European Union decided to face this challenge in the form of a regulation legitimized by Article 16(2) of the TFEU Europe, wherein the EU selected a means that aims to bring control over data to individuals understood as data subjects.[144] As quoted below, recital 12 of the General Data Protection Regulation directly refers to the mentioned article of the Treaty:

> *Article 16(2) of the TFEU mandates the European Parliament and the Council to lay down the rules relating to the **protection of natural persons** with regard to the*

[140] O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford, 2016, p. 69.

[141] G. Frosio, *Oxford Handbook of Online Intermediary Liability*, Oxford, 2020, p. 487.

[142] Some special impact was made by the right to be forgotten and the *Google Spain* case (CJEU, Request for a preliminary ruling from the Audiencia Nacional — Spain, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12, May 2014, ECLI:EU:C:2014:317.). Even though the right to be forgotten did not make it to the final stage of GDPR in the form known from the Google Spain case, it is still an important element of data processing regulation.

[143] S. Sharma, *Data Privacy and GDPR Handbook*, Hoboken, 2020, p. 12.

[144] See European Commission Communication, *A comprehensive approach on a personal data protection in the European Union*, COM (2010) 609 final.

processing of personal data and the rules relating to the free movement of personal data.[145]

The formulation of what is said above brings up one important notion that remains a vital element of all this Regulation, namely the *protection of natural persons*. It should be noted that such an approach strongly affects the practical implementation of this act. It also teaches us the meaning of what constitutes personal data. Before analyzing the scope of rights protected under the GDPR, it is worth mentioning that during the analysis of this text, a broad and conditional understanding of this act should be applied. By *personal data*, one should understand any data that leads toward a natural person. The meaning of what we classify as personal information will be conditional on circumstances and impact based on risk assessment, but according to the underpinning values of the GDPR, the controller should always assume a high standard for data safety measures. Furthermore, the GDPR laid down basic principles concerning data processing precisely within the spirit of Article 1 defining the scope of Regulation, Article 4 implying the scope, and Article 14 further defining it[146]. Such principles may be traced back to the following rights belonging to any individual:

- The right to be informed (Article 12);
- The right of access (Articles 12-15 and Recitals 59 and 63);
- The right to rectification (Article 16 and Recital 65);
- The right to erasure (Article 17, Recitals 65 and 66);
- The right to restrict processing (Article 18 and Recital 67);
- The right to data portability (Article 20 and Recital 68);
- The right to object (Article 21 and Recitals 68-70);
- Rights concerning automated decision making and profiling (Article 21).

[145] General Data Protection Regulation, rec. 12.

[146] M. Krzysztofek, GDPR: *General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union*, European Monographs, Wolters Kluwer, 2018, pp. Chapter 1.
M. Krzysztofek, *Subject Matter and Objectives of the GDPR and the Nature of Changes Introduced By It; Direct Applicability of the GDPR; The Right to Protection of Personal Data as a Fundamental Right; The Context of Personal Data Protection in the European Union; International Models of Personal Data Protection; Update of the Council of Europe Convention No. 108* [In:] *ead., GDPR: General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union,* Alphen aan den Rijn, 2019. Retrieved April 17, 2023 from https://books.google.pl/books?id=Uo6WDwAAQBAJ&pg=PT9&hl=pl&source=gbs_selected_pages&cad=2#v=onepage&q&f=false.

The above-listed catalog of rights is directly implied by the GDPR within the scope of articles or recitals. The GDPR includes several key rights that are grounded in the right to privacy, including the right to be informed, the right to access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights concerning automated decision making and profiling. These rights are essential to protecting individuals against unlawful interference with their personal data. However, it is important to note that these rights are not absolute and may be subject to certain limitations. Despite this, the GDPR represents a significant step forward in protecting individuals' privacy rights in the digital age.

The right to privacy and protection against unlawful processing of personal data have been recognized in a number of jurisdictions, and the European approach to protecting individual rights in this regard has become a commonly-shared value. Several other jurisdictions have enacted data protection laws that aim to protect individuals' privacy rights. For example, the California Consumer Privacy Act (CCPA) in the United States provides California residents with the right to know what personal information businesses collect about them and the right to request that their personal information be deleted. The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada regulates the collection, use, and disclosure of personal information by businesses and government organizations. In Australia, the Privacy Act 1988 regulates the handling of personal information by government agencies and businesses. These acts share common values with the GDPR in seeking to protect individuals' privacy rights and placing obligations on organizations to handle personal information responsibly. However, the specifics of these acts can differ, and it is important to understand the specific provisions of each act when considering their impact on data privacy.

Furthermore, the approach taken by the GDPR in enlisting the rights included there undoubtedly proves that the underpinning value of the act is to protect individuals' personal data from any misuse. The right to be informed, the right to access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights concerning automated decision making and profiling are all designed to give individuals greater control over their personal data. In today's digital age, new technologies are rapidly evolving, and individuals are generating vast amounts of personal data every day. This data can be collected, analyzed, and used in ways that were previously impossible, and this

poses significant risks to individuals' privacy[147]. As a result, it is crucial to view the GDPR through the lens of new technologies to ensure that its protections remain effective in the face of changing technological landscapes. By doing so, we can ensure that individuals' privacy rights are protected and that they can have confidence that their personal data is being handled responsibly. At the same time, execution of the rights included in the GDPR requires a certain degree of foreseeability. The GDPR places a significant emphasis on the accountability of controllers in protecting individuals' privacy rights. Controllers are responsible for ensuring that individuals' personal data is processed in a lawful, fair, and transparent manner, and that their rights are respected. Accountability is crucial because it provides a framework for controllers to demonstrate their compliance with the GDPR and ensures that individuals have recourse if their rights are violated. However, the current uncertainties surrounding the GDPR make it less reliable in practice. For example, there is a lack of clarity around certain provisions of the GDPR, such as the definition of consent and the rules for international data transfers. This lack of clarity can make it challenging for controllers to comply with the GDPR and for individuals to exercise their rights. Additionally, the GDPR is a complex legal framework that can be difficult for smaller organizations to understand and implement. These challenges can lead to non-compliance with the GDPR and undermine individuals' trust in the protection of their personal data. Therefore, it is essential to address these uncertainties and provide clear guidance to ensure that the GDPR is effective in practice and that individuals' privacy rights are protected.

[147] To depict the scale of data processing, it's worth viewing, for example, the Facebook Transparency Report, where according to the collected data for the second half of 2020, the company received over 129,000 requests for user data from governments around the world, covering over 227,000 user accounts. It's worth noting that this includes requests for data in criminal investigations, emergency situations, and national security matters. Retrieved February 20, 2023 from https://transparency.fb.com/data/?source=https%3A%2F%2Ftransparency.facebook.com%2F. Similarly, Google published the report that depicts the scale of processing at least by the fact that according to the report, in the second half of 2020, Google received 106,186 requests to remove 857,440 pieces of content under the GDPR. Of those requests, 89,514 requests were related to removals of search results, while 16,672 requests were related to removals of other types of content. Retrieved April 20, 2023 https://transparencyreport.google.com/

1. The right to be informed.

The General Data Protection Regulation's (GDPR) Article 12 is a key clause that establishes the groundwork for data subjects' ability to exercise their rights under the legislation. This article outlines the data controller's responsibility to offer clear information, communication, and methods for the data subject to exercise their rights. This essentially means that the data controllers must be transparent about how they gather, use, and treat personal data, as well as the rights of the data subject. Furthermore, this requires the controller to define itself and its relations with other subjects taking part in processing activities, such as, for example, other controllers in the case of joint controlling or processors. This includes supplying information on the activities involved in the processing, the goals of the processing, the legal justification for the processing, and the rights of the data subject with regard to the data. The goal of Article 12 is to make sure that data subjects are fully aware of their rights and can exercise them effectively. Data controllers can increase customer trust and show their dedication to protecting personal data in accordance with GDPR by developing clear communication and procedures for exercising these rights.[148]

Article 12 of the Regulation states the very first right included in the act and regulates *transparent information, communication, and modalities for the exercise of the rights of the data subject*[149]. The commented provision regulates the procedural aspects of exercising the rights of the data subjects referred to in Chapter III of the GDPR. The provision of information to the data subject and any communication with the data subject, under Articles 13-22 and 34 of the GDPR, should be made in a concise, transparent, understandable, easily accessible form, in clear and plain language. This requirement should be understood as requiring transparency in communication with the data subject. Such an approach was also highlighted in the preamble

[148] The European Data Protection Board (EDPB) has provided guidance on the interpretation of Article 12 of the GDPR in its Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. The guidelines provide detailed explanations of the requirements set out in Article 12, including the types of information that must be provided to data subjects and the modalities for exercising their rights. Retrieved February 24, 2023 from: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201901_on_the_processing_of_personal_data_under_article_6_1_b_of_the_gdpr_in_the_context_of_the_provision_of_online_services_to_data_subjects_en.pdf.

[149] General Data Protection Regulation, Article 12.

of the act under the transparency principle[150]. The mentioned principle in its first part recalls what follows:

> *The principle of transparency requires that any information addressed to the public or to the data subject be* ***concise, easily accessible, and easy to understand, and that clear and plain language*** *and, additionally, where appropriate,* ***visualization be used****. Such information could be provided in electronic form, for example, when addressed to the public, through a website.* (emphasis added).

What is even more important is that the right to be informed extends to the delivery of precise information about processing details, including explaining the complexity of algorithms or usage behind algorithms that process personal data.[151] Furthermore, the right to be informed affects the right to give free, conscious consent, which places certain challenges on online operating software providers to ensure a certain level of transparency.[152]

The GDPR Article 12 idea was preceded by an evaluation of Recital 11, which formulates a broad concept of improving and specifying data subjects' rights and the obligations of companies processing such data.[153] An important legal consideration is a fairly wide approach to the problem, defining basic principles and the nature of the standard - protection of individual rights, imposing information duties on companies processing personal data. Furthermore, from the standpoint of the transparency principle, the most important thing is to ensure that the data subject is fully capable of comprehending the information. Furthermore, it is critical to ensure that data access is simplified and communicated in such a way that it allows for a complete understanding of the information.[154] This provision itself suggests that, once appropriate, a data controller may use different means of communication, such as visualization or delivery of

[150] The transparency principle is included in recital 58 of the General Data Protection Regulation.

[151]M. C. Kettemann, T*he Normative Order of the Internet: A Theory of Rule and Regulation Online*, New York 2020, p. 55.

[152] *Ibid.*

[153] *Privacy and Identity Management. Fairness, accountability, and transparency in the age of big data. 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers*, E. Kosta, J. Pierson, D. Slamanig, S. [et al.] (Eds.), Cham 2019, p. 138. Retrieved April 17, 2023 from https://link.springer.com/book/10.1007/978-3-030-16744-8.

[154] *The UN Convention on the Rights of Persons with Disabilities: A Commentary*, I. Bantekas, M. A. Stein, [et al.] (Eds.), Oxford, New York 2018, p. 941.

information via electronic form. All means should be focused on an effective understanding of the rights granted to a human being. In the following part of Recital 58, it is stated that:

> *This is of particular relevance in situations where the proliferation of actors and the **technological complexity of practice** make it difficult for the data subject **to know and understand** whether, by whom, and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that **children merit specific protection**, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand. (emphasis added)*

In the above-quoted part of the legal act, the legislator acknowledges that technological complexity and advanced practice may make it difficult for a data subject to be aware of and understand the processing of personal data. What is more, it assumes special treatment when it comes to children as a group that need to be granted a special scope of protection to ensure adequacy.[155] In fact, it is stated that technological complexity shall not take advantage of individual rights granted under the Act. What follows from this understanding is that the right to be informed should be practically applied in a way that limits barriers to understanding. It included misleading practice, for example, Internet users and requests data sharing with no legal grounds for such action. In the case of children, the right to information shall be performed in a way that takes into account the limited capacity of a child and grants full understanding of an action performed where processing is addressed to a child's data. The approach of access to data along with the right to be informed is further described by the legislator in Recital 60 of the GDPR, where it is stated that fair and transparent processing requires that the data subject be informed and aware of the processing purpose and processing operations. The above-mentioned right is further defined by the obligation relying on the controller to provide the data subject with any further information necessary to ensure that the processing is fair and transparent. It means that the data subject shall be capable of making his own decision about the processing and understanding the processing activities, as well as whether it is obligatory or not to have his data processed. On the side of the processor, the form of delivering such information may vary and shall be limited only by the effectiveness of understanding, with no formalized requirements.

[155] J. G. Dwyer, *The Oxford Handbook of Children and the Law*, New York 2020, p. 382.

The idea behind the right to be informed, as presented above, refers to the concrete understanding of privacy - namely that there is a possibility to determine what information about individuals is shared, with whom, and why. Such a concept is already known in the doctrine, for example, in German law, where the idea of self-determination is present and recognized.[156] The theory assumes that to be able to have privacy as a right granted, an individual must be able to decide upon quantitative and qualitative aspects of the information shared about them. It further indicates that automatic data processing, global access to data, network routing, and all the technological background that makes the data accessible world-wide should still be bound by a simple rule concerning the individual's access to the data and ability to shape it if needed. The idea may clash with free speech in the context of access to data as well as the idea of the truthfulness of speech and the rights arising from freedom to hold opinions. The freedom to hold opinions is a fundamental aspect of individual liberty and human rights. It refers to people' freedom to create and retain their own opinions, viewpoints, and convictions without intervention or compulsion from other sources such as governments, institutions, or individuals. This freedom spans a vast spectrum of ideas, opinions, and ideologies, allowing people to express and explore various thoughts and perspectives. Respecting and protecting this freedom contribute to a society that encourages critical thinking, fosters intellectual diversity, and promotes a culture of open dialogue and tolerance. Nevertheless, the idea of the self-determination of information is currently having an impact on the perspective of data processing in Europe and remains a vital point. The concept of self-determination of information within the scope of the right to privacy relates to an individual's control over their personal information and the ability to make decisions regarding its collection, use, and disclosure. It recognizes the fundamental right of individuals to maintain autonomy and control over their personal data and the information they share with others. The concept finds its support in legal guarantees as the right to correct data, informed consent or right to remove data.

It is important to note that the extent of actual self-determination will always be affected by circumstances and technical ability. The above-presented rational remains a policy underpinning Article 12 and helping the understanding of the role of access to data and the right to be informed in the most up-to-date EU law.

[156] Rule, also known as *informationelle Selbstbestimmung*, was first discussed by Westin and understood as the possibility of having control over how information about a person is handled and communicated to others.

The legal background prior to GDPR for the general rule of the right to be informed was formulated, among others, by the Data Privacy Directive.[157] In fact, while the formulation of the right to be informed as presented by the GDPR is more precise and Article 12 of the DPD only partially deals with the subject matter appointed by Article 12 of the GDPR, the primary purpose of those two remains to some extent similar. In fact, Article 12 of the DPD assumes that the right to information should be granted with no excessive delays or expenses; nevertheless, the focus on the delivery of access seems to be less concentrated than in the case of the GDPR regulation. When looking for a similarity between the current formulation of Article 12 of the GDPR and prior law, the Consumer Rights Directive comes in handy.[158] The definition of what the customer is entitled to in light of Article 6(1) of this Directive overlaps to some extent with the idea of what belongs to the individual as the outcome of GDPR-based rights. According to Article 6(1), *Before the consumer is bound by a distance or off premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a* ***clear and comprehensible manner (emphasis added)***. Furthermore, a part of this article refers to what and in what manner the customer is entitled to the aforementioned. What matters is that all rights shall be delivered to the customer in a clear and comprehensive manner and regardless of location and in consider of other factors that may affect the delivery. Similarly, rules that find their application to electronic communication remain similar to the approach of clear and comprehensive information access as presented by the GDPR. The Universal Service Directive (2002/22/EC) introduces the idea of representation of consumer interest, which is reflected as the end user having access to comprehensive, comparable, and user-friendly information.[159] The above-quoted examples are only a sample of the tendency towards presenting access to information as a right belonging to individuals.[160] Nevertheless, it remains a fact that there is no other directive or regulation that impacts the right to access information or the right to be informed as much as the GDPR.

[157] Data Privacy Directive 95/46/ WE.

[158] Consumer Rights Directive (2011/83/EU).

[159] I. Benohr, *EU Consumer Law and Human Rights*, Oxford 2013, pp. 167-168.

[160] Among other examples, there is the EU regulatory framework for public access to environmental data (Directive 2003/4/EC). On the level of international instruments, the approach is shared by Modernised Convention 108 in art 8(1)(b) and it was also further discussed by the ECtHR, for example *Rees v. UK* or *Roche v UK*: ECtHR, Application, *Rees v. the United Kingdom*, no. 9532/81, October 1986; ECtHR, Application, *Roche v. the United Kingdom*, no. 32555/96, October 2005.

The right to be informed has been a subject of interest to the EU Court of Justice in a number of cases, including *Google Spain*, where the search engine was assessed as a data controller and was consequently made to bear responsibilities otherwise directly belonging to the data controller. In Rijkeboer, the Court of Justice directly interpreted the rule derived by Fuller, including the statement of advocacy for the congruence between official action and declared rule.[161] Apart from all prior outstanding codification approaches, Article 12 of the GDPR is targeted towards unification both from the perspective of technicalities as well as from the procedural aspects of the exercise of various information and access rights.[162]

2. The right to access personal data.

Under the GDPR, the rights of data subjects are protected through a range of provisions, including Article 12. This article establishes the data subject's right to receive information about the processing of their personal data and to access that data upon request. Specifically, Article 12 requires data controllers to provide data subjects with confirmation of the processing, information about the processing, and access to their processed data. The right conferred by Article 12 is a critical component of the GDPR's overall data protection framework, including both rights for data subjects and duties for data controllers. Furthermore, Articles 12 and 15 of the GDPR work together to establish data subjects' rights to access their personal data, with Article 12 focusing specifically on data accessibility and Article 15 providing a broader right to confirmation of personal data processing. More precisely, under the regime of Article 12 of the General Data Protection Regulation, a data controller *shall not refuse to act on the request of the data subject for exercising his or her rights*.[163] In fact, the right granted by Article 12 of the GDPR is composed of three layers, namely receiving confirmation about the processing, receiving information about the processing, and receiving access to the processed data itself. The right granted by Article 12 creates a right for data subjects and an obligation for data

[161] CJEU (Third Chamber), Judgment *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, Case C-553/07,May 2009, ECLI:EU:C:2009:293.

[162] C. Kuner, L. E., Bygrave, C. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Kettering 2018, pp. 401-402.

[163] GDPR, art. 12(2).

controllers.[164] Furthermore, Articles 12 and 15 of the Regulation imply the right to access data. The above-quoted Article 12 refers directly to data accessibility, while Article 15 states that data subjects *have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.*[165] In its following part, the article lists a catalog of data that may be requested by the data subject from the data controller, and such information includes the following:

A. *the purposes of the processing;*
B. *the categories of personal data concerned;*
C. *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
D. *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
E. *the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*
F. *the right to lodge a complaint with a supervisory authority;*
G. *where the personal data are not collected from the data subject, any available information as to their source;*
H. *the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*[166].

Article 15 outlines an individual's right to access their personal data. This provision requires controllers to provide individuals with specific information about their personal data processing. The following elements must be included in the response:

- Firstly, the individual has the right to know the purpose of the processing of their personal data. The controller must provide a clear and concise explanation of the

[164] According to article 28(3)(e) of the GDPR, data controllers can maintain a contractual obligation towards data processors to assist them in processing and fulfilling requests from data subjects.

[165] GDPR, art. 15(1).

[166] *Ibid.*

purpose(s) for which the data is being processed. This information must be easily understandable and accessible.[167]

- Secondly, the individual has the right to know what types of personal data are being processed. The controller must provide a description of the categories of personal data that are being processed. This information must be specific and accurate, enabling the individual to understand the extent to which their data is being used.[168]

Furthermore, the individual has the right to know to whom their personal data has been disclosed. The controller must provide a list of the recipients or categories of recipients to whom the personal data has been or will be disclosed, including any third countries or international organizations. This information must be provided in a transparent and easily accessible format.[169]

What is more, the individual has the right to know how long their personal data will be stored. The controller must provide an estimate of the period for which the personal data will be stored, or the criteria used to determine that period. This information must be specific and accurate, enabling the individual to understand the length of time their data will be used.[170]

Individuals have the right under 15(1) to have their personal data corrected, deleted, or the processing of their personal data limited. The controller shall notify the individual of this right, allowing them to take appropriate steps to protect their personal data.[171]

What is more, the individual has the right to lodge a complaint with a supervisory authority if they believe their data protection rights have been infringed. The controller must inform the individual of this right, enabling them to take action if necessary.[172]

Furthermore, if the personal data has not been collected from the individual, the individual has the right to know the source of the data. The controller must provide any available information

[167] GDPR, art. 15(1)(a).

[168] GDPR, art. 15(1)(b).

[169] GDPR, art. 15(1)(c).

[170] GDPR, art. 15(1)(d).

[171] GDPR, art. 15(1)(e).

[172] GDPR, art. 15(1)(f).

about the source of the personal data, enabling the individual to understand how their data has been obtained.[173]

Lastly, if the personal data is being processed through automated decision-making, the individual has the right to know about this. The controller must provide information about the logic involved, the significance of the decision, and the envisaged consequences of such processing for the data subject. This information must be specific and clear, enabling the individual to understand how automated decision-making affects their personal data.[174]

As a consequence, the commented article of the GDPR regulates the right of access to a data subject to his/her personal data and places certain expectations and requirements on the controller for the delivery of such access to the requesting data subject.[175]

Its scope covers all cases of personal data processing, regardless of whether the processing takes place in the data filing system or outside the system. The catalog of information that the data subject may request from the data controller is closed. The basic information that the data controller may require from the data subject is whether his or her personal data are being processed. If the answer to this question turns out to be 'yes', then the person may, based on the above-stated catalog, apply for access to the processed data. The result of exercising the right of access to personal data should be to provide the data subject with the information requested by the person. By virtue of Article 12(3) of the GDPR, the provision of information shall take place without undue delay and not later than one month after the receipt of the request. The element of the right of access to personal data is the right of the data subject to receive a copy of personal data from the data controller. This right should be distinguished from the so-called right to transfer personal data (included in Article 20 of the GDPR). The content of the right to transfer personal data is the right to receive data in a structured, commonly used machine-readable format and the right to send the data to another controller, while the right of access to the data is limited to the individual concerned's receipt of the data. Furthermore, portability is defined as an individual's ability to move, copy, or transfer personal

[173] GDPR, art. 15(1)(g).

[174] GDPR, art. 15(1)(h).

[175] D. Kościuk, *General Data Protection Regulation (GDPR) – The EU Law Strengthening the Information Society in Poland*. Białostockie Studia Prawnicze 2018 vol. 23, no. 2p. 144.

data easily from one IT environment to another safely and securely, without affecting its usability.[176] As a result of exercising the right of access to personal data, the data subject may obtain a copy of personal data in the format indicated by him/her. However, if the person asks for a copy by electronic means and does not indicate otherwise, the information is provided by a commonly used electronic means. As it seems, in such a case, the data should be sent using the same means of communication by which the data subject shared it. Article 15 stands as a ground for the principle regarding the right of access by the data subject; nevertheless, a broader perspective on the interpretation of the article is laid down by Recital 58, which refers to the transparency principle and the right of data subjects to have easy access, accessibility, and understanding of data processing. Furthermore, Recital 59 comes in handy with the explanation of modalities that should be provided to facilitate the exercise of the data subject's rights under the GDPR, which includes a technical background that facilitates request management as well as free of charge access to and rectification or erasure of personal data upon the data subject's request[177]. Lastly, when it comes to GDPR recitals, Recital 63 comes into consideration with an explanation of the right to access in light of the lawfulness of processing. Recital 63 highlights the need for access to data to assess the lawfulness and correctness of processing.

The obligation of the data controller in this regard was also mentioned in Recital 64, where it is stated that the controller should use all reasonable measures to verify the identity of the data subject requesting access to data, and going even further, it is not treated as a reasonable ground for data processing to process data solely for the purpose of responding to potential requests.

The discussed matter is tightly connected with the question of data portability. Of course, there is no one format or sharing type that would ensure data portability compliance, and its execution will always require a bit of common-sense understanding.[178] This approach was further highlighted by the UK Information Commissioner. On the government page, the right

[176] H. Carr, D. Goosey, *Law for Social Workers.* 15th edition, New York 2019, p. 123.

[177] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.,* pp. 450-452.

[178] I. J. Lloyd, *Information Technology Law.* 9th edition, New York 2020, pp. 110.

to access is summarized as *the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.*[179]

In fact, the importance of discussing rights derived from Article 15 of the GDPR is also grounded in the frequency of complaints filed in this regard. The underlying policy behind this subject matter leads us to the conclusion that the right to access the data subject is one of the most frequently used rights. For example, in the United Kingdom, the Information Commissioner's Office has presented an annual report that shows an 8% growth in complaints regarding access to data rights, which overall amounts to 46% of complaints.[180] Similar statistics were reported by other countries, such as Ireland.[181]

Prior to GDPR's entry into force, the right to access was already discussed in Article 8 of the European Convention on Human Rights (CJEU) in a number of cases.[182] The above-quoted right was also of interest to the CJEU; among others, in Rijkeboer, the Court discussed data retention and access to the data in all of its disclosures.[183] Article 12 discussed in Rijkeboer refers to two aspects of the article, namely access to data and legality of processing, which bring a similar concept to what is currently presented by the GDPR.[184]

The right to access personal data is a fundamental right under the GDPR, but it can be challenging for data controllers to comply with this obligation. Providing individuals with

---

[179] Right to data portability [In:] *Guide to the General Data Protection Regulation (GDPR)* [online]. Retrieved February 16, 2021 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/.

[180] *Information Commissioner's Annual Report and Financial Statements 2019-20*, London 2020. Retrieved June 9, 2021 from https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

[181] According to the Data Protection Commissioner Annual Report from 2020 around 27% of complaints that were reported concern right to access. *DPC 2020 Annual Report* [online], Dublin, Data Protection Statement, 2020. Retrieved June 9, 2021 www.dataprotection.ie/en/resources/tuarascalacha-reachtula/annual-report-1-january-2020-31-december-2020.

[182] For example, *Leander v. Sweden* concerning a request to access data made by a Swedish citizen or *K.H. and Others* that deals with the obligation of the state to provide the data in the case of medical field.

[183] CJEU Case C-553/07, *Rijkeboer*, para. 51-52 and 54.

[184] R. Gellert, *The Risk-Based Approach to Data Protection*, Oxford, 2020, p. 77.

access to their personal data can be time-consuming and costly, especially for large organizations with complex data processing systems. Furthermore, in some cases, the right to access may not be proportionate, as it can impose a significant burden on data controllers and limit their freedom to operate their businesses efficiently. This has been a subject of debate in some cases before the CJEU, where the court has sought to balance the rights of individuals to access their personal data against the interests of data controllers to be free from unfair and/or unnecessary burdens. However, it is important to remember that the right to access personal data is a fundamental right and plays a crucial role in ensuring the protection of individuals' privacy and data protection. Therefore, while it may be difficult for data controllers to comply with this obligation, they must do so in a way that respects individuals' rights and freedoms.

3. The right to rectification – the right to correct personal data.

Access to personal information remains one of the elements belonging to individuals. The right, along with the right to erasure, constitutes an expression of the data subject's right to control their data and its quality. The right to rectification is a fundamental component of the General Data Protection Regulation, which grants individuals the ability to request the correction of any inaccurate or incomplete personal data held by a controller. This right is crucial in ensuring the accuracy and integrity of personal data and enables individuals to exercise greater control over their personal information. Controllers must respond to requests for rectification without undue delay and communicate any changes to third parties, where necessary. The GDPR's emphasis on the right to rectification underscores the importance of accurate and up-to-date personal data in maintaining individuals' privacy rights and their ability to make informed decisions about how their data is processed.[185]

[185] Despite the clarity of the right to rectification under the GDPR, there are still some uncertainties around its scope. One area of ambiguity is the extent of the right's application to public authorities, as the GDPR does not explicitly address whether it applies to public bodies or only to private entities. Another issue is the scope of the right in relation to the requirement for data accuracy under Article 5(1)(d) of the GDPR. It is unclear whether the right to rectification applies only to data that is inaccurate or incomplete, or whether it also covers data that is outdated or irrelevant. Additionally, there may be some difficulties in determining when a request for rectification is manifestly unfounded or excessive, which may affect controllers' obligations to respond to such requests. These

The right to rectification is intuitively linked to the right to access, and along with this one, it has a substantial impact on shaping how an individual is perceived. Furthermore, under the General Data Protection Regulation, an individual may request data rectification. Similarly, as in Directive 95/46, the GDPR highlights the accuracy principle. The principle is picked up by the specific provisions of this Act, and among others, Article 16 provides a ground for data rectification. The article reads as follows:

> *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.*[186]

The article directly ensures that data subjects are entitled to ask for data rectification, and such action shall be delivered without any undue delay; this being followed by simple technical steps necessary to erase the data regardless of the physical access to the device storing the data.[187] What is more, GDPR itself does not offer any timeline that may assist when it comes to the determination of the performance of any rectification or erasure.[188] The commented provision gives the data subject the right to proceed with two main actions to protect digital privacy, namely:

- rectify incorrect personal data, simply speaking to correct the data that are in question[189]; and
- rectify incomplete personal data which allows the data subject to add missing information to further ensure full scope of correct data is being processed by the controller.[190]

---

uncertainties may lead to inconsistent application of the right to rectification, which could undermine its effectiveness in protecting individuals' privacy rights.

[186] GDPR, art. 16.

[187] J.L.H. Ramos, A.Skarmeta, *Security and Privacy in the Internet of Things: Challenges and Solutions*, Amsterdam 2020, p. 36.

[188] D. Rucker, T. Kugler, *New European General Data Protection Regulation. A Practitioner's Guide Enduring Compliant Corporate Practice*, Baden-Baden, 2018, p. 69.

[189] G. Z. Capaldo, *The Global Community Yearbook of International Law and Jurisprudence. Volume 1*, Oxford University Press, New York, 2015, pp. 240.

[190] *Ibid.*

Furthermore, these rights can be summarized as the data subject's corrective rights. The above-mentioned provisions must apply to personal data for which the mode of rectification or supplementation is determined by separate legal acts or laws. The right to rectification under the GDPR is sometimes referred to as the *corrective right* because it allows individuals to correct inaccurate or incomplete personal data that is held by controllers.[191] The right to rectification is an essential component of the GDPR's data protection framework, as it enables individuals to exercise greater control over their personal information and helps to ensure the accuracy and integrity of personal data. By allowing individuals to request the correction of inaccurate data, the right to rectification empowers them to take corrective action and mitigate the potential harm that may result from inaccurate or incomplete data.

An example of a legal act that the right to rectification may not cover is a decision made through administrative proceedings. This provision specifically allows individuals to correct data that is classified as incorrect or incomplete but does not extend to challenging the validity or legality of a decision made through a separate legal process. Such an understanding of the scope of the data processing legislation is known across a number of jurisdictions.[192] By this means, GDPR

[191] The term corrective right is sometimes used to refer to the right to rectification under the GDPR. See for example: I. Bartoletti, *An Introduction to the GDPR: Your Rights as a Data Subject*, CPO Magazine May 14, 2018. Retrieved July 20, 2021 from https://www.cpomagazine.com/data-protection/introduction-gdpr-rights-data-subject/.

[192] Several legal acts and jurisdictions include the concept of incomplete data as falling under the scope of rectification or correction. For example, under the California Consumer Privacy Act (CCPA), individuals have the right to request the correction of incomplete personal information held by businesses. Similarly, the Australian Privacy Principles (APPs) define *incomplete* personal information as falling under the scope of correction, which includes the addition of new information to complete the record. In addition, the European Convention on Human Rights (ECHR) also recognizes the right to correct inaccurate or incomplete personal information. The European Court of Human Rights (ECtHR) has interpreted Article 8 of the European Convention on Human Rights (ECHR) to include the right to correct inaccurate personal information maintained by public agencies. The concept of incomplete data falls under the scope of rectification because incomplete information can be just as damaging or misleading as inaccurate information. By allowing individuals to correct incomplete information, they can ensure that their personal information is accurate and complete, which is essential for protecting their privacy rights and making informed decisions about the processing of their data.

introduces the notion of *accurate data*[193]. Such notion finds no definition in this legal act and, furthermore, was neither defined under the regime of Article 16 and Recital 65 nor under Article 5(1). Consequently, the lack of definition in this regard may be viewed as legal uncertainty[194]. This notion was interpreted by the Working Party, according to the interpretation, accurate means *accurate as to a matter of facts.*[195] Incorrect data is data that does not correspond to the actual state of affairs. In other words, incorrect data is false data. The correctness of personal data should be assessed from the perspective of the data subject, and the conformity of the data with the reality it describes should be examined.[196] The correctness or irregularity of personal data is assessed objectively by the data subject. Incomplete data is correct, but incomplete in scope. The completeness of personal data should be assessed from the point of view of the purpose of data processing, which, based on the principle of personal data minimization, determines the scope of data processing. In other words, the state of completeness or incompleteness of the data is subject to an objective assessment, concerning the purpose for which the data are processed.[197] Furthermore, in practice, the accuracy of data goes along hand-in-hand with the quality of data in reality.[198] The right to rectify incorrect, non-accurate and incomplete personal data places some obligations on the data controller.[199] Under the GDPR, the individual rights of data subjects must always be respected and protected by data controllers. Consequently, if the data subject demonstrates that the controller processes incorrect or incomplete data, then the controller shall be obliged to immediately correct the incorrect data or complete the incomplete data. The choice of one

[193] The GDPR requires that personal data be accurate, meaning it must be factually correct and free from errors. Organizations that collect and process personal data are responsible for taking reasonable steps to ensure the accuracy of the data they hold.

[194] *Ibid.*

[195] *Ibid.*

[196] T. Hoeren, B. Kolany-Raiser, *Big Data in Context: Legal, Social and Technological Insights*, [S.l.] 2017, p. 8.

[197] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, pp. 396-397.

[198] P. Coppel, *Information Rights. A Practitioner's Guide to Data Protection, Freedom of Information and other Information Rights*, Edition 5, Oxford, 2020, p. 211.

[199] If the controller records data in the right way from a technical perspective and the recording is correct but the data given on the recording by the data subject is incorrect, such a situation still triggers the GDPR rule concerning accuracy.

of the indicated methods of operation shall depend on the content of the request of the data subject, but at the same time, it shall be adjusted to the nature of the existing and proven defect in the data processing. Furthermore, according to the Article 29 Data Protection Working Party (WP29), *Controllers need to introduce robust measures to verify and ensure on an ongoing basis that data reused or obtained indirectly is accurate and up to date.*[200] Prior to the GDPR, the matter of rectification was discussed by the European Court of Human Rights (ECtHR) and Court of Justice of the European Union (CJEU), and what is more, the idea finds its early origins in EU legislation. In *Ciubotaru v. Moldova*, the ECtHR held that there is a positive obligation on the signatories of ECHR to have the data concerning individual changed[201]. In rulings of the CJEU, *Nowak* discussed a request to access data as defined by the Data Protection Directive, and more particularly, the ruling discussed the access to exam scripts by students.[202] Apart from this, the CJEU raised the issue of rectification under *Schrems*, wherein a Safe Harbor Agreement was invalidated based on the data removal and access regulations under national US law.[203] The CJEU held that the Safe Harbor Agreement did not provide adequate safeguards for the protection of EU citizens' personal data, particularly with respect to US national security laws that allowed for indiscriminate surveillance and access to personal data. The CJEU's ruling highlighted the importance of data protection safeguards, including the right to rectification, in ensuring the privacy rights of EU citizens. The CJEU's decision also raised concerns about the effectiveness of the right to rectification in the context of US national security laws, which may limit individuals' ability to exercise their data protection rights. The ruling emphasized the need for robust data protection safeguards and accountability mechanisms to ensure the protection of personal data in the context of international data transfers. In this regard, the right to rectification may be viewed as a critical instrument for defending individuals' private rights, particularly when their data may be exposed to access by national security services. Overall, the CJEU's decision in *Schrems* emphasizes the need for strong data protection protections and ensuring that individuals have the right to manage their personal information, including the right to correction.

[200] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251, Adopted on 3 October 2017, pp. 19.

[201] ECtHR, Application, *Ciubotaru v. Moldova*, no. 27138/04, April 2010, para. 58-59.

[202] *Peter Nowak v Data Protection Commissioner*, Case C-434/16, *op. cit.*, para. 49.

[203] CJEU, Case C-362/14, *Schrems*, para. 95.

4. The right to erasure – right to remove personal data.

In addition to the right to correct or adjust personal data (rectification right), GDPR also includes the right to erase personal data, also known as the *right to be forgotten*. At the beginning, it is important to elaborate on the semantic differences between those two terms, namely, *the right to be forgotten* and the *right to erasure.* Currently, both are used interchangeably, but there are some technical differences that are worth highlighting at this early juncture.[204] The right to be forgotten and the right to erasure are two related but distinct rights under the GDPR. The right to erasure, also known as the *right to be forgotten,* allows individuals to request the deletion of their personal data by controllers under certain conditions. Yet, while the right to be forgotten or the right to data erasure is one of the most clearly defined terms and right under the GDPR, it still raises some controversies with regard to its actual and formal scope and purpose.[205] This right is closely related to the GDPR's data minimization principle, which requires controllers to only collect and retain personal data that is necessary for specific purposes. The right to erasure is not absolute, and controllers may refuse to comply with a request if they can demonstrate a legitimate reason for retaining the data, such as for compliance with a legal obligation[206]. The right to be forgotten, on the other hand, is a broader

[204] The conditions under which people may exercise their right to be forgotten are outlined in Article 17 of the GDPR, including when the data is no longer required for the purposes for which it was obtained, when the person withdraws their consent, or where the data was handled unlawfully. In its *Google Spain* decision, Case C-131/12, the CJEU acknowledged the concept of the right to be forgotten and found that, under certain conditions, people have the right to ask for the removal of connections to their personal data from search engine results.

[205] Some critics have argued that the right to be forgotten may be used to suppress legitimate information and undermine freedom of expression. For instance, journalist Robert Peston claimed that the right to be forgotten poses *a danger to freedom of speech* and that it might be used to restrict journalism and the historical archives of an essay for the BBC. In a report on the right to be forgotten, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression voiced concerns about the potential effects of the right on freedom of expression and access to information. It should be emphasized that there are many people who favor the right to be forgotten and claim that it is a crucial instrument for defending personal freedom and privacy in the digital era.

[206] Much discussion and disagreement have surrounded the rights to be forgotten and to have personal information deleted, especially in relation to how they should be used and implemented. Concerns have been raised, for instance, regarding the possibility of a conflict between the right to be forgotten and the freedom of speech, as well as the practical difficulties of putting the right to be forgotten into practice. The right to be forgotten may result in censorship and the suppression of accurate information, according to some detractors. Nonetheless,

concept that goes beyond the deletion of personal data. It refers to an individual's right to request the removal of links to their personal data from search engine results and other online platforms. This right is not explicitly provided for in the GDPR but has been recognized by the CJEU as the outcome of the *Google Spain* ruling. The right to be forgotten is based on the idea that individuals should have the right to control their online reputation and the dissemination of their personal information. However, the right to be forgotten is also subject to limitations, such as the public interest in access to information and freedom of expression. In summary, while the right to erasure and the right to be forgotten are related, they are distinct concepts under the GDPR. The right to erasure allows individuals to request the deletion of their personal data by controllers, while the right to be forgotten refers to an individual's right to request the removal of links to their personal data from search engine results and other online platforms. Both rights are important tools for protecting individuals' privacy and data protection rights, but they are subject to limitations and conditions under the GDPR.

The scope of the protection granted by Article 17, along with Recitals 65-66 ensures individuals' rights to effectively remove data from the Internet. Such removal shall include a right to withdraw the consent granted for data processing and, deletion of personal data. Article 17 directly states that the individual shall be entitled *to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data,*[207] Recital 65 further states that the erasure may be performed *where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject.*[208] Article 5, which relates to data processing principles, Article 19, which is responsible for notification obligations regarding rectification or erasure of personal data or restriction of processing and finally, Article 21, which refers to the right to object, provide some practical guidelines in the case of the right to erase data. When it comes to data processing law in the EU, the right to be forgotten, also known as the right to erasure, has been viewed as a new topic, and it is undoubtedly receiving greater attention due to the extent of its application to data subjects.

supporters of both rights contend that they are crucial instruments for preserving people's autonomy and privacy in the digital era.

[207] GDPR art. 17

[208] GDPR Recital 65.

In fact, the Data Protection Directive has previously addressed similar issues under Article 12 - the provision granting data subjects the right to seek the removal of their data from the controller and to know who else (third-party subjects) is involved in the data processing[209]. Among all the rights, the right to be forgotten is one of the most important as far as the potential exploitation of personal data is concerned. Looking at the current state of technology and data processing on a large scale by computer systems, search engines, artificial intelligence models, and/or any other mechanisms of Internet intermediaries, it is clear that the complexity of data storage and the challenge of removing such data without incurring disproportionate business costs are clear. Because of this fact, attempts to regulate the right to be forgotten were also raised on the international level in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (also known as Convention 108), which mentions the right to obtain, as the case may be, rectification or erasure of such data if such data has been processed contrary to the provisions of domestic law[210]. It might be debated how much of an influence regulation of the right to be forgotten truly had, but there is no question that Article 17 prompted a substantial conversation about it. Furthermore, the right to be forgotten was a topic of discussion in other international rulings. [211]

Some aspects of the right to be forgotten have been widely commented on by the *Google Spain* judgment of May 13, 2014, where the ECJ (Grand Chamber) decided that the data subject has the right to have the information concerning him or her no longer associated with his or her name through a list displaying the results of a search, with the starting point being the name.[212] In other words, the data subject is entitled to ask the operator of the Internet search engine, in this case, Google, to block the possibility of searching for specific information concerning

[209]S. Allen, *Remembering and Forgetting – Protecting Privacy Rights in the Digital Age*, European Data Protection Review 2015, vol. 1(3), pp. 164-177, Retrieved June 13, 2021 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2776048.

[210] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention No. 108, Strasbourg, 28.01.1981, article 5-6.

[211] ECtHR Application no. 33846/07 *Węgrzynowski and Smolczewski v. Poland* dealing with data removal in the light of freedom of expression, CJEU C-398/15 *Manni* referring to the fact that there is no requirement on the side of a Member State to remove certain personal data from a public company register.

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

him.[213] According to the ECJ, this specific right to be forgotten has its source in Articles 7 and 8 of the Charter of Fundamental Rights of the EU. The judgment brought a lot of controversy over the protection of free speech and was recognized the greatest threat to free speech on the Internet in this decade.[214] Furthermore, in the aforementioned judgment, the Court has interpreted the right to be forgotten to be a fundamental individual right in stating what follows:

> *Article 7 of the Charter* ***guarantees the right to respect for private life****, whilst Article 8 of the Charter* ***expressly proclaims the right to the protection of personal data****. Article 8(2) and (3) specify that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that* ***everyone has the right of access*** *to data which have been collected concerning him or her and the right to have the* ***data rectified****, and that compliance with these rules is to be subject to control by an independent authority. Those requirements are implemented inter alia by Articles 6, 7, 12, 14, and 28 of Directive 95/46.*[215] (emphasis added)

The Court emphasized the significance of individual control over personal data. On the other hand, the Court emphasized that, in some cases, interference in a person's fundamental rights is a legitimate overriding interest of the search engine users in having access to given information through the operation of the search engine. Likewise, based on the judgment C-131/12, the right to be forgotten is a right that can be exercised with search engines. This right does not extend to source information, the removal or non-removal of which does not, in the Court's judgment, alter the problem of interference in the Internet search engine's search results.[216] Judgment C-131/12 laid down a basis for the further inclusion of standards of Article 17 of the GDPR, stating that this is a consequence of the controller's obligation to delete personal data of a data subject on request performed under the regime of Article 17(1).[217] Even if the right to be forgotten as we know it now was not described by the CJEU in the *Google*

---

[213] A. Murray, *Information Technology Law: The Law and Society,* Glasgow 2016, p. 570.

[214] E. Schweighofer, Leitold H., Mitrakas A.,Rannenberg K., P*rivacy Technologies and Policy: 5th Annual Privacy Forum, APF 2017, Vienna, Austria, June 7-8, 2017*, Revised Selected Papers, Springer, Vienna, 2017, pp. 37.

[215] *Ibid*, para. 69.

[216] P. Litwiński, PP. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w swobodnym przepływem takich danych… opt.cit,* pp. 401.

[217] D. Rucker, T. Kugler, *opt.cit.*, pp. 141.

Spain judgment, it still represents an important step in the discussion.[218] Further elements of the article include the controller's obligation to take reasonable steps to remove personal data from other controllers or processing subjects where the data subject's data has been shared during processing activities. The right to be forgotten can be exercised against the personal data controller. According to the *Google Spain* judgment, the operator of the search engine has the status of a controller of personal data about information containing personal data, that is localized, indexed automatically, organized and stored, and shared according to the preferences of users. The status of a web browser provider is different from, for example, a hosting provider, which cannot, in most cases, be considered a personal data controller but only a processor. The right to be forgotten can be traced back to two parts:

- the right to request the removal of personal data by the controller; and
- the right to require the controller to inform other data controllers to whom controller has made the data available that there is a request for the controllers to delete the personal data.[219]

The information of the other administrators is clarified based on Recital 66 of the GDPR, which states that *the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to or copies or replications of those personal data. In doing so, that controller should take reasonable steps,* ***taking into account available technology and the means available*** *to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.*[220] (emphasis added).

The EU legislator has therefore explicitly provided that the effective right to be forgotten obliges the controller to delete data from the backups as well.[221] This raises serious doubts about the costs associated with such an action. The obligation to inform the controllers was created *ex lege*, and the only reason for its creation is that the personal data, about which the

[218] E. Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, Human Rights Law Review 2014, vol. 14, no. 4, p. 765. Retrieved June 9, 2021 from https://doi.org/10.1093/hrlr/ngu033.

[219] A. Nielsen, *Practical Fairness. Achieving Fair and Secure Data Models*, Sebastopol, 2021, p. 240.

[220] GDPR, Recital 66.

[221] W. C. Preston, *Backup & Recovery. Inexpensive Backup Solutions for Open Systems*, Sebastopol, 1999, pp. 7.

right to be forgotten has been exercised, should be made public, i.e., has made the personal data public. Limitations placed on the right to be forgotten on the ground of GDPR are as follows:

- technological limitations;
- costs of implementation; and
- the reference to taking reasonable steps in carrying out this duty.

The subjectivity of the recording and its evaluation through the prism of the data management company are determined by the technological premise and cost - the ability to implement technological solutions for a market monopoly such as Google or Facebook will be significantly different from the implementation capabilities of medium or small businesses. Finally, the right to be forgotten has no application in the exercise of free expression and information. If a data controller can demonstrate that data processing is required in order to exercise free expression or the right to information, the reasons for the data deletion procedure are rendered moot. Furthermore, the European Court stated that Europe could not impose the right to be forgotten on countries that did not recognize the law, so the right to be forgotten is geographically limited and narrowed down[222].

5. The right to restrict processing.

The right to be forgotten in the form known from GDPR, along with the right to restrict processing, constitute a novelty brought upon by European Legislation.[223] The concept of the right to restrict the processing of personal data arises from the very basic idea that individuals have the right to shape information about them that is shared externally.

[222] New York Times, 'Right to Be Forgotten' Privacy Rule Is Limited by Europe's Top Court, A version of this article appears in print on Sept. 25, 2019, Section B, Page 1 of the New York edition with the headline: Decision Limits Europe's 'Right To Be Forgotten'. A. Satariano, *'Right to Be Forgotten': Privacy Rule Is Limited by Europe's Top Court: The European Court of Justice said the landmark privacy law cannot be enforced beyond the European Union*. New York Times, Sept. 25, 2019, Sect. B, p. 1. Retrieved June 9, 2021 from https://www.nytimes.com/2019/09/24/technology/europe-google-right-to-be-forgotten.html.

[223] There are only minor antecedents regarding the right to restrict processing in the case of EU law prior to the GDPR, and there is no direct provision from DPD that refers to the same subject matter. DPD used a wording to request the blocking of data in cases of processing in light of data subjects' rights.

As discussed in Chapter I of this thesis, the definition of privacy is complex and understood in numerous ways, one of which is the right to decide what others know about us. The right to restrict processing is a legal concept shared across multiple jurisdictions. It is a basic right that permits individuals to restrict how businesses use their personal information. This right is recognized in various privacy laws, such as the EU General Data Protection Regulation under Article 18, the California Consumer Privacy Act under Section 1798.120, and Brazil's General Data Protection Law under Article 18. Individuals have the right to restrict processing in a variety of instances, including when the accuracy of personal data is questioned, when processing is unlawful, or when the subject objects to the processing of their data.

Under Article 18 of the GDPR, a further right for the individual appears, namely the understanding of a restriction on data processing. In fact, it may serve as a support for individuals, as the right to restrict processing to some extent may be used interchangeably with the right concerning data erasure.[224] The core element of restriction on processing finds its origins in Article 18 of the GDPR, but there are other relevant articles and recitals that raise the issue of limitation on processing that creates an obligation for the controllers. Article 18 gives individuals the right to restrict the processing of their personal data in certain situations, such as when the accuracy of the data is contested or the processing is unlawful. One example of this was the case of *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12), which concerned a complaint by a Spanish citizen against Google for displaying outdated and irrelevant search results related to him. The European Court of Justice ruled that individuals have the right to request that search engines remove links to information that is inadequate, irrelevant, or no longer relevant, thus restricting the processing of their personal data. Another example is the case of *Bundesverband der Verbraucherzentralen und Verbraucherverbände v Facebook Ireland Ltd*. (Case C-40/17), which focused on Facebook's use of facial recognition technology to automatically tag people in photos uploaded to the platform[225]. The court found that Facebook had violated the GDPR by not obtaining users' explicit consent for this processing and ordered the company to delete

[224] G. Zanfir-Fortuna, *Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right*, [In:] *Reforming European data protection law*, S. Gutwirth, R. Leenes, P. De Hert (Eds.), Dordrecht, 2015, p. 6, Retrieved June 13, 2021 from https://ssrn.com/abstract=2501312.

[225] CJEU, Judgment (Second Chamber) of 29 July 2019, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, Case C-40/17, July 2019. ECLI:EU:C:2019:629. Case also known as *Schrems II*.

the facial recognition data and restrict further processing.[226] Even though the main focus of Schrems II is well-known from its attempt to restrict data transfer to the US, it is important to highlight that the right to restrict processing to countries where the level of protection formally differs from the one represented by the GDPR was an important element of the judgment. The fact that Facebook, now operating as Meta, was said to lack sufficient consciousness to remove the data because the company decided to remove it only from the main servers and not from backups demonstrates an important aspect of data controller responsibility and the still poorly defined scope of such responsibility under GDPR. [227]

Article 18 directly states that the data subject is entitled to obtain from the controller a restriction of processing in regulated circumstances. Furthermore, restriction of processing is present in Article 4(3) of the GDPR in the following manner *'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future*.[228]

It is vital to recall that processing as an activity requires a broader scope of understanding, and that processing should be understood as any action performed on data, including storage. The

[226] In the case of Facebook, the plaintiffs argued that the company violated their right to restrict processing by continuing to process their personal data even after they had requested that it be deleted. Facebook argued that it had complied with the plaintiffs' requests and had deleted the data in question, but the plaintiffs contended that Facebook had only deleted the data from its main servers and had not ensured that it was also deleted from all backup copies. The CJEU ultimately found that Facebook had not properly addressed the plaintiffs' requests to restrict processing, and that it had failed to ensure that the data in question was deleted from all copies, including backup copies. The court emphasized that the right to restrict processing is an important privacy protection measure that allows data subjects to control the use of their personal information, and that data controllers like Facebook have an obligation to respect this right and take all necessary measures to ensure that it is properly implemented.

[227] Furthermore, the requirement regarding the right to restrict processing on the grounds of the *Schrems II* judgment remains expensive and technologically difficult to implement. Due to the complexity of backup systems, it might be difficult from a technical standpoint for platforms like Facebook to abide by demands to remove personal data from backups. It might be challenging to locate and delete specific data since backup systems frequently employ different storage technologies, data formats, and retention regulations than the primary system. Moreover, backup systems use redundancy or snapshot technologies that make it challenging to remove specific data without compromising the integrity of the backup in its entirety. These technologies are used to defend against data loss. Although it can be difficult to comply with the right to be forgotten, data controllers like Facebook are required to make sure that all essential steps are taken to correctly remove personal data.

[228] GDPR, art. 4(3).

limitation of processing in this context tries to limit the extent of any action taken on data beyond storage. Every action that goes beyond storage activities is possible only in the case of the following exemptions:

a. the data subject has consented to this;
b. to establish, pursue, or defend claims;
c. for the legal protection of another natural or legal person; and
d. for reasons of the public interest of the European Union or a Member State.

If there are reasons directly indicating the need to stop such activities, the controller is required to stop or limit the processing of personal data. First and foremost, under Article 16 of the GDPR, when the data subject concerns the accuracy of personal data. In such cases, the limitation applies automatically for a period of time, allowing the controller to verify the correctness of the data. A person's objection to the erasure of improperly processed personal data is another indicator of a processing limitation. In this case, the legal basis for processing personal data ceases to exist (under Article 6(9) GDPR). In such a situation, the controller should decide to restrict the processing. The last reason for limiting the processing of personal data for the controller is to object to the processing under Article 21(1) of the GDPR.[229] In such a case, the processing should be suspended automatically for a period of time thereby enabling the controller to determine the legitimate grounds on the part of the controller and whether such grounds prevail over the objection raised based on the risk-based balancing test.[230] Furthermore, the commented regulation suggests some technical aspects of processing restrictions under Recital 67[231]. The described recital reads as follows:

> *Methods by which to restrict the processing of personal data could include, inter alia, **temporarily moving the selected data to another processing system**, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing*

[229] According to art. 21(1) of the GDPR, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her that is based on points (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.

[230] R. Gellert, *The Risk-Based Approach to Data Protection*, Oxford University Press, Oxford, 2020, pp. 58.

[231] P. Coppel, *Information Rights: A Practitioner's Guide to Data Protection, Freedom of Information and other Information Rights, Edition 5… opt.cit.*, p. 67.

> *should in principle be ensured by **technical means** in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be **clearly indicated in the system**.*[232] *(emphasis added)*

The above-presented quote mentioned a technical benchmark for data controllers to include in the course of restricted processing activities, namely a clear indication of the limited scope of processing along with the potential necessity to move such data to another system or introduce other technical measures that ensure limited processing activities. Furthermore, Recital 156 introduces the idea of *restriction of processing* by highlighting the archiving purpose in the public interest and scientific field that shall be balanced against the right in question.

6. The right to data portability

The right to data portability is a basic right given to individuals by data protection laws such as the European Union's General Data Protection Regulation. It gives people the right to request a copy of their personal data in a structured, widely used, and machine-readable format and to transfer that data to another data controller without limitation. This right is intended to provide data subjects with more control over their personal data while also encouraging service providers to compete with one another.

By enabling data subjects to quickly access and move their data between services, it also attempts to encourage transparency and accountability. Ultimately, the right to data portability is a crucial instrument for safeguarding people's data and privacy. The capacity of people to transfer their personal data from one organization to another is referred to as *data portability*. Since people depend more and more on digital services that gather and use their personal data, this idea has gained in importance. Yet, when working with other jurisdictions, the issue of data portability gets more challenging. The process of ensuring that data is moved in compliance with all applicable rules is demanding due to the plurality of requirements across multiple jurisdictions. Also, various countries may have differing degrees of data protection, which can make it difficult for enterprises to meet data portability laws.

[232] GDPR, rec. 67.

The GDPR's latter sections defined fresh cues for mobility. The right to transfer data, which is closely related to the right of access but also dissimilar in many aspects, is covered by Article 20. The reason for the right to data portability may be traced back to a few distinct yet interconnected reasons that underpin this policy. Data portability remains one of the controversial matters under the GDPR, as in some opinions, it may hinder technological growth or enhance the free flow of personal data in keeping with the integrity as one of the objectives of the European Union Single Market.[233] This right enables data subjects to receive, in a structured, commonly used, machine-readable format, personal data that they have provided to the controller and send this personal data to another controller upon a request. The purpose of this article is to strengthen the position of the data subject and give the subject more control over personal information shared with the controller.[234] The right to data portability enables the transmission of personal data by one controller directly to another, so it is also an important tool that will support the free flow of personal data in the EU and encourage competition between controllers. It will also facilitate the change of service providers and thus foster the development of new services in the context of the digital single market strategy. Article 20 of the Regulation may be traced back to two main elements that formulate the scope of application of this law, namely: (1) the right for the data subject to receive, in a structured and commonly used format, the personal data entrusted to him or her, and (2) the right of the data subject to send personal data concerning him/her to another controller, without any obstacles from the controller. These rights may be exercised independently of each other and independently of the right to obtain copies of personal data (regulated by Article 15(3) GDPR). The right to data portability, on the other hand, supplements the right to access to personal data, and the differences between these rights can be seen in the fact that the right to data portability requires that data be provided in a machine-readable, generically used format, whereas the right to receive a copy and access to data does not specify any technical grounds and provides no further indications concerning interoperability. [235]

[233] Working Party 29 acknowledged the possibility of *fostering opportunities for innovation* (Article 29 Working Party, Guidelines on the Right to Data Portability, WP 242, April 2017), while the Commission supports the idea that strengthening the control over personal data flow that belongs to individuals may have a positive impact on startups.

[234] J. L. Grama, *Legal and Privacy Issues in Information Security*, Third Edition, Burlington, 2020, p. 58.

[235] W. Saffady, *Managing Information Risks: Threats, Vulnerabilities, and Responses*, Maryland, 2020, p. 228.

When it comes to the requirements placed by Article 20, it is necessary that:

a. *the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1);*
b. *and the processing is carried out by automated mean.*[236]

The possibility of transferring personal data from one service provider to another becomes particularly important in the case of services provided in the cloud computing model.[237] In such a case, the traditionally understood right of access to the data content is of little use in terms of enabling the cloud client to change the provider of such a service. This introduces the necessity of the so-called *data migration*, which automatically transfers data from a first controller to another. This action always takes place at the explicit request of the data owner, as a result of his clearly expressed will, and by automatic means of transfer. Encouragement to facilitate data transfer between controllers finds support in Recital 68 of the Regulation, which states that *data controllers should be encouraged to develop interoperable formats that enable data portability.*[238] In addition to providing consumer empowerment by preventing *lock-in*, which refers to the lack of ability to move personal data to another source, the right to data portability is expected to foster opportunities for innovation and the sharing of personal data between data controllers safely and securely under the data subject's control.[239] Furthermore, Recital 68 provides an exclusion to this obligation by stating that *it should therefore* ***not apply*** *where the processing of the personal data is* ***necessary for compliance with a legal obligation*** *to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.*[240] (emphasis added). What is more, Recital 73 finds its application in the case of the interpretation of Article 20 due to the explanation of the restriction that may be required by a Member State regarding the right exercised by the individual.

[236] GDPR, art. 20(1)(a)(b).

[237] V. Jain, G. Chaudhary, M. Cengiz, *Advances in Data Sciences, Security and Applications: Proceedings of ICDSSA 2019*, Singapore, 2020, p. 200.

[238] GDPR, rec. 68.

[239] Guidelines on the right to data portability, Adopted on 13 December 2016 As last Revised and adopted on 5 April 2017, Article 29 Data Protection Working Party, p. 5.

[240] GDPR, rec. 68.

From the perspective of underpinning values, the right to data portability remains a composition of interconnected yet distinct rationales. The scope of reasoning behind the right to data portability extends to the promotion of competitiveness between enterprises when it comes to data transfer[241]. During the legislative process, the idea of data portability already raised some concerns, for example, the United Kingdom referred to the right to data portability within the scope of competition or consumer law rather than the data processing law. Similar concerns were raised by Denmark, Germany, France, or Ireland.[242] At the same time, researchers on the subject matter question the right to data portability versus trade secrets that may be affected depending on the structure of stored data.[243] Even though, personal data are not, *per se*, trade secrets, it's worth noting that businesses and organizations that collect and process personal data have a legal obligation to protect the confidentiality and security of that data. By providing additional protection against the misuse of personal data by third parties, which will be enforced by the manufacturer, the manufacturer's trade secret protection may even serve the personal interests of the data subject. Nonetheless, disputes could occur when data subjects rely on their rights to data access, deletion, or portability. The Trade Secrets Directive and the GDPR have not consistently resolved the dispute in this regard. Particularly, Articles 15(4) and 20(4) of the GDPR should not be interpreted in a way that gives the data processor's trade secrets protection priority over the rights of the data subject.[244]

The next challenge in this regard arises from the concept of who is in charge of data control vs. who actually owns the data. It is currently well-recognized that the data controller may not be the only entity in exclusive possession of data and, in fact, may not personally perform all processing activities itself. As a consequence, the right to data portability becomes even more challenging as the definition of data controller *per se* seems to derive from different

[241] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.*, p. 499.

[242] *Ibid.*

[243] In some examples, data portability may refer to the disclosure of other information originating from the company that is obliged to transfer the data to another subject, as for example, the data structure that is associated with the database structure (which, for example, under multiple jurisdictions is considered to be protected by intellectual property and may be subjected to patent protection).

[244] J. Drexl, *Data Access and Control in the Era of Connected Devices Study on Behalf of the European Consumer Organisation BEUC*, Brussels 2008, p.11. Retrieved March 5, 2023 from https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf.

assumptions than Article 20 regarding data portability. In the subject of data privacy and protection, the idea of who is responsible for protecting and owning data is a complicated and developing topic. In the past, the data controller was frequently assumed to be the only party in charge of managing and regulating the data, and other parties who could have an interest in the data were frequently ignored. This viewpoint has been called into question recently, although, since then, it has become apparent that data ownership and control are not always the same thing. It is conceivable for different entities to be involved in various stages of data processing and for there to be several parties with a stake in the data. This complexity creates challenges when it comes to the right to data portability, which is enshrined in Article 20 of the General Data Protection Regulation. This right gives individuals the right to obtain their personal data from a data controller in a structured, commonly used, and machine-readable format, and to transmit that data to another data controller without hindrance. However, the definition of a *data controller,* as set out in the GDPR, may not always align with the requirements of Article 20. For example, a data controller may not be the only entity with access to the data or the party responsible for performing all processing activities. This mismatch between the definition of a data controller and the requirements of data portability can make it difficult for individuals to exercise their right to data portability effectively. It also creates challenges for organizations that need to comply with the GDPR and ensure that individuals are able to exercise their data protection rights. As a result, there is an ongoing debate and discussion around the concept of data ownership and control and how this relates to the right to data portability. This is an important issue that will continue to evolve as technology and data processing practices continue to advance.

It is worth mentioning that data portability remains one of the biggest challenges for data controllers due to the risk-based approach; in fact, there are many opportunities to face data breach risks and limited remedies defined by the GDPR to support controllers.[245] It remains even more challenging once we take into account that there is no clear minimum standard when it comes to processing and security measures (there is no detailed list of security measures that should apply to certain assets of data)[246]. What is more, the technical aspect of data controller

[245] Examples of data breaches that may be caused in the case of data transfer: interference during transfer between controllers or processors, access exercised by an individual in a fraudulent manner, unauthorized access to data on the device of the data subject.

[246] C. Bistolfi; L. Scudiero, *Bringing Your Data Everywhere in the Internet of (Every) Thing: A Legal Reading of the New Right to Portability*, European Data Law Review, 2017, pp. 119.

responsibility is difficult to grasp, and it lacks the specificity to draw any definition or standard. It becomes even more complex when it comes to different IT standards and programming languages. Working Party 29 suggests that there should be several options available for data subjects, such as, for example, direct data download or an Application Programming Interface (API) available to access the data.[247]

7. The right to object, automated decision making, and profiling.

The General Data Protection Regulation introduced an extensive right for the data subject to raise an objection and, as a consequence, place some focus on the control of data subjects over information processed as a central element of this legal act. In fact, the right to object may be traced back to two basis, namely, based on Article 21(1) of the GDPR, the general right to object, and based on Article 21(2), the right to object to direct marketing. The general right to object, as set out in Article 21(1) of the GDPR, allows individuals to object to the processing of their personal data on grounds relating to their particular situation, unless the data controller can demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the individual or for the establishment, exercise, or defense of legal claims. This means that individuals can object to the processing of their data where they have specific reasons for doing so, such as where the processing is causing them harm or is being carried out without their consent. However, data controllers may still be able to process the data if they can demonstrate that they have a compelling legitimate interest in doing so, or if they need to process the data for legal reasons.

The right to object to direct marketing, as set out in Article 21(2) of the GDPR, is a specific right that allows individuals to object to the processing of their personal data for purposes of direct marketing. This means that individuals can request that their personal data be no longer used for marketing purposes, and that they cease to receive any marketing communications. Unlike the general right to object, there are no specific exemptions or conditions that apply to the right to object to direct marketing. If an individual requests that their data no longer be used for marketing purposes, the data controller must comply with this request. In general, the right to object is a crucial data protection privilege that gives people control over their personal

[247] *Article 29 Working Party, Guidelines on the Right to Data Portability, WP 242*, 5 April 2017, p.5.

information. Individuals can safeguard their privacy and stop their personal information from being used in ways they do not approve of by using this right.[248] The conditions for exercising the *right to object* vary according to the type of processing. According to Article 21(1) of the Act, the data subject has the right to object at any time, on compelling grounds relating to his particular situation, to the processing of personal data concerning him based on Article 6(1)(e) or (f), including profiling under these provisions.[249] Such a right to object bars the controller from further processing activities if no other compelling grounds to facilitate such processing are presented. Article 21(1) states as follows: *the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*[250] Such an approach was to some extent known beforehand, as Article 14 of the Data Protection Directive (DPD), which also referred to two elements for the right to object - general and marketing.[251] Data Protection Directive,

[248] This scope was discussed by *Wirtschaftsakademie Schleswig-Holstein GmbH v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (CJEU, Judgment (Grand Chamber), *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*, Case C-210/16, June 2018. ECLI:EU:C:2018:388.). In this example, the German education provider Wirtschaftsakademie Schleswig-Holstein GmbH (WAS) has gathered and processed the personal information of its pupils, including their names, addresses, and dates of birth. The Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), which is responsible for protecting personal information in the German state of Schleswig-Holstein, has issued an order to WAS to cease processing this data. WAS challenged the ULD's decision in court, arguing that it had a legitimate interest in processing the data for the purposes of maintaining its student records and managing its educational programs. However, the ULD maintained that the processing was not lawful and that individuals had the right to object to the processing of their personal data. The case was referred to the ECJ, which ultimately ruled in favor of the ULD. The court held that individuals have a right to object to the processing of their personal data under Article 21 of the GDPR, and that this right can only be overridden if the data controller can demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the individual. The court also held that the legitimate interests of the data controller must be balanced against the rights and freedoms of the individual, and that the data controller must be able to demonstrate that their legitimate interests outweigh the individual's rights.

[249] M. Foulsham, B. Hitchen, A. Denley, *GDPR: How To Achieve and Maintain Compliance*, New York 2019, p. 31.

[250] GDPR, art. 21(1).

[251] After a careful analysis, Article 14 of DPD allowed Member States to derogate from the right to object under their discretionary power, which constitutes a big difference between the legal ground provided in DPD and GDPR. What is more, the burden of proof relied on the data subject requesting the right to object.

which stands for Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The DPD directive was a European Union directive adopted in 1995 and served as the primary legal framework for data protection in the European Union until it was replaced by the General Data Protection Regulation (GDPR) in 2018. When it comes to the specification of marketing communication objections, the issue has been a point of interest for the ePrivacy Directive as well. Article 13 of the Directive addresses the issue of data processing for the purpose of marketing, unsolicited communication and places certain standards on the processing itself. Because of this fact, article 13(2) of the ePrivacy Directive may be viewed as the *lex specialis* of the right to object based on the GDPR.[252] In its further parts of the GDPR, Article 21 specifies situations wherein individuals are entitled to raise objections to marketing processing stating that at any time, the data subject is fully entitled to object towards processing to the extent that processing of such data is made to fulfill marketing goals where ethical and data safety matter was always of a vast importance[253]. The implementation of the GDPR has had a real impact on the hitherto considered gray area relationship regarding the processing of personal data for marketing purposes.[254] So far, it has been quite common to acquire or build personal databases. These databases were, in many cases, processed without any time limits and without paying attention to the formal requirements of obtaining consent. The commented provisions of the Regulation not only give the right to object to the collected data but also force the administrators of personal data not to collect excess data but only those necessary for the assumed processing purposes.[255] It is especially important when considering the regulation's legal grounds for data processing. Unlike with certain Member States, data protection regulations under Directive 95/46 provides no special or independent legal footing for commercial scenarios such as marketing operations. As a result, data controllers must rely on the more general basis of Article 6(1) (a) to (f) to

[252] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[253] S. Sharma, *opt.cit.*, pp. 146-147.

[254] Direct Marketing Activities are also regulated by Recital 70 of the GDPR, which states that *[...] the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge*.

[255] M. Kołodziej, *Ochrona danych osobowych w marketingu internetowym po zmianie przepisów*, Warszawa, 2016, pp. 7-9.

justify processing for compliance with non-consent-based processing constraints in this respect.[256] Similarly, Article 89(1) of the Act underlines the right to object to processing in the case of scientific research and/or for statistics purposes. To draw the line between legal basis and legitimate processing, the approach of a balancing test is suggested to be user. GDPR as a legal act promotes the use of the balancing approach and, beside practice, the risk-based approach supposed to be the main way to weight rights included in the GDPR against the practical possibility to implement certain measures[257]. The approach states that whenever the controller receives an objection to the processing of personal data, such processing shall be ceased and deemed no longer valid until the moment of revealing the compelling legitimate interest of the controller for the processing.[258] The right to object remains of use only as long as there is a simple and available form of execution. Consequently, according to requirements put into place by the GDPR, objections may be raised in any form, and there is no need to justify such objections. Article 21 not only regulates the generic meaning of the right to object but also refers to profiling activities. By profiling, one shall understand automated, algorithm-based processes that classify data and, as the outcome, enables automated decision-making. Such mechanisms can be used to deliver behavioral advertisements, automated human behavior scoring, and other systems designed to provide tailor-made content for individual preferences. As such, the EU decided to comprehensively regulate profiling grounds and establish certain rules to the effect that:

- when is profiling allowed,
- what are the obligations related to profiling activities,
- what are the rights of profiled people, and
- in what cases a particularly sensitive automated decision-making system can be used, including systems that are making decisions based on previous profiling.[259]

[256] D. Rucker, T. Kugler, *opt.cit.*, pp. 75.

[257] In my opinion, balancing approach or the risk-based approach is the least used when it comes to the practical implementation of the GDPR what partially impairs how GDPR functions in practice.

[258] S. Sharma, *opt.cit.*, p. 221.

[259] GDPR, art. 22.

Recent cases law shows the heavy impact of profiling on individual rights correspond to the level of protection granted to the objection to profiling ensured by Regulation[260]. Due to the growing impact on individual rights of profiling activities, the GDPR states in Recital 69 that *a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation.*[261]

The approach taken by the GDPR differs not only from prior EU instruments but also from international ones. On the international level, the Modernized Convention 108 introduced the right to object. There is one substantial difference between the approach offered by the GDPR and Convention 108, namely the legitimate interest. Under the regime of the GDPR, legitimate grounds are used to justify processing performed by the data controller.[262] Convention 108 objections concerning data processing may be dismissed based on legitimate grounds[263]. Consequently, it creates a potential danger of underestimating the need to object to processing whenever it is not in line with a will or interest of the data controller, regardless of the interest of the data subject.

The issue of the right to *object* was also discussed by case law in the CJEU's *Nowak* case, and this case remains to this day to be an important element of the catalog of related case law. In the case, the court referred to the importance of the right to object as an element of individual rights of the data protection legal framework.[264] The right to object as a parallel to the right to erase the data was also touched upon in the *Manni*[265]. The case called for case-by-case assessment of the data to be collected in the Companies Registrar - National Public Administration Institution[266].

---

[260] An example of the heavy effects of processing on individual rights can be seen in the Cambridge Analytica case, where profiling activities based on Facebook affected the 2016 election in the United States of America based on the assumption of racial surroundings as well as behavioral practices performed by Facebook users.

[261] GDPR, rec. 69.

[262] GDPR, art. 6(1)(f).

[263] *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, art. 5(2).

[264] *Peter Nowak v Data Protection Commissioner,* Case C-434/16, *op. cit.*, para. 48.

[265] *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, Case C-398/15, *op. cit.*

[266] *Ibid*., para. 30.

The GDPR not only provided innovative input regarding the right to object, but it also regulated the automated individual decision-making, such being of vital interest in light of the right to object under Article 22 of the GDPR. Relevant recitals refer to the aim of processing as serving mankind, children's merits, or the right not to be a subject to the decision based solely on automated means.[267] *Travaux préparatoires* to the GDPR elaborate on the rationale of Article 22. Because of this, it is safe to assume that the shape of Article 22 as we know it today was highly impacted by prior Article 15 of the Data Protection Directive, that represents an early attempt to control automated decision-making affecting individuals. What is more, as mentioned in Recital 4, *the processing of personal data should be designed to serve mankind. The right to process personal data is not an absolute[...]*. It is right to believe that the logic behind this statement calls back to the idea of human dignity in the age of big data processing and automated means of decision making. Consequently, rights enshrined in Article 22 of the GDPR shall be interrelated to those rooted in Article 21 representing the right to object.

Data controllers, especially those who provide Software as a Service (SaaS) solutions, face a number of challenges and uncertainties when it comes to the right to object. One challenge is determining when an individual has the right to object to the processing of their personal data. Individuals have the right to object to the processing of their data under Article 21 of the GDPR on the basis of their unique situation, unless the data controller can provide compelling justification for the processing. Although it may not always be obvious if a person's circumstances qualify for an objection, data controllers may need to consult legal counsel or seek assistance from data protection authorities to ascertain whether an objection is legitimate. Making sure that people are fully informed of their right to object presents another difficulty. Data controllers must provide individuals with clear information about their right to object, including how to exercise the right and the consequences of doing so. This can be particularly challenging for SaaS providers, who may be providing services to individuals in multiple jurisdictions with different data protection laws and requirements.
The boundaries of the right to object may also be unclear, particularly in relation to direct marketing. Although individuals have the right to object to the processing of their data for direct marketing purposes under Article 21(2) of the GDPR, it is not always clear what falls

[267] Respectively included in rec. 4, rec. 38, rec. 71 of the GDPR.

within the scope of direct marketing or whether specific types of communications, like emails related to customer service or sales messages are exempt from the right to object.[268]

Lastly, while processing personal data, data controllers may struggle to strike a balance between their legitimate interests and the rights and freedoms of individuals. While the GDPR provides data controllers with some flexibility in determining when they can override an individual's right to object, it can be difficult to strike the right balance, particularly in cases where data controllers are relying on their legitimate interests for processing purposes. In summary, the right to object poses a number of challenges and uncertainties for data controllers, especially SaaS owners. These difficulties include figuring out whether a person has the right to object, effectively explaining the right to object to people, comprehending the boundaries of the right to object, and weighing legitimate interests against a person's rights and freedoms.

8. Individual rights derived from Article 5 of the General Data Protection Regulation.

Principles related to lawfulness, transparency of processing, or fairness are a key backbone of the European data processing approach. The principles of lawfulness, transparency of processing, and fairness are fundamental tenets of the European Union's data processing approach, as enshrined in the General Data Protection Regulation (GDPR). The principle of lawfulness requires that personal data be processed for specific and lawful purposes and that data subjects are duly informed of such purposes. Transparency of processing mandates that individuals be provided with clear and concise information concerning the processing activities, including the identity of the data controller, the purpose of the processing, and any other information necessary to ensure fair processing. The principle of fairness requires that personal data is processed in a manner that is fair to individuals, taking into account their rights and interests. These principles serve as a framework for ensuring that personal data is processed in a manner that respects the rights of data subjects, promotes transparency, and enhances trust in the digital economy, in line with the EU's broader objective of protecting fundamental rights and freedoms. The shape and main assumptions of this area have remained stable in the European jurisdiction for a while; the principles set forth by the 1980 OECD Guidelines and in

[268] At least from the perspective of market marketing communication is distinct from the sales communication and service messages that are delivered for the purpose of agreement fulfilment, and from practical perspective as the outcome of, for example, subscription purchase.

Convention 108 represent over 30 years of practical implementation of these rules.[269] Prior to the GDPR, the Data Protection Directive referred to a similar scope in its Article 6(1), but the GDPR brought a novelty in the principles of integrity and confidentiality that were not present in the previous act[270]. Aside from the rights directly named in the regulation, the GDPR enumerates some general principles that are applicable to the processing of personal data. Said principles are regulated by Article 5, which sets forth criteria placed upon the data controller while processing personal data. As a shortcut, the principles enumerated in Article 5 are as follows:

- lawfulness, fairness and transparency[271],
- purpose limitation[272],
- data minimisation[273],
- accuracy and up-to-date data[274],
- storage limitation[275],
- integrity and confidentiality[276].

What remains even more important is that Article 5 directly implies that the controller shall remain fully accountable for the processing of and compliance with the above-listed principles. Even though the list presented above constitutes a catalog of rules on how to process personal data; in fact, it can be reverted to the language of rights belonging to the individual while his or her data are being processed. What remains important in the scope of Article 5 interpretation is Recital 39 of the GDPR, which states a general principle that data shall always be processed in a lawful and fair manner. Recital 39 of the GDPR provides a crucial framework for

[269] Article 5 of Convention 108 is an inspiration for Article 6 of the Data Protection Directive and refers to a similar scope to that currently known in Article 5 of the GDPR, with some limitations. Furthermore, Modernized Convention 108 brings new ideas supporting the rights included there beforehand, such as notification duty under Article 7(2) or accountability measures in Article 10(1).

[270] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.*, p. 313.

[271] GDPR, art. 5(1)(a).

[272] GDPR, art. 5(1)(b).

[273] GDPR, art. 5(1)(c).

[274] GDPR, art. 5(1)(d).

[275] GDPR, art. 5(1)(e).

[276] GDPR, art. 5(1)(f).

interpreting the scope of Article 5 of the GDPR, which outlines the principles of data processing. In order to comply with the principle of lawfulness, data processing activities must have a clear and legitimate basis in law, such as consent or contractual obligation. Additionally, data processing must not exceed the purposes for which it was collected under the data processing and must be proportional to the legitimate purpose for which it was collected. The principle of fairness requires that data subjects be treated fairly and not be subjected to unfair or discriminatory processing. This includes considerations such as ensuring that data subjects are provided with clear and concise information about the processing activities, and that they are able to exercise their rights effectively. Taken together, the principle of lawful and fair processing reflects the importance of respecting individuals' fundamental rights to privacy and data protection, while also ensuring that data processing activities are carried out in a responsible and transparent manner. Compliance with this principle is essential for organizations to build and maintain trust with their customers, stakeholders, and the broader public.

The first part of Article 5 establishes the principle concerning the lawfulness of data processing. It is conceptually broad in nature. The meaning of this principle is quite simple to establish and relates to the whole *universum* of provisions under the Regulations. Article 6 of the GDPR is entitled: *Lawfulness of processing*[277]. The words *lawfulness* are thus a cross-reference clause to the title of Article 6 of the GDPR, which sets out the conditions for the admissibility of ordinary data. The grounds for the admissibility of processing sensitive data are found in Article 9(2) of the GDPR. Although Article 9(1) GDPR is entitled: *Processing of special categories of personal data*, undoubtedly Article 9(2) GDPR contains the prerequisites for the admissibility of the processing of sensitive data. On the other hand, as far as the processing of personal data relating to criminal convictions and infringements is concerned, the prerequisites for admissibility derive from Article 10 of the GDPR. It is worth mentioning that, apart from Recital 40, there is no definition or guideline for what lawfulness means[278]. One may argue

[277] M. Klamert, M. Kellerbauer, J. Tomkin, *Commentary on the EU: Treaties and the Charter of Fundamental Rights*, Oxford 2019, p. 408.

[278] Recital 40 of the GDPR reads as follows: *In order for processing to be lawful, personal data should be processed* ***on the basis of the consent*** *of the data subject concerned or some* ***other legitimate basis***, *laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation,* ***including the necessity for compliance with the legal obligation to which the controller is subject*** *or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data*

that the meaning is restricted to what is approved by Article 6 itself, but one could also argue that the concept of lawfulness extends beyond this legal act and encompasses a larger context. Another interpretation of the principle of lawfulness of personal data processing is the presumption that processing of personal data is usually forbidden unless there is an exception to such a restriction in the form of legal reasons stated by the GDPR.[279] The approach of *general prohibition with exceptions* is a legal concept that may be found, for example, in German jurisdiction and leads to the conclusion that processing is not allowed unless the case of several exceptions applies.[280] In this understanding, Recital 41 clarifies the meaning of the quality of legal basis as well as its legitimacy, namely, *where this Regulation refers to a legal basis or a legislative measure, this* ***does not necessarily require a legislative act adopted*** *by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned.*[281] This sentence clearly states that, without prejudice to the requirements of the constitutional order of the Member State concerned, there is no requirement of full legislative procedure to treat particular legal grounds as justifying data processing.[282]. Finally, when it comes to the legal grounds for data processing, Article 6 presents an exhaustive list of the same as follows:

- consent to the processing;
- processing is necessary for the performance of a contract that the data subject entered;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- processing is necessary for the purposes of the legitimate interests.[283]

subject prior to entering into a contract. Consequently, it points to the legitimate basis or consent as grounds further listed in Article 6 of this act.

[279] D. Rucker, T. Kugler, *opt.cit.*, p. 51.

[280] *Ibid.*

[281] GDPR, rec. 41.

[282] D. Rucker, T. Kugler, *opt.cit.*, p. 51-52.

[283] GDPR, Art. 6

The above-discussed article introduces grounds for permissibility for the processing of personal data. In the development of the principle of lawfulness of data processing, the commented provision defines the so-called grounds of permissibility of personal data processing. In the GDPR, an indication of the grounds on which the processing may be based has been made in the commented provision in relation to Article 9, which defines the division into sensitive and ordinary data. At this point, it is important to review the previously stated concept, which is based on the GDPR's Article 6 exceptions to the restriction on processing. Due to the open-ended and relatively broad language of Article 6(1)(f) of the GDPR, this interpretation has limitations as well as disadvantages. This is because, in accordance with the maxim *exceptiones non sunt extendendae*, provisions defining exceptions to the maxim should be written and interpreted strictly. It means that solely automated decision-making that is based on prior profiling cannot be carried out if it has significant effects on people, unless the decision is required for entering into or carrying out a contract between the data subject and a data controller, according to the Information Commissioner's Office, one of the most influential supervisory authorities.[284] Meanwhile, the premise of processing for the purposes of legitimate interests has so far been regarded as having a relatively broad scope of meaning. Reference to data obtained from illegal sources is also presented in the literature. Although there is no explicit provision in the GDPR concerning illegally acquired personal data, it can be concluded that the controller is obliged to process data in accordance with the law, which implies the necessity of lawful acquisition. To conclude the analysis of the provisions of Article 6 and the grounds for processing personal data contained therein, it is worth mentioning that the nature of these grounds is autonomous, namely, each circumstance listed in Article 6 of the GDPR justifies and/or mandates independent and equal processing[285].

Processing standards under which the data controller’s obligations must be carried out extend beyond the aforementioned principals and lawfulness of data processing; the principle of fairness requires mentioning as another core aspect of the processing standards. In particular, the GDPR states that the data controller must apply the following rules of the processing: that the processing must be either based on the individuals consent or on an authorizing law. The general prohibition against processing personal data therefore applies not only to the public but

[284]V.: A. Dróżdż, *Protection of Natural Persons with Regard to Automated Individual Decision- Making in the GDPR*, Alphen aan den Rijn, 2020.

[285] S. Lohsse, R. Schulze, D. Staudenmayer, *Data as Counter-Performance - Contract Law 2.0?*: *Münster Colloquia on EU Law*, Baden-Baden, 2020, p. 135.

also to the private sector thanks to the GDPR as well as Article 5 (1)(b) of the General Data Protection Regulation (the latter requiring that personal data be collected for *specified, explicit and legitimate purposes)*[286]. As emphasized in the legal sciences, the principle of fairness in the processing of personal data has a fundamental function, as it is the starting point for the formulation of the other principles of the processing of personal data, while covering them within its scope.[287] The content of the principle of fairness as defined is extremely broad. It can be interpreted as a command for controllers to take into account the interests and reasonable expectations of data subjects. Fairness in the processing of personal data is also sometimes understood as an obligation to process personal data with respect to the interests of the data subjects - fair information practices.[288] An example of fair processing practices and their relationship to fairness *is British Gas Trading Limited v. Data Protection Registrar*. In that case, a British court assumed that it violated the duty of fair processing to make data available for the marketing purposes of others without the express consent of the data subjects, particularly when the role of a monopolist in the market is at stake.[289] The principles of lawfulness and fairness lead to the following concept of the purpose limitation principle. It states that personal data should be collected for specified, explicit, and legitimate purposes and should not be further processed in a manner that is incompatible with those purposes. It further requires that the purpose of processing shall include narrow definition of the scope, explicit and legitimate purpose, consent and accountability for processing activities. The GDPR refers to this concept in nearly the same way as Directive 95/46 and implies it in a similar way[290]. This principle is responsible for limiting processing whenever possible to the narrow scope for which the data were collected. Furthermore, this principle is composed of two main elements:

- Personal data is collected for a specific purpose that is specified, explicit, and legitimate. It also remains necessary that the data subject is aware of such purpose and can access the information about the purpose of processing; and

[286] M. von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws*, Baden-Baden 2018, p. 235. Retrieved March 18, 2021 from https://www.jstor.org/stable/j.ctv941v5w.5.

[287] P. Litwiński, P. Barta, M. Kawecki, *opt.cit*, pp. 258-259.

[288] L. A. Bygrave, *Data Privacy Law: An International Perspectiv*e, Oxford, 2014, pp. 107-116.

[289]A. Savin, *EU Internet Law*, Third Edition, Cheltenham, 2020, p. 313.

[290] Directive 95/46, art. 6(1)(b) further stipulated in art. 5 (1)(b) of the GDPR.

- personal data are not further processed in a manner that is incompatible with those purposes, consequently if there is a change of the purpose of processing the consent or any other legitimate ground for data processing must be revised.

In other words, the aforementioned principal is intended to ensure that only the amount of personal data is collected that is needed and is otherwise limited to what is necessary to achieve the purpose(s) for which the data is being gathered and eventually processed.[291] Processing data in accordance with the purpose limitation principle leads to further risks for controllers, namely, access to the data by third parties and further use of personal data. It is important to note that the GDPR restricts the breadth of permission granted by the personal data subject to the shortest feasible scope. When a personal data subject consents, at least to some extent, to processing by an entity, care should be taken when transferring data to third parties and performing additional processing that may go beyond the scope of the original consent.[292] Consequently, this understanding of purpose limitation implies further questions as to how to define a specific purpose and when the purpose is sufficiently defined. Such questions were raised by Article 29 Data Protection Working Party, which stated that the definition of purpose needs to be specific enough to point out processing activities and determine types of processing.[293] Consequently, names of processing purposes with a broad scope of understanding, such as IT services, maintenance work, and user experience research, shall not be understood as precise enough to meet this requirement.[294] Of course, as usual, there is no one standard to follow in this regard, and there is also no universal prescription on how to manage this. The terms of the GDPR do not operate in full isolation; consequently, the evaluation of what purpose is specified and whether it is enough depends on the particular

[291] L. A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements (June 20, 2017)*, Oslo Law Review 2017, vol. 4, no. 2. p.108 Retrieved March 18, 2021 from https://ssrn.com/abstract=3035164.

[292] R. El-Gazzar, K. Stendal, *Examining How GDPR Challenges Emerging Technologies*, Journal of Information Policy 2020, vol. 10, pp. 259. Retrieved April 18, 2021 from https://www.jstor.org/stable/10.5325/jinfopoli.10.2020.0237.

[293] *Article 29 Data Protection Working Party, 00569/13/EN WP 203*, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, pp. 15.

[294] D. Rucker, T. Kugler, *opt.cit.*, p. 55.

context. Similarly to what was just described, GDPR indirectly assumes the explicit purpose of processing personal data, which shall be understood as unambiguous and clearly expressed with no hidden purposes.[295] It is important to keep in mind that compliance with explicit and legitimate processing also implies revision of processing assumptions. Depending on the type of business, technology, and social and cultural changes, the legitimacy of the purpose can change over time[296]. Analysis of the concepts of legitimacy and purpose limitation further leads to the (in)compatibility test requirement[297]. As stated in Directive 95/46 Article 6, there will be different standards among Member States. This approach is also visible in Annex 2 of the Commission Staff Working Paper Impact Assessment, where the Working Party stated that *the test to determine incompatibility varies from reasonable expectations of the data subject (in certain cases in Belgium) to application of balancing tests (Germany and the Netherlands), or it is intimately linked to other safeguarding principles of transparency, lawfulness and fairness.*[298] It is critical to note that the understanding of storage limitation exceptions is entirely dependent on agreement. To remain compliant with the GDPR and the compatibility test, one must prevent purpose changes in the first or subsequent processing. The next principle that requires further analysis and remains within the scope of the controller's responsibility is the data minimization principle enshrined in Article 5(1)(c). In simple terms, processing of personal data should be limited to what is necessary and avoid any extensive processing unless it is a must. Recital 39 of the GDPR supports the idea mentioned above by stating that personal data should only be processed if the purpose cannot reasonably be fulfilled by other means[299]. This standard is tightly connected with the requirement of storage limitations that require a strict minimum of time when it comes to data processing duration. The notion of necessity includes two dimensions of data processing, the factual element and the judgmental element. According to the factual approach, personal data processing is possible only to the extent that the relevant purpose's processing actually causally supports the fulfillment of the relevant purpose[300]. From a judgmental perspective, personal data may be processed only if and to the

[295] *Article 29 Data Protection Working Party, 00569/13/EN WP 203… opt.cit,* p.12.

[296] *Ibid.* p. 20.

[297] The legal ground for purpose limitation is expressly stated in art. 5(1)(b) of the GDPR.

[298] *Article 29 Data Protection Working Party, 00569/13/EN WP 203… opt.cit,* p. 10.

[299] C. Kuner, L. E., Bygrave, C. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, 2020, p. 317.

[300] D. Rucker, T. Kugler, *opt.cit.*, p. 66.

extent that the relevant purpose cannot be reasonably achieved by other means avoiding such processing[301].

Similarly to Directive 95/46 in Article 1(d), the GDPR also highlights that personal data should be accurate and kept up to date. Such requirements are expressed in a complex manner; nevertheless, Article 5 of the GDPR implies the purpose limitation and, in its further parts, stipulates the relation between the necessity of processing (purpose) and the erasure of data performed with undue delay. Once principles are extracted from Article 5 of the GDPR, it is possible to relate them further to Article 16 concerning the data subject's right to rectification, Article 17 related to erasure, and Article 18, which includes restrictions on processing. As explained above, in the short term, the accuracy principle refers to the concept of the factual state, and according to the definition offered by the Article 29 Working Party, it, in its broad sense, means *accurate as to the matter of fact.*[302.] The processing within what is limited to minimum necessary processing activity further implies time limitation, also known as data storage limitation. In fact, data may be necessary to be processed at one point, and the validity of such grounds for data processing activities may expire over time. Consequently, personal data shall be kept for no longer than what is necessary for the purposes for which it was collected.[303] The principle of data processing limitation aims to protect the data subject from the processing of his/her data in an unlimited and/or indefinite manner. The concept of limitation of processing is a known phenomenon across different jurisdictions. At the same time, Recital 39 of the GDPR brought some new nuances to the scope of storage limitation.[304] It requires the controller to name the time limitation and, in the case of any doubt, to explain the rationale behind such a period of processing (data retention time). Furthermore, Article 4(1)(f) of the Law Enforcement Directive includes a similar prohibition as GDPR and mandates that appropriate time limits for data erasure or a periodic review of data storage be established.[305] The current situation of the legislation in this respect necessitates the implementation of procedural safeguards to ensure compliance with the storage limitation

[301] *Ibid.*

[302] *Article 29 Data Protection Working Party, 00569/13/EN WP 203… opt.cit*, pp. 15.

[303] R. El-Gazzar, K. Stendal, *Examining How GDPR Challenges Emerging Technologies*, Journal of Information Policy Vol. 10, Penn State University Press… *opt.cit.*, p. 244

[304] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.*, pp. 318.

[305] *Ibid.*

processes. It is crucial to note that the GDPR does not specify any detailed terms that must be considered reasonable for data processing.

Finally, the GDPR addresses the complex concepts of integrity and confidentiality. It is mentioned briefly in Article 5 of the Act, but it is also mentioned in other areas, such as a complete section of Chapter IV of the GDPR that refers to the requirements imposed on data controllers and data processors, as well as the duty of security imposed on all processing activities. In a nutshell, this principle requires the controller to reprocess personal data in a manner that guarantees appropriate data security, including protection against unauthorized or illegal processing as well as accidental loss, destruction, or damage. This principle is further detailed under Article 32 of the GDPR.[306] It is important to mention that Article 32 of the GDPR reverts to the open-ended requirement of appropriate security, which extends companies' (controllers) duties regarding the security of personal data to an uncertain extent.[307] The Law Enforcement Directive includes similar articulations of the principle as presented by the fundamental protection principles included in Article 4(1)(f) and Articles 29-31 of the Law Enforcement Directive. The implementation of Article 5 of the GDPR poses several technological challenges for organizations operating in the IT industry. The principle of purpose limitation, which calls for the collection of personal data for specific, explicit, and legal objectives and prohibits further processing that is inconsistent with those goals, is one of the main issues. Since changing business operations may necessitate new or expanded purposes for processing personal data, this concept might present technical issues when businesses need to adjust or update their processing activities. For example, a company may decide to introduce a new product or service that requires the processing of additional personal data or may need to modify its data processing activities in response to changes in legal or regulatory requirements. When dealing with large datasets or intricate processing systems, it can be challenging to verify that the processing of personal data remains consistent with the original goals for which it was gathered. The principle of data minimization, which stipulates that personal data be limited to that which is essential in relation to the objectives for which it is processed, presents another significant obstacle. This principle can create technical challenges when dealing with legacy data systems, where data may be stored in large quantities or in

[306] Article 32 of the GDPR requires the personal data controller and processor to implement appropriate security measures justified in accordance with the risk analysis. Furthermore, it imposes an obligation to design processes and solutions in accordance with the *privacy by design* principle.

[307] D. Rucker, T. Kugler, *opt.cit.*, p. 72.

formats that are difficult to manage or process. For example, backup systems may store large volumes of personal data that are no longer needed for their original purposes, but that must be retained for compliance or legal reasons. In such cases, it can be challenging to balance the need for data retention against the requirements of data minimization and to ensure that personal data is processed only in accordance with the purposes for which it was collected. Finally, the principle of storage limitation, which requires that personal data be kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which the data was collected, can also pose technical challenges. This principle can conflict with the need to retain personal data for compliance or legal reasons, particularly when dealing with legacy systems or large volumes of data. In such cases, it can be challenging to balance the need for data retention against the requirements and limitations of data storage along with ensuring that personal data is processed only for as long as necessary and in accordance with applicable legal requirements. Overall, the implementation of Article 5 of the GDPR requires organizations in the IT industry to navigate a range of technical challenges related to data processing, data management, and data retention. To comply with these requirements, organizations must ensure that their data processing activities are designed and implemented in a manner that respects the principles of purpose limitation, data minimization, and storage limitation, while also meeting the needs of their business and legal requirements. Consequently, the broad scope and limited possibility of implementing the requirements of Article 5 in an agile manner typical for this industry, make it challenging and costly when it comes to the implementation challenges. At the same time, uncertainty and a lack of precise technical requirements make it even more demanding to implement the GDPR and the requirements of Article 5 in medium and small enterprises.

B. Scope of application of the GDPR and areas excluded from it under the current legal order.

The GDPR's territoriality is nuanced, and, controversially, the scope of Article 3 of this legislative act does not align with the common understanding of what is territoriality. The idea that a nation's laws apply solely within its geographical limits is referred to as territoriality of law. This indicates that a country has the ability to govern and regulate activities within its borders, but its laws do not extend beyond such bounds. This notion is widely accepted in international law and is a vital part of national sovereignty. The notion of state sovereignty serves as the legal foundation for the territoriality of law under international law. Under this principle, each state has the right to govern and regulate activities within its territory, and its laws apply within its borders. This principle is recognized in a number of international legal instruments, such as the United Nations Charter, which states that *nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state.*[308] Furthermore, the territorial principle is reflected in customary international law, which is a set of unwritten rules and principles widely accepted and followed by states. Another legal basis for the territoriality of the law is the principle of jurisdiction. Each state has jurisdiction over its territory and its nationals and can exercise jurisdiction over criminal and civil matters that occur within its territory. Finally, the principle of territoriality is also reflected in the concept of *extraterritoriality,* which allows for the application of a state's laws to certain activities that occur outside of its territory. For example, a state may exercise jurisdiction over a crime committed by one of its nationals abroad or over a company that is headquartered within its territory but operates in another country. It is also worth stating that the Union has a stable and undisputed territorial area, and the question of territoriality of law in this regard raises barely any questions or objections.[309] Nevertheless, what raises the rubric understanding of the aspect of the territorial application is the scope of Article 3, GDPR and the respectful recitals that apply in this relation. Article 3 regulates territoriality of the GDPR. The principle of territoriality of the GDPR has three main objectives: processing of personal data by the controller or processor established in the Union, processing of personal data of the citizens of the Union; processing of data of the citizens of the Union

[308] Charter of the United Nations, art. 7.

[309] C. Kuner, L. E., Bygrave, C. Docksey, *opt. cit.*, p.76.

even the controller or processor has the law of the Union implied by the virtue of international law[310]. Consequently, it becomes very visible that the scope of application of the GDPR has been extended by virtue of the processing of personal data of Union citizens outside the scope of its exact territory. Furthermore, the language of Article 3 may be unclear with regard to the requirement of the offering of goods and services on certain territories in the following scope:

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) *the monitoring of their behaviour as far as their behaviour takes place within the Union.*[311] (emphasis added).

Article 3 of the GDPR is constructed to include two criteria, namely, the offering of goods or services and the monitoring of citizens' behavior, as noted above. As far as the aforementioned definition seems to be obvious on the ground of some business activities, it may raise a complex question when viewed through the lenses of new technologies.[312] For now, the approach of the Union, as also visible in recent decisions such as *Schrems*, is heading in the direction of a more strict understanding of territoriality and a higher burden of responsibility placed on the data controllers. Such an approach, however strict, has stood for the underpinning values of the GDPR as an EU policy. The DPD, which was prior to the GDPR, already signaled the idea of extensive application of EU jurisdiction regarding territoriality. In *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein against Wirtschaftsakademie Schleswig-*

[310] GDPR, art. 3.

[311] GDPR, art. 3(2).

[312] The GDPR's territorial scope has been criticized for being overly broad and potentially leading to confusion and conflicting laws. One criticism is that it can be unclear when a company is considered to be "offering goods or services" to individuals in the EU, and it can be difficult for companies to know when they are subject to the GDPR's requirements. Another criticism is that it may lead to extra-territorial jurisdiction and enforcement, which can be seen as a potential violation of the sovereignty of non-EU countries. Additionally, the GDPR is seen as imposing a heavy compliance burden on small and medium-sized enterprises (SMEs) that may not have the resources to comply with the regulation, and this can be seen as a potential barrier to competition. It also raised concerns that it could lead to a "race to the bottom" in terms of data protection standards as companies may choose to base themselves in countries with weaker data protection laws to avoid complying with the GDPR.

Holstein GmbH, para. 26, it is stated that: [...] *the directive aims to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (judgment of 11 December 2014, Ryneš, C-212/13, EU:C:2014:2428, paragraph 27 and the case-law cited).* [313]

The quoted paragraph may be seen as the early notion standing behind support for a broader interpretation of the territorial scope. Nevertheless, the final underpinning value for Article 3 of the GDPR and territoriality is the aspiration of this act to be considered an element of international law. A clear indication of it was further raised by the amicus brief of the EU Commission in relation to the matter between the US and Microsoft Corporation (the *Microsoft Warrant* case)[314]. The Microsoft warrant case related to the General Data Protection Regulation and is officially known as *Data Protection Commission v. Microsoft Ireland Operations Limited*, Case No. 2019/218. The Irish High Court heard the case, which raised the question of whether Microsoft was compelled to cooperate with a request made by the US government to access data kept on servers in Ireland. This case is significant as it dealt with the intersection of U.S. law enforcement and GDPR data protection rights. The GDPR requires companies to protect personal data and gives individuals certain rights with regard to their personal data, including the right to know when their data is being accessed and the right to have their data deleted. Microsoft argued that the warrant issued by the U.S. government was in violation of these GDPR rights and that it, Microsoft, should not be required to comply with the warrant. The Irish DPC ultimately ruled in favor of Microsoft, stating that the warrant did not comply with the GDPR and that the company was not required to comply with it. The court found that the warrant would have required Microsoft to access data stored in Ireland and would have required it to disclose personal data in a manner that would have been incompatible with the rights of data subjects under the GDPR. As a result, the court ruled that Microsoft was not required to comply with the warrant and that the Irish Data Protection Commission (DPC) had correctly refused to enforce it. This outcome of the case was considered a landmark decision as it clarified how the GDPR applies in situations where foreign law enforcement authorities

[313] CJEU, Judgment (Grand Chamber), *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein against Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, June 2018. ECLI: ECLI:EU:C:2018:388, para. 26.

[314] *Data Protection Commission v. Microsoft Ireland Operations Limited*, Case no. 2019/218, [2019] IEHC 674.

request access to personal data stored in the EU and established that GDPR rights must be protected even when foreign authorities seek access to personal data stored in the EU. As proven by the presentation of underpinning values of the GDPR discussed above, territoriality is a complex and broadly understood subject matter. It further brings a number of consequences for both data controllers and processors, as well as for the execution of the law itself. The general approach of the Union towards cross-border obligations was disclosed by *Geigy*[315] and *Air Transport*[316]. Furthermore, the understanding as presented by the quoted cases has been shared by the EC as per its' amicus brief in Microsoft:

> *Any domestic law that creates cross-border obligations – whether enacted by the United States, the European Union, or another state – should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union's foundational treaties and case law enshrine the principles of 'mutual regard to the spheres of jurisdiction' of sovereign state and of the need to interpret and apply EU legislation in a manner that is consistent with international law*[317].

It is obvious that the goal of EU policy is to broaden the reach of influence beyond traditional territoriality, with a very wide narrative towards purpose and intent. While it remains innovative and inspiring to view the application of law from a purely practical perspective and its impact on individuals, it also raises a question about true respect for the sovereignty of other states/regions to decide about their laws and the potential for disagreement with the EU's jurisdiction.

For another perspective on the application of the CJEU and Article 3 of the GDPR and Article 4 of the DPD in particular, one need look no further than Google Spain[318]. A main question raised by *Google Spain* was in response to Google's line of defense that the main engine processing data, including personal data, is subject to the control of a US-based company, while the underlying complaint in this case was brought on the national level directly against a different company, namely, one registered to do business within, and purposefully subject itself

---

[315] CJEU, Judgment, *J. R. Geigy AG v Commission of the European Communities*, Case C-52/69, July 1972. ECLI:EU:C:1972:73, para. 11

[316] CJEU, Judgment (Grand Chamber), *Air Transport Association of America and Others v Secretary of State for Energy and Climate Change*, Case C-366/10, December 2011. ECLI:EU:C:2011:864, para. 123.

[317] EC amicus brief, *United States v Microsoft Corporation*, p.7.

[318] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, *op. cit.*.

to the local laws and regulations of, the territory of Spain. At the same time, the main issue of *Google Spain*, namely the above discussed *right to be forgotten* and whether or not Google, as a search engine operator, was responsible for personal data appearing in its search results and whether still Google should remove the personal data at the request of an individual, when the information in question is deemed to be inaccurate, inadequate, irrelevant, or excessive. The case centered around the issue of territorial jurisdiction, specifically whether or not the right to be forgotten applies to search engines worldwide or only within the European Union. In this case, the CJEU took the approach from a purely practical perspective and stated in paras. 55-56 of the judgment that the search engines are *inextricably linked,* which means that Google Inc. falls within the scope of Article 4(1)(a) DPD[319]. Other rulings of the CJEU further supported that the main aim of Article 4 DPD was to extend the scope of influence of the EU to the extent that it goes beyond territoriality and focuses on the aspects of undertakings that are directed towards EU member states' citizens[320].

The approach as presented by the CJEU is reasonable when it comes to a situation where the practical capability of exclusion of liability for actions comes into play. One can imagine a situation where a company registers to the business in the United States only to avoid EU jurisdiction over data processing. In such circumstances, the regulations of Article 3 of the GDPR seem reasonable. On the other hand, under circumstances of less harsh events, when the prescribed aim is not to disapply the law but to run a day to day business, the rule of Article 3 brings controversies and makes it even more difficult to rely on the law. It is so at least to the extent that a company registered to the business in California, first applies the CCPA and all federal laws and not the GDPR.[321]The fact that the exterritoriality of this act is claimed by the European practice creates a new challenge for the companies registered outside of the EU.

---

[319] *Ibid*., paras. 55-56.

[320] Such an approach was in particular supported by Verein für Konsumenteninformation against Amazon EU Sàrl, para. 82, (CJEU, Judgment (Third Chamber), *Verein für Konsumenteninformation v Amazon EU Sàrl*, Case C-191/15, July 2016. ECLI:EU:C:2016:612) where it was stated that: *processing of personal data and on the free movement of such data must be interpreted as meaning that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State. It is for the national court to ascertain whether that is the case.*

[321] CCPA stands for the California Consumer Privacy Act, which is US federal law relating to the processing of personal data of California citizens.

The above challenge is not the only one that arose on the basis of currently existing Article 3. The next difficulty refers to the scope of a non-EU data controller that uses an EU-based data processor. In such circumstances, the processor is formally bound to act in line with EU requirements, while for the non-EU data controller, such an obligation would be conditional upon the origin of the processed data. In such circumstances, it is, *in abstracto*, possible that the EU-based processor will notify the controller about data subject notice and the controller will ignore such a request as being bound by a separate set of legal requirements than the processor[322]. Looking from a broader perspective, Article 3 of the GDPR, and more precisely, Articles 3(2) and 3(3), implies a broad scope of application – even broader than initially implied by Article 4 of the DPD. The broad theoretical reach of Article 3 makes it difficult to assess its factual impact, and as a consequence, it is difficult to rely on its scope of applicability in this regard. Secondly, it is possible to argue that the scope of application itself is too broad and vague and otherwise difficult to justify, as it may apply to situations where the legitimate interest of the EU would be based more in theory than in fact. Lastly, all of the above makes Article 3 disruptive and difficult to apply in practice, which makes the application of Article 3 at best selective and otherwise based upon external circumstances.

On the other hand, GDPR itself, by virtue of Article 23, places some limitations on its applicability. In fact, the GDPR as a legal doctrine is not absolute but includes certain limitations that were foreseen by the European legislator. Article 23 of the General Data Protection Regulation (GDPR) deals with the processing of personal data for the purposes of the *prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*[323]. This is also referred to as *law enforcement processing*. This article sets out the conditions under which personal data can be processed for law enforcement purposes and the rights of individuals in relation to such processing. It also states that the Member States shall provide for specific and targeted measures for the protection of the rights and freedoms of the data subject, taking into account the nature of the processing and specific circumstances, in particular when the personal data are processed for the purposes of safeguarding against and preventing threats to public security. More precisely, the exemption from Article 23 lists national security, defense, and public security as categories of circumstances to consider when implementing this Article. This approach deserves a special place when it comes to the relations

[322] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.,* pp. 86-87.

[323] GDPR, art. 23.

between the EU and the US, and the material scope of application of the GDPR to the processing of personal information by national intelligence as an outcome of surveillance laws.[324] Consequently, the perspective on the orthodox approach of the European Union towards the processing of personal data based on the alleged surveillance law's applicability, which seems to undermine the mutual interest between the US and EU.

The European Union and the United States have a vital and important mutual interest in ensuring that data is processed in a manner that is both effective for law enforcement and protective of individuals' privacy rights. As an example of such context, one can refer to the anti-terrorism and national protection initiatives. In regard to fighting terrorism, both the EU and the US have implemented a number of agreements that allow for the sharing of information, such as the EU-US Terrorist Finance Tracking Program (TFTP) Agreement, the EU-US Passenger Name Record (PNR) Agreement, and the EU-US Joint Statement on Counterterrorism Cooperation, which all aim to improve the ability of law enforcement agencies to detect and prevent terrorist activities. Both the EU and the US also have a mutual interest in ensuring that data protection and privacy rights are respected when personal data is transferred across borders. For this reason, both the EU and the US have implemented robust data protection frameworks such as the EU-US Privacy Shield Framework, which governs the transfer of personal data from the EU to the US for commercial purposes and includes robust protections for the privacy rights of EU citizens. Additionally, both the EU and US have agreed on the General Data Protection Regulation and the California Consumer Privacy Act, which are the main data protection regulations for the EU and US, respectively. These regulations aim to ensure that individuals' personal data is protected and that organizations that process personal data are transparent about their data processing activities and are accountable for ensuring that

[324] At this point, it is important to notice that apart from international agreements like NATO, the EU and US share common interests with regard to a number of international instruments, such as: the EU-US Terrorist Finance Tracking Program (TFTP) Agreement, which allows for the exchange of financial transaction data for the purpose of detecting and preventing terrorist financing, and the EU-US Passenger Name Record (PNR) Agreement, which allows for the sharing of airline passenger data for the purpose of countering terrorism and serious crime, the EU-US Joint Statement on Counterterrorism Cooperation, which was adopted in 2016 and reaffirms the commitment of both the EU and the US to strengthen their cooperation in the fight against terrorism, the EU-US Extradition Agreement, which allows for the extradition of individuals between the EU and the US for crimes, including terrorism, the EU-US Cybersecurity and Data Protection Agreement, which aims to ensure strong and effective data protection for data transferred between the EU and the US for law enforcement purposes, including fighting terrorism.

data is processed in a manner that is lawful, secure, and in compliance with data protection principles.

While viewing this challenge from a purely practical perspective, *Schrems* remains a milestone in understanding the territoriality of GDPR as one of the areas subordinated to the jurisdiction of the EU.[325] Having in mind all of the above-mentioned areas excluded from the GDPR's force, *Schrems'* judgment pushes the boundary of what is covered by European jurisdiction even further. The judgment found that the Privacy Shield was invalid due to the level of surveillance by US authorities and the lack of adequate protection for EU citizens' personal data. It also stated that Standard Contractual Clauses(SCCs) can still be used for data transfers, but the data exporter and the data importer must assess and ensure the level of protection for personal data in the recipient country. If the level of protection is not adequate, the transfer cannot take place. Regarding the territoriality of the General Data Protection Regulation (GDPR), the Schrems II judgment affirmed that the GDPR applies to the processing of personal data by companies established in the EU, regardless of whether the data processing takes place within or outside the EU. This means that EU companies are required to comply with the GDPR even when they are processing data in third countries[326]. This excerpt shows that the GDPR applies to companies not established in the European Union when they are processing the personal data of EU citizens in relation to the offering of goods or services or the monitoring of their behavior within the EU. This confirms the territoriality of the GDPR and its application to companies processing EU citizens' personal data, even when they are located outside the EU. Concerns regarding the scope of territoriality as understood by the CJEU have been expressed, among others, by US Secretary of Commerce Wilbur Ross and US Secretary of State Mike Pompeo, who estimated possible adverse effects on the US$7.1 million transatlantic economic relationship[327]. At the opening remarks for the Schrems II judgment, Vice-President Jourova stated that the EU is dedicated to providing an alternative solution to facilitate EU-US

[325] *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Case C-311/18, *op. cit.*

[326] Such understanding was disclosed by §83 of the Schrems II judgment (Case C-311/18) in the following wording: *It follows that the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 4(2) of the GDPR, carried out in a Member State, and falls within the scope of that regulation under Article 2(1) thereof (see, by analogy, as regards Article 2(b) and Article 3(1) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 45 and the case-law cited).*

[327] European Parliament, at a glance, The CJEU judgment in the Schrems II case. Retrieved February 5, 2023 from https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

data transfer, but at the moment the only possible mechanisms to rely upon are the ones that are currently available for international data transfers.[328]

As of yet, the GDPR's territoriality and, indeed, its scope of applicability are uncertain. In terms of territoriality, GDPR extends its coverage beyond the EU's recognized borders to the extent of impact or location where personal data of EU persons is processed. On the other hand, according to the CJEU's view, the scope initially excluded from its authority as national security, countering terrorism, justifies its rejection of data transmission to other nations (US). Consequently, the scope of application of the GDPR may be considered debatable, and what flows after that is the difficulty of relying on the law thereby posing an important implementation challenge. For any data controller or data processor to be able to apply the law, it remains necessary that the obligation to do so exists. Following that, a technical disadvantage emerges: the majority of databases do not support low-cost unique record extraction, which is required when exercising the right to be forgotten. As a result of the foregoing, the GDPR's early implementation presents two significant challenges: (1) being vague and currently broadening its field of applicability, as demonstrated by *Schrems II*; and (2) being technically ambiguous and difficult to rely on.

[328] European Commission, Opening remarks by Vice-President Jourová and Commissioner Reynders at the press point following the judgment in case C-311/18 *Facebook Ireland and Schrems*. Retrieved February 5, 2023 from https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366.

Chapter III: Idea of the responsibilities of the data controller and a risk-based approach in the practical application of the GDPR to the right to be forgotten and data transfer laws.

A. Definition of a data controller and its challenges under current practice.

The data controller defines the objectives for which personal data is processed as well as the means of processing. As a result, whenever any subject processing personal data, including governmental authorities, private sector corporations, or NGOs, chooses *why* and *how* data should be processed, this actor appears as a data controller. Furthermore, as the main actor bound by the GDPR, the controller, bears the broadest scope of responsibility and liability for data protection compliance. Its responsibility extends to all employees and representatives acting on behalf of the company and thus performing the data controller's tasks. GDPR assumes that there are two models of data control, namely individual and joint. A party is considered a joint controller if, with another entity, it jointly sets the goals and means of processing personal data with one or more organizations. To replicate the role of joint controllers, such actors are legally required to enter into agreements outlining their respective duties for GDPR compliance.

A situation in which two or more entities jointly define the aims and means of processing personal data is referred to as *joint controlling*. In this scenario, the controller's responsibility is to guarantee that all parties participating in the joint control arrangement abide by data protection rules and regulations. The controller, as the entity responsible for ensuring compliance with data protection laws, must communicate the main aspects of the arrangements to the individuals whose data is being processed, including the purposes and legal basis for the processing, the categories of personal data being processed, the recipients or categories of recipients of the data, and the individuals' rights with respect to their data. The controller must also guarantee that any personal data transfers between joint controllers are carried out in accordance with data protection laws and regulations. Apart from the data controller, GDPR assumes another important function in data processing, namely the data processor, which carries out the processing of personal data solely on behalf of the controller. The data processor is usually a third party, i.e., an entity external to the company. However, in the case of groups

of companies, one company may act as a processor for another company. The obligations of the processor to the controller must be specified in a contract or other legal act. The contract must, for example, indicate actions taken on the personal data upon termination of the contract. A typical activity of a processor is the provision of IT solutions, including cloud storage services. A data processor may subcontract part of its duties to another processor or appoint a co-processor only with the prior written consent of the controller. The complexity of roles performed during data processing creates the possibility that an entity may be either a controller or a processor, or perform both. The data controller's accountability is unquestionable under the GDPR, and as a result, the controller is in a position to bear complete responsibility for processing operations for itself and suppliers acting as processors or subprocessors. Up-to-date data processing law in the EU guarantees a number of judicial remedies and a threshold of responsibility for data processing relying on the controller. As GDPR attempts to face modern challenges arising from technological growth, an approach towards a risk-based definition of what's allowable has been taken. In general, risk assessment is a combined effort: identifying and analyzing potential events that could adversely affect people, property, and/or the environment; and making judgments *on the acceptability of risk based on risk analysis* that take into account influencing factors. The matter of risks and available remedies has been raised, among others, in Case C-311/18[329].

Aspects of the data controller's responsibility, its precise definition, and the risks placed by the GDPR on data controllers shall be described in the following parts of Chapter III.

The concept of data controller has been known in the field of data processing for a while, and it functions in multiple legal acts, such as the LED Directive (Directive EU 2016/680) under 3(8), the definition of the controller, or the EUDPR (Regulation EU 2018/1725) that in the very same article refers to the definition. The role is crucial from the logical perspective of responsibility implication, which is why in other foreign jurisdictions, for example, the California Consumer Privacy Act, the US legislator decided to appoint the role of service provider to address the needs of the key entity in charge while processing personal data. Similarly, other international instruments aside from the GDPR bring the idea of a data controller to the stage. A *data controller* as a function described under the GDPR, means that an entity or person is responsible for the course of events during data processing activities, including aims, purpose, scope, and all further elements of processing. The person who is competent according to factual authority to decide about the purpose and mean of certain

[329] *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, Case C-311/18, *op.cit.*

actions[330]. In fact, it would be impossible to organize functioning data protection standards with no indication of the main, responsible entity in the process, and that is why controllers are key actors in the operationalization of data protection laws as they are the main subject of obligations imposed by this law.

The idea of a controller shall be interpreted in the light of purpose interpretation with special focus on the effective decisiveness over data processing activities. As the Article 29 Working Party rightly pointed out, the concept is of a functional character, and its purpose is to allocate responsibility where factual influence is in place, even if there is a disproportion between formal and factual influence[331]. A concise explanation of the GDPR definition of *data controller* is provided in Article 4(7), which reads as follows: *'controller' means the* ***natural or legal person****, public authority, agency or other body which,* ***alone or jointly with others****,* ***determines*** *the* ***purposes and means of the processing*** *of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*[332]*. (emphasis added)*

Consequently, Article 4(7) places some minimum criteria for the controller definition, namely:

- *natural or legal person* - this element of definition implies that, in fact, there is no limit on who may be considered to be the controller.
- *determines* - the second element of the definition is viewed by virtue of influence and decision-making power. The definition as offered by the GDPR requires control over the purpose and goal of data processing. What is important, control and decision-making power are not equalized with access, and this abstract definition is capacious enough to encompass decisiveness grounded only in instructions and not in operational

[330] Convention 108 originally adopted a definition of controller of the file to address the role of a person who is in charge of the purpose of an automated data file and the data stored on this file.

[331] This approach was directly expressed in the case of Fashion ID by the Advocate General Bobek (CJEU, Judgment (Second Chamber), *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, Case C-40/17, July 2019. ECLI:EU:C:2019:629.) where the ECJ discussed that the operator of a website that features a Facebook 'Like' button can be a controller jointly with Facebook in respect of the collection and transmission to Facebook of the personal data of visitors to its website. EJC has further highlighted that GDPR largely inherits from Directive 95/46 and that the understanding of terms included shall be coherent. In fact, going against interpretation at the option of the Court would be surprising.

[332] GDPR, art. 4(7).

access. What is important is that the definition of the controller be factual and practical rather than theoretical in the absence of legal provisions, based on the analysis of the factual circumstances surrounding the processing.

- *alone or jointly with others* - definition of the controller as provided by Article 4(7) of the GDPR assumes that there may be more than one actor deciding about the processing. This implies that several different entities may act as controllers for the same processing.
- *purpose and means* - this element constitutes a substantive part of the definition and means that the controller is in full charge of the anticipated outcome that is intended or that guides your planned actions arising from data processing. It remains especially important while taking into account that data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. The purpose and means question will also refer to the essential versus nonessential elements of processing when it comes to the relationship between controller and processor. The definition as provided by the GDPR highlights that the controller shall have a role in essential processing decisions, while those of an implementation character may be left to the processors to decide with no migration of the role of data controller to the processors.
- *of the processing* - the last building block of the definition of data controller is purely a reference to the processing activities themselves. The role of the data controller remains important only to the extent that it is associated with the processing of personal data. Furthermore, the concept of a controller may involve either a single processing operation or a set of operations. In practice, this may mean that the control exercised by a particular entity may extend to the entirety of processing at issue but may also be limited to a particular stage in the processing.[333]

With an emphasis on determining the controller status, attention should be paid to the data subject's perspective, real allocation of responsibility/control, contractual allocation, or the

[333] In *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV,* , Case C-40/17, *op. cit.,* para. 74 states: *(A)s the Advocate General noted, [...-] it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means. By contrast, [...] that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means*.

assignment of such a role to the outcome of other legal instruments. It is worth mentioning that an entity may be recognized as a data controller even if its legal mandate states otherwise. What is more, when it comes to practical aspects of implementation (*non-essential means),* such matters may be left to the processor. It is not necessary that the controller to actually have access to the data that is being processed to be qualified as a controller.

From the organizational perspective, the controller can be equated to rather than be considered a mere member only of an organization at issue. Once the data controller is discussed, reference to any one organization individual, such as its CEO or any other executive board member takes a back seat to attributing controller actions to the entirety of the organization.[334] An interesting question was posed in the *Jehovah's Witnesses* case, namely, the CJEU was asked to determine if the community of Jehovah's Witnesses is a data controller of the data collected by the community's individual member's door-to-door activities.[335] Initial argumentation the Jehovah's Witnesses was that such actions were independently taken by its members. In the response to the prejudicial question with the case quoted above, the CJEU responded that, *However, a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46.*[336] Accordingly, in this case, the Court took the approach of effectively determining who is in charge of making a decision about the processing – who is the controller. After such a factual evaluation, it became clear that the organization, as well as coordination and further encouragement to perform actions, were carried out by the Jehovah's Witnesses Community, and thus the community meets the criterion of the data controller by definition.

We can clearly observe the backdrop of action attribution in such example[337]. The attribution of action done by independent contractors to the corporation is a comparable idea that is especially significant in the sphere of data processing and new technologies. If, as based on the case of *Jehovah's Witnesses*, an independent entrepreneur performs a service for a company,

---

[334] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 Adopted on 02 September 2020, p. 3. Retrieved November 11, 2021 from https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

[335] CJEU, Judgment (Grand Chamber), *Proceedings brought by Tietosuojavaltuutettu*, Case C-25/17, July 2018. ECLI:EU:C:2018:551.

[336] *Ibid.*, para. 68.

[337] The controller is the entity to which the practical impact over the decision to process personal data may be assigned. The processor is the entity acting on behalf of the controller.

but the company remains in a position to decide about the mean, goal and purpose of such processing, the company shall be understood as a data controller.[338] Further functional understanding of the data controller was given by the CJEU *Google Spain* case[339] where the Court in para. 38 states as follows:

> *Inasmuch as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.*

From a purely practical standpoint, this implies that the data controller's perspective is always upheld by an effective appraisal of who can decide on the objective and purpose of processing. When it comes to market monopolists like Google, this strategy appears to be extremely natural because such large entities independently decide about their scope and purpose of data processing and any attempt to control this either contractually or effectively is likely to fail. However, when it comes to the practical operation within the IT market, the role of the data controller may be less obvious. Currently, the IT market, which is at its most sensitive when it comes to data processing, is heavily reliant on global corporations, which are only partially affected by the definition of data controller *per se.*

A big part of the market is currently dependent on the role of companies such as Google, and in fact, in a growing number of use cases, Google will be considered a data processor acting on behalf of data controllers. To understand deeply the idea of a data controller and the missing parts, one can use the example of a medium and small size company. Currently, to research, market, or store files, a growing number of companies are searching for cloud solutions to reduce costs and handle the challenges arising, among others, from remote work.

[338] Among other examples, one can list a situation where developers or analysts perform services on behalf of the company. Even if there is no direct employment relationship between these two subjects, the practical subordination of the developer or data analyst to the company shall place the obligation of the data controller on the company due to no decisive power on the side of either developer or data analyst. Even though in both professions there is a dose of technological know-how that requires independent decision making, milestones regarding how personal data are processed will usually be assigned to the decision-making process of the company.

[339], *Google Spain…*,Case C-131-/12, *op. cit.,* paras 36-38.

Consequently, data processing on a daily basis shall be distributed among multiple sources and, as a consequence, depend on the processors or sub-processors quality of service. In fact, as the controller, you are in a position to take responsibility for the processing of the data subjects' personal information, we stand in front of the question – can any data controller in fact affect it? Most service providers, including software as a service (SaaS) and platform as a service (PaaS) providers, or cloud service providers, recognize themselves as data processors acting in accordance with the instructions of the data controller.

Currently, Google remains one of the most recognized search engines, owning around 85% of the market share worldwide. The statistics starting from 2010 show that the market share decreased from around 90%; nevertheless, the role of global market leader remains untouched.

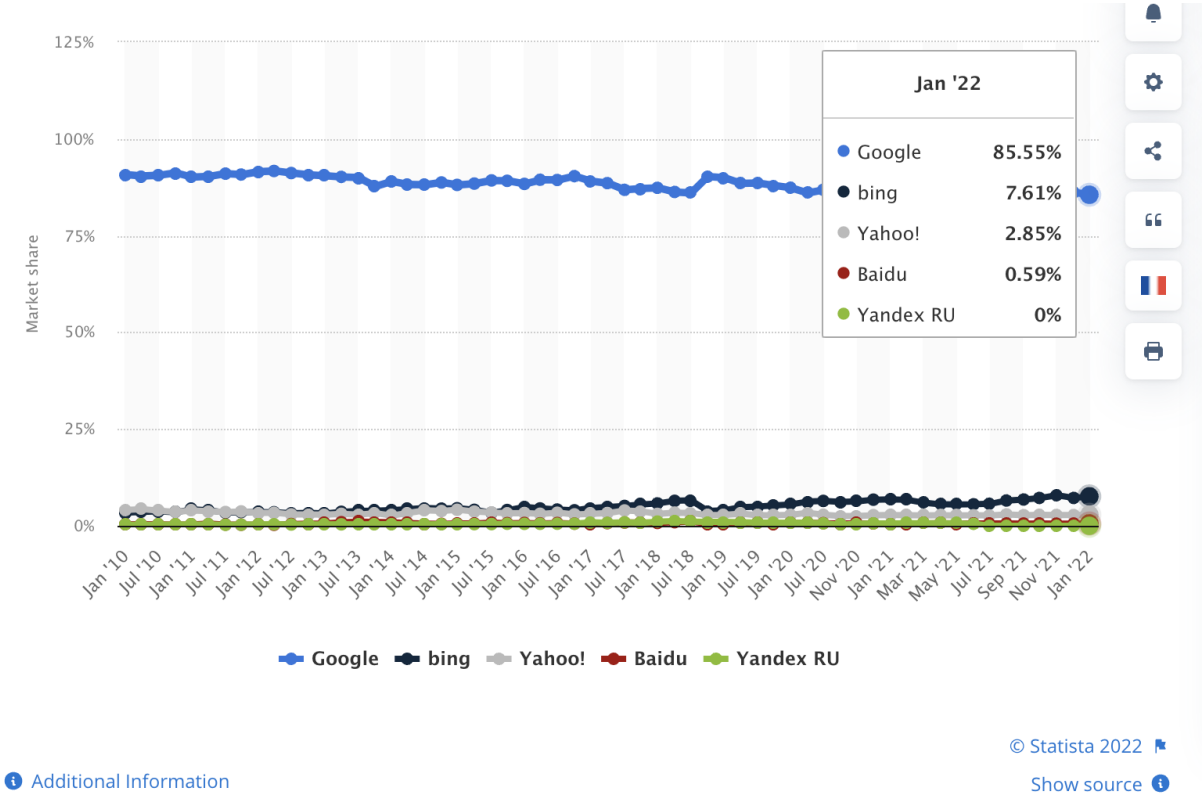


***Figure 1**: Worldwide desktop market share of leading search engines from January 2010 to January 2022* [340].

Similarly, with file storage, according to a *Datanyze* assessment, Google Drive as a storage service owns around 33% of the global market share.

[340] Worldwide desktop market shares of leading search engines from January 2010 to January 2022. Retrieved June 20, 2022 from https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/.

Of course, the question is not about Google as a provider, but about the role of data controllers and their factual impact on the data processing activities.

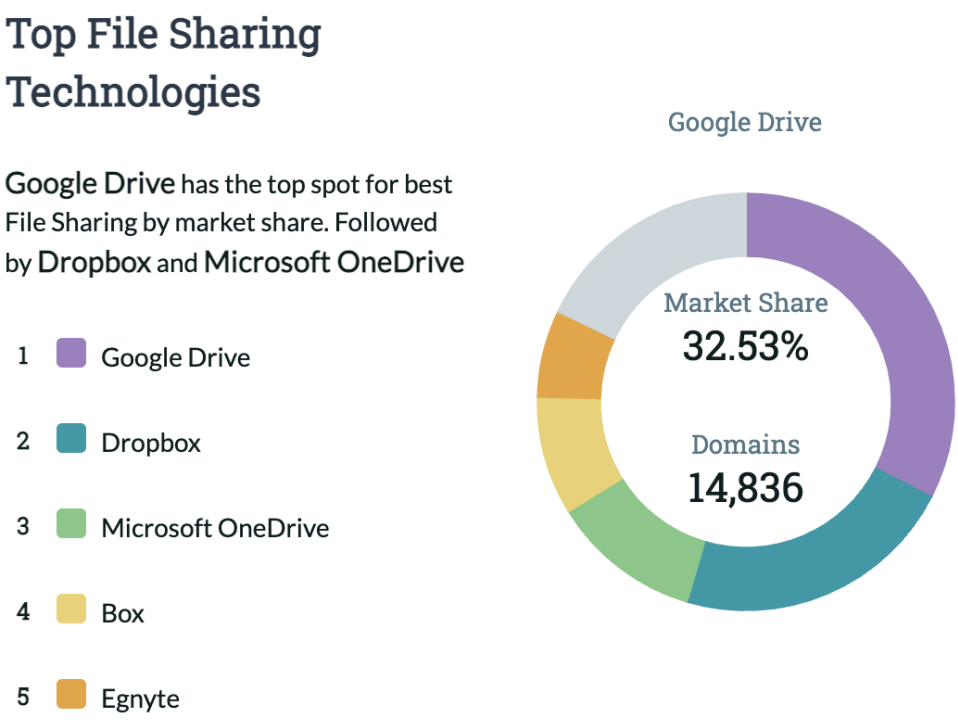


***Figure 2**: Datanyze assessment of file storage market share globally, with the highlight on Google Drive share*[341].

In clause 5 of the Data Processing and Security Terms (Customers), Google defines itself according to the definition below:

*Google is a **processor** of that Customer Personal Data under European Data Protection Law* [342].

Consequently, in all cases where any company decides to use Google Drive or conduct a Google search, there is implied consent for the way Google operates. Such an approach seems obvious; nevertheless, it to some extent clashes with the approach to real control doctrine as

[341] Datanyze assessment of file storage market share globally. Retrieved June 20, 2022 from https://www.datanyze.com/market-share/file-sharing--198.

[342] Google Cloud Data Processing Addendum (Customers). Retrieved June 20, 2022 from https://cloud.google.com/terms/data-processing-terms.

disclosed above. In fact, the majority of service providers assume that the customer is a data controller, with no possibility for the data controller to affect processing activities.

In fact, the very same policy implies the acceptance of Google's security standards by the data controller under point 7 of this policy:

*Customer **agrees** that the Services, Security Measures implemented and maintained by Google, Additional Security Controls and Google's commitments under this Section 7 (Data Security) **provide a level of security appropriate to the risk to Customer Data** (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals)*[343].

From the perspective of the agreement, of course, such information falls within the scope of freedom of contract; nevertheless, it misses the possibility for the data controller to share the responsibility with the data processor. It is important to observe that the obligation to rely on data controllers is composed of three elements to comply with, namely:

- Principles - those codified directly in the GDPR and all supplementary legal acts (as quoted in Chapter II of this thesis),
- Prior information requirements - this mirrors the obligation to inform data subjects about the scope of processing and all conditions that shall affect the processing of personal information and that may affect individual rights[344], and
- Lawful processing conditions - in fact, the principles described in point a above are not an exhaustive list of processing requirements. Risk-based approach implies the obligation to monitor the quality of processing and even processing that from formal perspective meet the requirements of principles laid down in the GDPR from a practical perspective of possible data integrity and security infringement may be considered insufficient[345].

Despite the fact that the data controller remains in a position to choose an appointed processor, such a guarantee seems to be void when it comes to the real functioning of the IT service provider market, where the majority of services are provided on an *as-is* basis. This known practice remains typical for cloud environments, including SaaS. The *as-is clause* usually refers to the fact that software provided in the form of a service is delivered only in the form currently

[343] *Ibid*. pp. 7.

[344] Prior information obligation relies on Chapter III of the GDPR requirement regarding the rights of individual data subjects and precisely on the requirements of Section I including transparency and modalities.

[345] P. Lambert, *Understanding the New European Data Protection Rules*, Boca Ratón 2018, p. 134.

available. In practice, it means that there is no possibility for the data controller or any other entity to shape the way the service works.

The challenges arising from the marketplace leaders remain only one perspective on the challenges of data controllers and the selection of data processors. In fact, the purchase of certain market-recognized solutions implies purchasing a bundle. Market leaders usually place more than one product or exclude the possibility of integration with any other tool than the one developed by them. For example, Google LLC delivers a group of products that are natively integrated one into another. The use of Gmail automatically implies Google Workspace, including Google drive[346]. It remains a popular practice to sell software in packages, and some of those use built-in sub-products to upsell the customer or differentiate the onboarding process. In such circumstances, the ability of the data controller to exclude any scope of data transfer is only fictional and creates the illusion of a real impact on the shape of processing activities, while currently available market solutions, especially cloud-based SaaS or PaaS, are delivered only as-is. Currently, we can observe a tendency to force the open-up of the software providers to other technologies, the growth of API aggregators as Zapier paves the way for cross-provider integrations. Such practice is also supported by the European Commission and all legislative movements supporting fair competition. Before this openness stands as a standard, the ability of the data controller to really select the processor will be even more foreign and difficult to execute in practice. Under such circumstances, the data controller needs to balance the question of whether the data processor forces data transfer once delivering the software in bundles or while using sub-processors necessary to deliver the service? Such forcing of a transfer, whether intentional or not, is a real problem, generating liability strictly on the part of the data controller.

Article 4(8) of the GDPR and further Article 28 and recital 81 provide a definition of a processor and describe his close relation to the data controller. The aim of introducing the role

[346] Even from a simple perspective, clicking on the attachment to an email received via a Gmail account creates a draft file on Google Drive, and such functionality is always promoted and supported by Google LLC as a provider. On the other hand, one can use communication channels where the customer contacts the company through instant messaging. Such channels usually imply an asynchronous communication mode that transfers the communication from the instant chat channel to email, WhatsApp, or any other configured tool. Under such circumstances, the data subject is barely aware and has no possibility to withdraw the content of such data transfers, and the data controller, while using such solutions, has almost no possibility to exclude, limit, or affect data transfers.

of the processor was the operationalization of data protection laws[347]. In fact, GDPR itself was a step towards the broader responsibility of data processors compared to DPD[348].

In fact, the risks presented above regarding data processing in a cloud computing environment were noticed by the Working Party Group in 2012 in Opinion 05/2012 on Cloud Computing. The Working Party Group referred directly to the lack of control and issues with confidentiality as well as integrity[349]. In fact, in 2012, the WP29 opinion directly stated that the responsibility for cloud computing environments lies in the hands of the data controller, who is the customer of Cloud service [350]. Such an approach seems to be the most accessible from the perspective of making an entity reliable; nevertheless, the practical approach raises a practical question. If the processor is understood as the agent of the data controller and the data controller remains the entity to decide about processing, how does the currently known legislation support the data controller to effectively undertake the responsibility for data processors? From a purely formal perspective, the distinction between the data controller and data processor seems to be the obvious one; nevertheless, looking at the practical side of the growing IT industry, it seems to bring some technical challenges for data controllers to use the services of more powerful providers like Google due to inequality of resources and enforcement options. Even though Article 4(8) of the GDPR provides only a general understanding of the role of the data processor, Article 28(1) of the GDPR brings clarity towards an understanding of the role, namely that the controller shall use only processors that ensure guarantees assessed as appropriate. From a practical perspective, GDPR includes an extensive scope of responsibility for the data controller, including responsibility for all actions of the data processor. In fact, the data controller stands in a role that seems to be similar to that of a *bad guy* who wishes mostly to know the law and be able to foresee the consequences. Unfortunately, the GDPR, in my opinion, pushes the responsibility towards the data controller in an extensive but also hard to rely on way. Technological advancement, along with the need to defend people's rights, necessitates a growing focus on the enforcement of rules in order to ensure the law's application in practice. In the next sections of the thesis, it will lay out the risk-based strategy, which strives to balance the duties of the controller and, as a result, offer a stable operating environment

[347] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.,* p. 157.

[348] DPD, art. 30(2) or 33(2) refers to the role of data processor.

[349] *Ibid.,* art. 29 .

[350] *Ibid*., p. 7, the cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organization.

1. Definition of data controller responsibilities under the GDPR.

The General Data Protection Regulation defines a *data controller* as a person or organization that determines the purposes for and means of processing personal data. As a data controller, he or she is responsible for ensuring that the processing of personal data complies with the GDPR, including protecting the rights of data subjects and implementing appropriate technical and organizational measures to secure the data. The data controller is also responsible for cooperating with data protection authorities and reporting personal data breaches to them when required. Being a data controller under the General Data Protection Regulation comes with several risks, including:

- Legal liability: Data controllers can be held legally responsible for non-compliance with the GDPR, which can result in significant fines and reputational damage. The fines under the GDPR can be substantial, with the maximum fine for a single infringement being up to €20 million, or 4% of the company's global annual revenue, whichever is higher[351]. Reputational damage, on the other hand, can have far-reaching and long-lasting effects on an organization's credibility, trust, and public perception, and can be even more costly in the long run. The exact impact of reputational damage under GDPR is subjective and dependent on various factors, such as the nature and severity of the violation, the industry, the size and reputation of the organization, and the responsiveness and transparency of the company in addressing the issue.
- Data breaches: Data controllers are responsible for protecting personal data from unauthorized access, theft, or loss, and must report data breaches to the relevant authorities within 72 hours.[352]
- Compliance costs: Implementing and maintaining compliance with the GDPR can be costly, especially for small and medium-sized organizations. Furthermore, practical implementation of the GDPR usually requires technical and legal support. Especially with regard to IT solutions, where small and medium enterprises rely on ready-to-use market solutions as the only possible solution to affect the scope of processing and verify the scope of processing that the controller takes responsibility for is on the formal level of the agreement that implies the need of external legal assistance.

[351] GDPR, article 83.

[352] GDPR, article 33.

- Reputation damage: Non-compliance with the GDPR can harm a data controller's reputation and damage customer trust.[353]
- Data subject complaints: Data controllers may face complaints from data subjects regarding the processing of their personal data, which can lead to costly legal proceedings.[354]

It's important for data controllers to understand these risks and take appropriate measures to mitigate them, such as implementing effective data protection measures, conducting regular data protection impact assessments, conducting transfer impact assessments, and keeping up-to-date with changes to the GDPR along with the GDPR interpretation offered by the CJEU. Furthermore, the principle of accountability in the GDPR is a cornerstone of the regulation, which requires organizations to take responsibility for their data protection practices and demonstrate that they are in compliance with the GDPR. The principle of accountability requires organizations to:

- Adopt appropriate technical and organizational measures to ensure that they process personal data in a lawful and secure manner.
- Keep records of their data processing activities, including a description of the categories of data processed, the purposes of processing, and the measures taken to ensure the protection of personal data.
- Designate a Data Protection Officer (DPO) if necessary.

[353] One example of a company that faced reputational damage due to a data breach under GDPR is British Airways. The UK's Information Commissioner's Office (ICO) penalized the corporation £183 million ($230 million) in 2018 for a data breach that exposed the personal and financial information of over 400,000 clients.

The breach, which was attributed to a vulnerability in the company's website and mobile app, led to significant public backlash and a loss of customer trust, which had a lasting impact on British Airways' reputation. The company faced widespread criticism for its handling of the breach, which was seen as slow and inadequate, further exacerbating the damage to its reputation.

[354] Data controllers can receive complaints from data subjects regarding the processing of their personal data in several ways, including via phone, email, post, or online form, depending on the way that is enabled by the data controller. Once a complaint has been received, the data controller must respond promptly and in accordance with the GDPR. They must also ensure that the complaint is investigated thoroughly, and that any necessary corrective actions are taken to address the issue. The data controller may also need to communicate with the data subject to provide them with information about the outcome of the complaint and any actions taken in response. If the data subject is not satisfied with the outcome, they may have the right to escalate the complaint to a supervisory authority.

- Perform data privacy impact assessments (DPIAs) when processing operations present specific risks to the rights and freedoms of data subjects.
- Provide training and awareness-raising activities for employees who handle personal data.
- Be transparent with data subjects about the processing of their personal data.
- Respond to data subject requests and cooperate with supervisory authorities in the event of an investigation.

The principle of accountability helps to ensure that organizations take a proactive approach to data protection and maintain a culture of data protection that is woven into the fabric of the organization. By doing so, organizations can demonstrate their commitment to protecting the privacy rights of individuals and build trust with their customers, employees, and other stakeholders. The general concept of accountability of the data controllers is introduced by Article 5(2) of the GDPR, which further highlights that the controller is responsible for compliance with all binding laws. GDPR introduces a new element when compared with the DPD, namely the obligation to demonstrate the above-described compliance. Such an obligation to prove compliance with laws finalizes the principles of accountability. Such an understanding is further supported by Article 24, which refers to the responsibility of the controller *as-is*. Article 24 also points to the principle of accountability, in the following sentence, it states:

> *Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to <u>demonstrate</u> that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*[355]

As disclosed by the quote from Article 24 of the GDPR, it is visible that the whole underpinning policy of the GDPR around the responsibility of the data controller is moving towards the demonstration of compliance. From a purely practical perspective, it means that the controller must operate on a hypothetical risk that the controller is obliged to address. GDPR assumes a risk-based approach; based on that Working Party or any other think tank organization interpreting the scope of the GDPR, it suggests a case-by-case assessment of risk for personal freedoms. It further gave rise to transfer impact assessments, risk assessments, and disaster

[355] GDPR, art. 24(1).

recovery plan evaluations. It still further shows that data controllers operate on a fictional evaluation of risks that is highly affected by external factors. Especially when it comes to online operating environments. Risk assessments under the GDPR as a necessary element to extract the scope of the data controller and its responsibility may be especially challenging when the following are taken into consideration:

- Complexity of data processing: SaaS solutions often involve processing a large amount of data from multiple sources, making it challenging to identify and assess all risks associated with such processing and to draw an exact line between particular elements of the processing[356];
- Multi-tenant architecture: In SaaS, multiple customers share the same platform, which can make it difficult to assess the risks associated with each customer's specific data processing activities[357];
- Technical expertise: Conducting a comprehensive risk assessment may require specialized technical knowledge, which may not be readily available in-house[358];
- Changes in technology: SaaS solutions are continuously evolving, and new risks may arise as technology changes. This makes it challenging to keep risk assessments up-to-date[359];

[356] As an example of such complex processing activity, one may point out lead scoring or incoming customer segmentation. Usually, such a process involves several steps of defining the ideal customer profile (ICP), gathering the data from the ICP segment, identifying their key features, assigning a score to each factor, and prioritizing based on the prior steps.

[357] Multi-tenant architecture is a software architecture in which a single instance of a software application serves multiple customers (tenants), each with their own isolated and secure data and configuration. The term *multi-tenancy* refers to the ability of a single instance of the software to support multiple tenants, who share the same infrastructure, but have their own unique data and configuration. Multi-tenant architecture is commonly used in cloud-based software as a service (SaaS) applications, where the provider hosts the software and provides access to multiple customers over the internet. In this model, each customer has their own instance of the software, but the underlying infrastructure and hardware are shared, which helps to reduce costs and simplify management for the provider.

[358] Such an issue raises the operational question for data controllers how to comply with the GDPR where the reliability and predictability of the law are low, the cost of implementation is high, and its correction or repetition may be hardly achievable for small and medium enterprises.

[359] It's important to notice that even pure use of technology such as Java or Phyton leaves companies with new vulnerabilities arising that are based on the new versions of the coding language and a need to upgrade the version in order to be able to use new libraries and other software components that depend on the version of the language.

- Responsibility for data protection: In SaaS, the responsibilities for data protection are shared between the SaaS provider and the customer. This can make it difficult to determine who is responsible for conducting a risk assessment and implementing measures to mitigate risks. From a legal perspective, the responsibility for data processing remains fully on the side of the controller (often acting as a customer of SaaS providers), but at the same time, the controller is required to be aware of and control all potential responsibilities that arise from the processing activities. Consequently, practical responsibility and the burden of adequate measures to check vendors remain in the hands of the controller.

The scope of the responsibility of the data controller is built upon the data controller's ability to demonstrate compliance with currently binding law. As GDPR does not narrow down certain remedies to be implemented by the controller, and further, there is no internationally recognized certification of GDPR compliance as there may be in the case of ISO or SOC standards, the controller may know its responsibility only if a risk assessment is performed. To perform an efficient risk assessment under the General Data Protection Regulation, the controller should consider the following steps:

- Identify the personal data processed: Determine the types of personal data being processed, the sources of that data, and the reasons for processing it. Usually, the brief determination of the above is possible based on the assessment of the database.
- Assess the risks: Evaluate the risks associated with the processing of personal data, taking into account the nature, scope, context, and purposes of the processing. With regard to this action point, it remains difficult due to the technological dependency of the multi-tenant environment and external exposure to vulnerabilities that are outside of realistic scope of action of the controller.

For example, the frequency of Java releases depends on the version of Java being used. For Java Standard Edition (SE), a new version is usually released every 3-4 years. This allows sufficient time for users to adopt the latest version and for developers to update their applications. For Java Enterprise Edition (EE), the release frequency is typically slower, with a new version being released every 4-5 years. In recent years, there have also been *interim* releases of Java SE that provide security and bug fixes, but do not include significant new features. These interim releases are typically released on a quarterly basis. On the other hand, for Python 3.x, a new version is typically released every 18-24 months. This allows sufficient time for users to adopt the latest version and for developers to update their applications. In between major releases, there are also smaller maintenance releases that provide bug fixes and security updates. These are released on an as-needed basis.

- Implement measures to mitigate risks: Choose appropriate measures to address the identified risks and ensure the protection of personal data, such as technical and organizational measures. In such regard, implementation is highly dependent on the realistic scope of impact of the controller, in line with the risks discussed above regarding dependency on external solutions.
- Document the risk assessment: Document in a formal process the risk assessment process, the outcomes, and the measures taken to mitigate the identified risks.
- Regularly review and update the risk assessment: Regularly review and update the risk assessment to ensure that it remains current and effective in light of changing circumstances.

As discussed above, the definition of the responsibility of the controller fluctuates, and the controller himself is assigned not only the obligation to demonstrate compliance with the law but also the obligation to demonstrate with what and to what extent he is obliged to comply, as the GDPR fails to recite and detail guidelines on this matter. In this regard, some of the key criticisms of the current understanding of the GDPR responsibility of the controller may be based on a lack of clarity. The GDPR's definition of a controller and their responsibilities are often considered vague and unclear, making it difficult for organizations to know exactly what they need to do to comply with the regulation. Furthermore, the burden on small businesses is not proportionate to their realistic ability to act. Small businesses, in particular, have faced challenges in complying with the GDPR due to the cost and resources required to implement the necessary changes and processes. Enforcement of these requirements is highly involved with the technical layer of any software and as such implies cost. The GDPR requires significant investment in technology and personnel to enforce its regulations, leading to criticism that smaller organizations may struggle to comply. The requirements of the controller’s responsibility are complex and difficult to define. The GDPR's requirements are complex and difficult to understand, and as a consequence, it is challenging for organizations to know what they need to do to comply. Lastly, it implies unintended consequences, namely that the GDPR's impact on data innovation and research has been criticized, with some suggesting that it may stifle technological innovation and limit the ability to use data for scientific research. Data protectionism: The GDPR is often seen as overly focused on data protection and privacy at the expense of innovation, creativity, and economic growth.

2. Meaning of a risk-based approach.

The General Data Protection Regulation introduced a risk-based approach to the interpretation and implementation of its provisions and used this well-known legal practice balancing standard to ensure the application of adequate measures for processing activities. This approach requires that all security measures and data protection mechanisms be assessed and viewed through the lens of risk assessment. In other words, the GDPR mandates organizations to evaluate the potential risks associated with data processing activities and implement appropriate measures to mitigate such risks.[360] The risk-based approach highlights the necessity for enterprises to address data protection in a proactive and preventative manner as opposed to only meeting the GDPR's bare minimum standards. Data controllers shall make sure they are appropriately protecting individual users' personal data and adhering to the GDPR's data protection principles by performing risk assessments and taking suitable steps to mitigate risks. Furthermore, data controllers, or any entity processing personal data that falls within the scope of processing assessment, while using the risk-based approach, must also be able to show that they have taken the necessary steps to reduce risks and safeguard personal information in the form of documentation.[361] Since companies must continually adapt to new risks and vulnerabilities in order to maintain an appropriate degree of data protection, this necessitates a continuous process of risk assessment, monitoring, and improvement. In order to defend people's basic rights and freedoms, the risk-based strategy is ultimately intended to make sure that companies adopt a proactive and successful approach to data protection.

[360] Article 25(1) of the GDPR states that data controllers must implement appropriate technical and organizational measures to ensure that data processing activities meet the requirements of the regulation and protect the rights of data subjects. This includes measures that take into account the nature, scope, context, and purposes of the processing activities, as well as the potential risks to the rights and freedoms of data subjects.

[361] The European Data Protection Board (EDPB) has provided guidance on the risk-based approach, where it was strongly emphasized that there is a need to provide documented proof of risk assessment and employed mitigations. EDPB has also stressed the need for organizations to document their risk assessments and data protection measures to demonstrate compliance with the GDPR. More information is available in Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020, Retrieved March 24, 2023 from https://edpb.europa.eu/sites/default/files/files/file1/ edpb_guidelines_201904_ dataprotection_by_design_and_by_default_v2.0_en.pdf.

Article 35 of the GDPR introduces the obligation to carry out a data protection impact assessment whenever there is a risk or high probability of infringements on individual rights.[362] In fact, the current understanding of the requirements of the DPIA means that every company working with new technologies as massive data processing including SaaS products and Internet processing of personal data on a scale that calls for the risk assessment. Along with the growth of GDPR practice, the responsibility of data controllers and the measures applied in practice should be viewed from the perspective of what tangible effect loss or damage to processed data may be caused to the data subject. In fact, such evaluation differs from known certifications such as ISO or SOC I / SOC II and calls for a practical evaluation of the data processed and the potential effects of such processing.

When analyzed closely one notices that the approach of GDPR is to keep the gateway open and state that even though such processing was secured with measures provided by the controller, such measures were not adequate to the type of processed data, the transfer involved, or any other aspect of processing that is exposed to weaknesses. On the other hand, it leaves a scope of freedom to data controllers to select means and measures of processing to fit into the context and process of operation on personal data. Subchapters presented below elaborate on different aspects of the risk-based approach as presented by the GDPR, its practical meaning to the data controllers, and further practical guarantees provided to individuals by such an approach. To ensure that the security measures used by data processors acting on behalf of data controllers would directly require auditing procedures every time there is a change in the system. Wherein, the accomplishment by the processor should equalize the security measures of the controller used in particular data processing scenario with the measures used by the processor. Although auditing is essential for ensuring GDPR compliance, it can be difficult for data controllers to regularly audit their data processors. Every time there is a change in the system, such as the use of a new sub-processor, a change in the data structure, or organizational changes within the company, data controllers are required by the GDPR to audit their data processors. However,

[362] Article 35 (1) of the GDPR states as follows: *Where a type of **processing in particular using new technologies**, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.* As quoted above the article places a special emphasis on the use of new technologies as a factor that increases the potential risk factor and suggests DPIA.

it might not be practical or feasible to conduct audits at such a high frequency. The information required for auditing the processors may be difficult to obtain since some of it may be regarded as proprietary or trade secret information. Furthermore, conducting frequent audits might place a heavy burden on data controllers and even interfere with how the data controller and the data processor conduct business. As a result, while auditing is necessary to ensure GDPR compliance, a more realistic and long-term strategy that strikes a balance between auditing and business continuity is required. The most effective manner to conduct audits is still up for debate, despite the fact that they are a crucial part of the GDPR compliance process and that data controllers must make sure their data processors are implementing sufficient security measures to protect personal data. Due to how frequently data processing technologies used by data processors change, auditing can be difficult for data controllers. It might not always be feasible to perform an audit every time a change is made to the system, and data controllers could lack the resources and knowledge necessary to do so themselves. In certain situations, data controllers might have to depend on outside consultants or external auditors to carry out the audit. Data controllers may yet encounter difficulties throughout the auditing process, such as the time and expense required to complete the audit, even when depending on external auditors. Furthermore, some information may be regarded as protected know-how or trade secrets, making it challenging for data controllers to access it in order to audit their data processors. The absence of specific instructions or models from the EU Commission on how to carry out the auditing process presents another difficulty in the auditing process. This can result in inconsistent practices across various data controllers and third-party auditors, which may ultimately lead to variable degrees of GDPR compliance. In certain instances, auditing may merely lead to a formal statement rather than a thorough examination of the data processor's security procedures. The EU Commission must provide more thorough instructions and assistance on how to undertake realistic and efficient audits of data processors in order to meet these concerns.

3. Data protection impact assessment and prior consultations.

At the core of the GDPR, one can observe two regulatory presumptions: a neutrality of technology and a risk-based approach. To begin with, the GDPR understands neutrality of technology to be the principle that technology should be designed and developed in a way that does not discriminate against any particular group or individual, furthermore, it implies that the

selection of certain technology should not have the effect of discriminatory or unfair practices. This means that technology should be neutral in its processing and, if applicable, decision-making, and should not result in unfair or disproportionate impacts on certain groups or individuals.[363] From a practical perspective, this means that the data controller or any processing entity must be mindful of the potential biases and discriminatory effects of their technological systems and take steps to mitigate these risks. This may involve conducting impact assessments to identify and address potential biases, implementing appropriate data protection safeguards, and ensuring that individuals have the right to challenge and appeal automated decisions that affect them. As a consequence, the key to proper implementation of the GDPR is to perform a risk analysis, also referred to as the DPIA (Data Protection Impact Assessment). It is related to the processing of the personal information of individuals whose data a particular entity processes and provides the basis for a reasoned decision to implement technical and organizational measures to minimize the risk. In this way, an adequate level of protection of the rights of data subjects is to be evaluated and further assessed to provide sufficient measures. Section 3 of the GDPR directly relates to the data protection impact assessment and prior consultations, with Article 35 being focused on the impact assessment itself. Article 35(1) reads as follows:

> *Where a type of processing in particular using **new technologies**, and taking into account the nature, scope, context and purposes of the processing, **is likely to result** in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out **an assessment of the impact** of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.[364] (emphasis added).*

This above-quoted article serves as a very generic and descriptive indication of the fact that if you, as a controller, process personal data with new technologies and there is a likelihood of potential data security breach, there is a need to assess the potential impact on the individual

[363] In accordance with the GDPR, individuals must also be made aware of how their data is handled, including any automated decision-making, and given the option to opt out of those procedures as necessary. The GDPR aims to preserve person's fundamental rights and freedoms in the digital era by supporting the neutrality of technology.

[364] GDPR, Art. 35(1).

rights of the data subject.[365] At the same time, it should be noted that the standard of security as required by the European Commission is one of the highest in the world, as only 14 countries aside from the EU member states were assessed as being in line with the requirements promoted by GDPR.[366] Passing personal data to the countries covered by the so-called adequacy decision requires no further security measures to mitigate the risk of such a transfer. At the same time, transfer to any other region requires further implementation of security measures. Any other transfer issued by the data controller or data processor located on the territory of the EU shall be further followed by an assessment of the risks regarding such a transfer. Furthermore, the assessment as described above is also of a repetitive nature, as indicated by para. 11 of Article 35, which further defines:

> *Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a* ***change of the risk*** *represented by processing operations.*[367] *(emphasis added).*

Following the general understanding offered by Article 35(1) of the GDPR, the threshold to meet the requirement of high risk is likely to result in a potential infringement of data subject rights as directly included in the GDPR Further explanation in this regard is offered by Article 35(3) with the non-exhaustive list of high-risk indications:

- Automated processing, including profiling – according to the GDPR, all processing that is automated and further results in the decision-making process fulfills the criteria of higher risk;

[365] Article 35 is further related to Article 24 of the GDPR, which defines the responsibility of the controller; Article 25 refers to protection by design and by default, Article 32 refers to the security of processing; and Recitals 94-95. It may be further interpreted in light of the provisions about the Data Protection Officer (Article 39) and Article 63 about consistency mechanisms.

[366] Full list of documents regarding adequacy decisions issued by the European Commission, see: *Adequacy decisions*. Retrieved March 24, 2023 from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents.

[367] GDPR, art. 35(11).

- Processing of sensitive data – regulated by Article 9 of the GDPR processing of personal data classified as a special category requires special circumstances for the legality of processing[368]; and
- Systematic monitoring of publicly accessible areas, especially with the use of optical-electronic devices, remains especially important when refusal of the data processing (for example, a client refusing to be recorded in the shopping center) equals the inability to use the area.

The currently known list of high-risk indications has been narrowed down compared to the initial draft proposed by the UE Parliament.[369] From a purely academic perspective, DPIA is a form of impact assessment that is considered a well-known balancing mechanism that aims to provide a practical check to the implemented measures in order to provide an adequate level of security. The mechanism itself was used as early as the 1960s to evaluate technological inventions.[370] Later on, in the 1990s, privacy impact assessment was used as a mechanism in Canada, New Zealand, and Australia by public sector bodies and later on by multiple data processing subjects[371]. Finally, Article 6 (1)(f) of the GDPR refers to legitimate interest and evaluation if the interest of the controller is not overridden by the interests or fundamental rights of individuals. Simply put, the GDPR is asking for a balancing test to weigh these two values against one another.[372] The outcome of this test represents the answer to the question of

[368] Article 9 paragraph 1 of the GDPR states as follows: *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.* Furthermore, paragraph 2 of the same article provides a very narrow list of exceptions for the processing of sensitive data.

[369] Initially, the European Parliament offered a dedicated article (Art. 32a) fully focusing on the risk analysis that further included a list of nine potential cases that would serve as a pattern for risk evaluation. Article 32a was not included in the final version of the GDPR; nevertheless, some of the suggested cases can be found in the Wording Party 29 recommendation on DPIA guidelines.

[370] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.*, p. 668.

[371] K. van Dijk, G. Böröcz, T. Mantovani, *Data Protection Impact Assessment in the European Union: Completing the New Legal Framework towards a more robust protection of individuals*, d.pia.lab Policy Brief 2017, no. 1, Retrieved June 25, 2022 from https://osf.io/preprints/lawarxiv/b68em/download.

[372] According to the Art. 29 Working Party the idea of impact assessment as the equivalent of a balancing test is a simplification. The Working Party highlights the need of a more extensive and in-depth assessment than just weights compared on two sides. The impact assessment requires the evaluation of the nature and source of the

whether or not a particular data processing is in fact justified by law. As a consequence, the predictability of the law in this regard requires the evaluation of the balancing test outcome. The requirements of the balancing test (or more often named on the ground of the GDPR, the evaluation of justified interest of the data controller) remain similar to the requirements placed in Directive 95/46 Article 7(1)(f).[373] The similarity in wording between the GDPR requirement of Article 6 and the Directive 95/46 requirement of Article 7 brings a similar doubt about the predictability of law and lack of legal certainty, as observed by the Article 29 Data Protection Working Party. The following is from the 2012 Commission Staff Working Paper on Impact Assessment:

*The implementation of the "balance of interest" criterion (Article 7(f)) **differs substantially between Member States**. In the UK it is largely left to controllers to conduct the assessment and to determine whether they can process personal data on this basis. In the Netherlands, the explanatory memorandum to the data protection law sets out guidance on what issues should be taken into account when applying this criterion. Given its vagueness, several Member States (including Belgium, Ireland and UK) have envisaged issuing further rules for the application of this criterion, but have not yet adopted such rules. DPAs have provided guidance in their opinions interpreting the law. In some countries, it is explicitly indicated that the balance test applies only to the private sector (e.g. Germany) or in cases specified by the Data Protection Authority (Italy) or on the basis of the permission of the national data protection supervisory authority in a specific case (Finland). Other countries (including Greece and Spain) impose stricter requirements on processing on the basis of this criterion. Thus, **by its nature, this criterion gives the Member States latitude to adapt its application to specific situations.**[374] (emphasis added).*

legitimate interest and then comparing it with the impact on individuals, looking through the prism of individua rights and potential risks. Consequently, despite the idea seeming to be similar to the currently known balancing test, the data controllers are still left with a dose of new, adjusted context that requires separate interpretation.

[373] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 7(1)(f): *processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)*.

[374] European Commission, *Commission Staff Working Paper Impact Assessment on the Proposal for a General Data Protection Regulation, accompanying the document Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final*, Brussels 2012. Retrieved January 10, 2023 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072.

In the above-quoted part, the Article 29 Working Party directly expresses its doubts about the lack of clarity and the lack of defined requirements on the balancing test in the form of impact assessment. In the following years, the Working Party attempted to further define the notion of legitimate interest and the criteria for balancing tests. Nevertheless, as the nature of Working Party documents is of an advisory character and the practice still differs from country to country, there is a factual question of the predictability of the law, especially for data controllers. If, after the controller performs the test of impact on individuals, the outcome of such a test prevails on the side of the controller's benefits with no proper risk mitigation on the side of individual rights, then the data controller is obliged to implement additional safeguards and reassess the impact afterwards to lead to a situation where all potential risks are adequately addressed.[375] The cycle of assessing the impact on individual rights and freedoms as defined by the GDPR and as further explained by the Working Party may be traced back to five essential steps, namely:

- Step 1: Assess the nature and source of the legitimate interest. There is no unified definition of the *legitimate interest* scope, it remains fully within the discretion of the data controller to define it with a use of non-binding recommendations as the Working Party.
- Step 2: Assess the impact on data subjects. In this regard, current practice suggests taking into account two important factors namely likelihood of the risk to occur in practice and severity of consequences should the risk occur.[376]
- Step 3: Provisional balance. In this regard, the Working Party recommended evaluating the preliminary conclusion. It is important to highlight that, according to the work of Article 29 Data Protection Working Party, not all negative impacts have to be balanced in a proportionate way. The key element is to prevent any disproportionate impacts.[377]

[375] D. Rucker, T. Kugler, *opt.cit.*, pp. 84-86.

[376] According to recital 47, the assessment has to take into account the reasonable expectations of data subjects based on their relationship with the controller while taking into consideration the context of data collection. The relationship between the data subject and the data controller further requires checking the nature of the processing, the circumstances of the data being shared, and the balance of powers between the controller and the data subject. The Working Party gives some special attention to the importance of the specific and restrictive context of the collection (Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Adopted on 9 April 2014, 844/14/EN WP 217*.).

[377] Data Protection Working Party, *Opinion 06/2014*, Iop. cit., p. 41.

- Step 4: Implement additional safeguards and reassess the measures against the risks. If the outcome of Step 3 implies that there is a need for additional safeguards, it is the obligation of the data controller to employ additional safeguards to balance the risks.
- Step 5: Document the assessment. It remains within the scope of responsibility of the data controller to document the steps taken to secure data processing (including potential data transfers that shall be discussed in the following subchapter).

The steps provided above constitute only a generic framework for justifying data processing. The more complex data processing is, the more demanding the lack of defined guidelines becomes. Such disproportion is especially visible in the case of new technologies and complex solutions, such as SaaS software, where data processing, including processing of personal information, constitutes a core activity for business functionality. In abstract circumstances, the question of right or wrong arising from the interpretation of the legitimate interest as proposed by the GDPR may fall within the scope of the question of pragmatism of law as discussed by Justice Holmes. One element remains certain, the question of how and to what extent data controllers may rely on the risk assessments as defined through their subjective standpoint remains unanswered.

4. The phenomenon of the right to be forgotten in the light of a risk-based approach.

The right to be forgotten is a concept that is enshrined in the General Data Protection Regulation, which is a regulation in European Union law on data protection and privacy effecting all individuals within the EU and the European Economic Area. The right to be forgotten is also known as the *right to erasure*. It gives individuals the right to request that their personal data be erased from a company's or organization's records if there is no compelling reason for it to be retained. This right is intended to give individuals control over their personal data and protect their privacy. The concept of the right to be forgotten originated from a ruling by the European Court of Justice in *Google Spain v. AEPD and Mario Costeja González*[378] In this case, the European Court of Justice held that individuals have the right to request the removal of personal information that appears in search engine results if the information is outdated, no longer relevant, or if its continued publication would infringe on the individual's

[378] *Google Spain…,* Case C-131/12, *op cit.*

privacy. The right to be forgotten was created as part of the GDPR to address growing concerns about the collection, storage, and use of personal data by companies and organizations. With the increasing use of the Internet and digital technologies, more and more personal data is being collected, stored, and shared, which can potentially lead to privacy violations. The right to be forgotten is one of the most controversial ones, at least from the perspective of both technical aspects and practical implementation. For example, as a result of *Google Spain* and additionally certain GDPR legislation, Facebook moved around 1.5 billion user accounts from EU based servers to non-EU based servers, which was vastly criticized as the avoidance of EU legislation over data processing.[379] Directly after the *Google Spain*, Google received around 2.3 million URLs to de-index from the search engine that were directly reported by European users.[380] The right to be forgotten was created to give individuals more control over their personal data and to help protect their privacy in the digital age. Directly because of GDPR, the right to be forgotten is included in, among others, Recital 65, that states as follows:

> *A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. 2In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation.*[381]

The above quote is one of the very first appointments of the *right to be forgotten* as one of the rights of data subjects under the GDPR. The right to be forgotten gives individuals the right to have their personal data erased and no longer processed if it is no longer necessary in relation to the purposes for which it was collected, if the individual withdraws their consent or objects to the processing, or if the processing otherwise does not comply with the GDPR. This right is particularly relevant in cases where a child has given consent for the processing of their personal data and later wants to remove it. However, the right to be forgotten is not absolute and may be balanced against other interests, such as the right to freedom of expression and

[379] F. Werro, *The Right To Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia*, Washington, 2020, p.24.

[380] *Ibid*., p. 25.

[381] GDPR, rec. 65.

information, the need to comply with a legal obligation, the performance of a task in the public interest, public health, scientific or historical research, or the establishment, exercise, or defense of legal claims. As a result, Recital 65 of the GDPR defines the right to be forgotten as a core right of data subjects under the GDPR and explains when it may be overridden by other interests. Recital 65 is also strongly tied to Article 5 of the GDPR, which establishes the standards governing the processing of personal data, as well as Recitals 69–70.

The basic formulation of the right to be forgotten is in Article 17 of the GDPR and is regarded as a revolutionary notion that modernizes the approach of European data protection regulations.[382] The right to be forgotten is considered a novel concept in data protection law mostly because it introduces a new set of rights for individuals with respect to their personal data. Prior to the GDPR, there was no comprehensive right for individuals to have their personal data erased, and individuals only had limited control over how their personal data was processed. In fact, the right to be forgotten represents a significant shift in the balance of power between individuals and organizations that process personal data. It gives individuals a new and powerful tool to protect their privacy and control how their personal data is used[383].

The right to be forgotten empowers individuals to request that organizations erase their personal data if it is no longer necessary, if they withdraw their consent, or if the processing otherwise does not comply with the GDPR. This right is also considered novel because it applies to the internet and other online platforms.

The internet has made it possible to store and spread vast amounts of information about individuals, and the right to be forgotten gives individuals a new way to control their digital footprint and protect their privacy in the digital age. In conclusion, the right to be forgotten is considered a novel concept in data protection law because it gives individuals a new set of rights to control how their personal data is processed and used and because it applies specifically to the internet and online platforms.

[382] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.*, p. 477.

[383] Early attempts to codify the right to be forgotten or the right to erasure were contained in DPD article 12, furthermore, Article 8(c) of Convention 108 referred to the right to obtain or erase the data in line with Article 5 of the Convention, enlisting individual rights.

A simple form of the right to erasure was already known from the DPD in the provisions on the right to access included in Article 12.[384] The right to be forgotten as an element of the legal infrastructure is not a new thing, it can be found, aside from the GDPR, in Convention 108, where, under Articles 5 and 6, the right to obtain the data or erase the data has been included. The right to be forgotten has become an increasingly important aspect of data protection and privacy law as more and more personal information is being collected, stored, and processed by organizations. This right gives individuals the ability to request that their personal data be deleted or removed from the Internet if it is deemed to be no longer relevant, is inaccurate, or is harmful to the individual's privacy. The right to be forgotten can help address the risk that sensitive or outdated personal information may cause harm to individuals if it falls into the wrong hands or is used inappropriately. In light of this, the risk-based approach has become an important framework for considering the right to be forgotten. A risk-based approach recognizes that not all data processing activities pose the same level of risk to individuals' privacy and seeks to balance the potential benefits of processing personal data with the potential risks it poses. This allows organizations to make informed decisions about how to handle personal data in a way that best protects the rights and freedoms of individuals. For example, a risk-based approach might involve conducting a thorough assessment of the personal data that an organization collects, the purposes for which it is collected, and the risks associated with its processing. If the organization determines that certain information poses a significant risk to individuals' privacy, it may take steps to remove that information from its systems, limit access to it, or implement stronger security measures to protect it. In conclusion, the right to be forgotten in the light of a risk-based approach can help organizations better understand and address the potential risks associated with the processing of personal data. By considering the risks and balancing them against the benefits of processing personal data, organizations can ensure that they are protecting the rights and freedoms of individuals while still being able to make use of the valuable information they collect.

As stated in *Google Spain*, the right to be forgotten shall also be understood as a non-absolute right.[385] In fact, it does not apply if, among other things, it stands against freedom of expression,

[384] Article 12 of the DPD grants individuals the right to request data removal or correction once processing of such data is not in compliance with the data processing laws.

[385] In *Google Spain v. AEPD and Mario Costeja González* (2014) that is often cited as a landmark case on the right to be forgotten, the ECJ ruled that individuals have the right to request the removal of links to personal

including free speech and freedom of information. The right to be forgotten may be limited by the need for freedom of expression and information, as well as by public interest considerations. This means that if the processing of personal data is necessary for the exercise of these rights or for the performance of a task in the public interest, the right to erasure may not apply. Similarly, the right to be forgotten may not apply if the processing of personal data is necessary for the establishment, exercise, or defense of legal claims.[386] This is because the right to erasure could potentially hinder the ability to obtain evidence and pursue legal proceedings.[387] In summary, the right to be forgotten is not an absolute right, and its application is subject to certain limitations and exceptions, as proven by a certain line of case law, including *Google Spain*.[388]

Evaluation of *Google Spain* brings to light the relevant works of Finnish professor of law M. Koskenniemi. In his famous essay entitled *From Apology to Utopia,* Koskenniemi describes the argumentative framework of international law.[389] Every persuasive argument in

information from search engine results if the information is inadequate, irrelevant, or no longer relevant. However, the court also stated that this right is not absolute and must be balanced against other fundamental rights, such as freedom of expression and information. In this case, the ECJ ruled that Google was not required to delete the personal data in question, as the public interest in the information outweighed the individual's right to privacy.

[386] If the processing of personal data is necessary for the exercise of freedom of expression and information, such as for journalistic purposes, the right to be forgotten may be excluded. It is important to remember that on the European level, free speech and the right to express yourself are not absolute and may be limited by the execution of other rights that are higher in the hierarchy.

[387] In each of these cases, the right to be forgotten may be excluded because there is a legitimate reason for retaining the personal data, such as for legal, public interest, or research purposes, and the right to be forgotten could potentially hinder these important interests. Consequently, the possibility of excluding the right to be forgotten shall be further subjected to the balancing tests.

[388] Other cases that referred to the same subject matter (non-absolute character of the right to be forgotten) are *Ryneš v Úřad pro ochranu osobních údajů* (2014) where the ECJ ruled that the right to be forgotten did not apply to personal data that has been lawfully processed and published online. The court held that the right to be forgotten is not an absolute right and must be balanced against the right to freedom of expression and information. Another case that referred to a similar subject matter is *Peter Nowak v. Data Protection Commissioner* (2017) where the ECJ ruled that the right to be forgotten did not apply to personal data that was published for journalistic purposes. The court held that the right to freedom of expression and information takes precedence over the right to be forgotten in such cases.

[389] M. Koskenniemi, *From Apology to Utopia: The Structure of International Legal Argument*, Cambridge University Press, 2009, Cambridge.

international law, according to him, combines utopian (normative) and realist (concrete) elements. He asserts that ideal standards of behavior for its subjects are what the law strives to accomplish. To keep its standards attainable in actuality, however, it must also take into account the current social realities. These two conditions present a challenge, though. On the one hand, if legal standards are established that are too remote from social reality, the relevant law is susceptible to the accusation of being a utopian ideal because its normative requirements cannot be met in reality. But, if law simply mimics existing social truths, it cannot attain the goals that law regards as advantageous to the larger political society. Instead, it turns into a tool used to defend (or legitimize) the dominant socio-political forces at play in a certain social context. The legal justification used by Advocate-General Jaaskinen in his opinion in *Google Spain* was in line with Koskenniemi's argumentation framework. The opinion specifically highlighted the interaction between the normative and concrete elements, which, despite being mutually exclusive, are both necessary to create strong legal arguments.[390]

The Internet Search Engines (ISE) are one of the most commonly used elements of the technology available online – it further exposes the need to properly address the matter from the perspective of data access and security. As we cannot all be considered *data controllers* for the purposes of the EU Data Protection Directive, it took that position. The Advocate-General said that in this sense, that EU data protection law needed to be rooted in social realities and evolve along with actual social customs[391]. From this perspective, it follows that the law runs the danger of not being successful if it is construed in a way that does not take into account the relevant social facts (utopian). Further sociological realities cited by the opinion demonstrate that ISE operators should not be regarded as data controllers under the terms of Article 2(d) of the Regulation. It specifically drew attention to the fact that ISE operators cannot control the content on source websites in response to a name search involving data on third party servers because of technological limitations that prevent them from knowing in advance when they are processing personal data in accordance with Article 2 of the GDPR (b).[392] Because of this, even though, according to a literal interpretation, they might be a *body which alone or jointly determines the purposes and means of the processing of personal data,* the Advocate-General

[390] S. Allen, *Remembering and Forgetting – Protecting Privacy Rights in the Digital Age*, European Data Protection Review 2015, vol. 1(3), p. 7.

[391] *Ibid.*

[392] *Ibid.*

claimed that ISE operators are incapable of fulfilling the obligations of a data controller as set out in Articles 6, 7, 12, and 14 of Directive[393].

While individuals have the right to request the deletion of their personal data in certain circumstances, this right must be balanced against other rights and interests, such as freedom of expression and information, public interest considerations, and the need to establish and defend legal claims. The aspect of freedom of journalism in light of the right to be forgotten was further discussed by the ECtHR in the case *Węgrzynowski and Smolczewski v Poland* where the court refers to the fact that even if personal data are incorrect or unlawful, the publication shall remain available as the right at stake is the freedom of press.[394] Precisely, in paras. 65 and 66, it states as follows:

> *§65: […] That court expressed the view that it was not for the courts to order that the article be expunged as if it had never existed (see paragraph 12 above). The Court accepts that it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations. Furthermore, it is relevant for the assessment of the case that the legitimate interest of the public in access to the public Internet archives of the press is protected under Article 10 of the Convention.*

And

> *§66: […] The Court is therefore satisfied that the domestic courts were aware of the significance which publications available to the general public on the Internet could have for the effective protection of individual rights. In addition, the courts showed that they appreciated the value of the availability on the newspaper's website of full information about the judicial decisions concerning the article for the effective protection of the applicant's rights and reputation.*

Both quoted paragraphs from the *Węgrzynowski and Smolczewski v Poland* judgment confirm the approach of the non-absolute right to be forgotten. In fact, there are relevant limitations to this regulation, and both implementation and legal understanding shall take into consideration that, due to already existing balancing practices, the request to remove personal data of an individual may not always be performed due to the circumstances of such a request. What is

[393] *Google Spain…,* Case C-131/12, *op cit.,* para. 25.

[394] ECtHR, Application, *Węgrzynowski and Smolczewski v Poland,* no. 33846/07, July 2013.

more, on the side of both data controllers and courts is the obligation to perform this challenging balancing test towards individual rights.

The question of the right to be forgotten and its limitations are not the only potential challenges in the case of both a risk-based approach and the direct applicability of the right. The right to be forgotten raises important technical questions, such as index-based search and its territoriality. Currently, search engines such as Google operate on country codes, and top-level domains such as, for example, google.pl, google.de, etc. (ccTLDs). On the other hand, the territoriality of the ccTLD is often not fully recognized, as shown by the case of a famous URL shortener being registered on a Libyan ccTLD, which for the majority of Internet users was considered to be only a part of their brand name (Bil.ly).[395] The question that arises from a purely technical perspective refers to the scope of the obligation to erase such data from the search events that are from another jurisdiction (featured by distinct ccTLD).[396] At the same time, it remains important to understand that delisting from one browser or even one ecosystem of products (for example, Google products) does not equal removal from the broadly understood Internet, as there is no universal and centralized manner to control published data that has already entered the network.[397] In *Google Inc. v Commission nationale de l'informatique et des libertés* (C-507/17), the court stated that the obligation to remove requested content, including personal data, extends only to the Member States:

> *In the light of all of the foregoing, the answer to the questions referred is that, on a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of*

[395] M. Jakobsson, *The Death of the Internet*, IEEE Computer Society, New Jersey, 2012, p.43.

[396] This question was raised by the French data protection office, and the case was further referred to the European Court of Justice, asking about the universal delisting. Case C-507/17 *Google Inc. vv.Commission nationale de l'informatique et des libertés* (CNIL). A request for a preliminary ruling from the Conseil d'État analyzed the fact that territoriality has no direct impact on the digital world. It further explicitly stated that it remains within the full power of the search engine to manage adequate security measures with regard to the search engine performance. Such a statement has been drawn in the §70 of mentioned judgment with the following wording: *[…] In addition, it is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Those measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name*.

[397] Consequently, the question of how to effectively perform the right to be forgotten is still alive, as the mechanisms seem to point to the solution only formally, with no possibility to execute a global, across all the Internet, removal process from one place.

> *Article 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679, where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.*[398]

Consequently, there is a visible tendency in a debate to ask, *what is the scope of right to be forgotten, does it extend over the jurisdictions, regardless of the territoriality*? Worldwide, the question of this rather new individual privilege has attempted to be interpreted in a plurality of ways. For example, the Canadian Supreme Court attempted to extend jurisdiction over the right to be forgotten to all indexed data processed by Google. In this regard, Google referred to the federal court to receive the interim relief on that matter that was granted, which, at the same time, limited the supranational character of the search engine's obligation to remove the personal data from the indexed page.[399] Many jurisdictions observed a similar challenge as Europe, and the question of de-indexing the results across all jurisdictions remains an important technical and legal question with regard to the right to be forgotten, especially while one takes into account the fact that Google, as an international actor, acts as a data processor and not a data controller.[400]

On the other hand, the challenge of the right to be forgotten, as promoted by the underpinning values of the GDPR, is the so-called right to explanation. Articles 13–15 of the GDPR provide rights to *meaningful information about the logic involved in automated decisions* that are often referred to as a *right to explanation*. On the grounds of the GDPR, Articles 13(2)(f), 14(2)(g), and 15(1)(h) directly require data controllers to provide data subjects with information about any potential existence of automated decision-making, including profiling, referred to in Article 22(1) and (4), and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for

---

[398] CJEU, Judgement, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, September 2019. ECLI:EU:C:2019:772, para. 73.

[399] F. Werro, *The Right To Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, opt. cit*…, p. 25.

[400] Such approach has been criticized as uncomfortable by a lot of companies and international law observers due to the uneven division of powers.

the data subject. Articles 13 and 14 are further established to include the notification duties imposed on data controllers. Lastly, Article 15 provides a right to access information throughout processing.

To summarize, the GDPR requires data controllers to inform data subjects about any automated decision-making, including profiling, that may impact them. This includes providing meaningful information about the logic involved, as well as the potential consequences for the data subject. These notification duties are established in Articles 13 and 14 of the GDPR. Additionally, Article 15 provides data subjects with a right to access information throughout the processing of their data. This means that data subjects have the right to know what information is being collected about them, how it is being processed, and the potential impact it may have on them. By providing this information, data controllers can help ensure transparency and fairness in the processing of personal data.

B. The phenomenon of data transfer in light of transfer impact assessment and the responsibility of data controllers'.

The previous subchapter presented above refers to the risk assessment, or so-called balancing test, and how the data controller can implement this in practice. The challenge placed on data controllers is wide-ranging as it relies on the discretionary power of the data controller to evaluate all risks and the level of detail with which such risks will be analyzed. The evaluation of data owned by the data controller is only one of the constituent parts of the data controller's risk assessment obligations. Aside from the evaluation of data at rest, the controller is also obliged to evaluate the risk arising from the transfer of personal data, including such transfers to third-party subjects, also referred to as *data processors*. The transfer as a phenomenon is regulated by Chapter 5 of the GDPR, starting with Article 44 which reads as follows:

> *Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organization.*[401]

Consequently, the GDPR itself does not provide a detailed definition of *data transfer*, and it is possible to draw the conclusion that *data transfer* is any movement of personal data from one location to another. Presumably, it is possible to draw a few interpretations about what is meant by *data transfer* and when the transfer should be further secured with additional guarantees. The first assumption to be made about the nature of the data transfer is that it is distinct from data collection. According to the British authority ICO the *transfer* means *intentional sending of personal data, or making it accessible*.[402]

Data transfer and data processing, or data collection, tend to overlap, mostly due to the broad understanding of what constitutes data processing itself.[403] In the simple understanding, data

[401] GDPR, art. 44.

[402] *International transfers* [In:] *Guide to the General Data Protection Regulation (GDPR)* [online]. Retrieved December 4, 2022 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.

[403] The definition of *data processing* is broad, according to the GDPR, data processing refers to almost every activity taken on the set of data, while data collection and data transfer refer to a separate subset of actions. The

transfer shall be deemed the responsibility of the data controllers, focusing on the determination of the need to transfer and further on the security measures that shall be applied to the transfer. As the aim of this thesis is to show the application of currently known laws to the reality of software, let's present a brief overview of regular software development. To present the context in a transparent manner, the software in question would be a web application operating in the SaaS model. This type of software is currently one of the most popular on the market, and almost every person with access to the internet uses some type of online or web applications, the majority of which are delivered in the form of Software as a Service.[404] A typical SaaS development process implies the need to be responsive to the market and otherwise agile when it comes to changes and product growth. SaaS providers use, at minimum, the following elements to deliver the software and maintain it:

- Server infrastructure – regardless of the type or architecture, on-site deployment of software is currently less and less popular with the growing impact of the cloud. Market actors, such as Amazon, IBM, or OVH, are widely selected by the software owners to facilitate the management of physical and virtual machines to provide data storage.
- Analytics, monitoring, and code management – to facilitate the security and integrity of personal data and the system as a whole, it remains necessary to use third party providers to facilitate analytics of application performance, responsiveness of the application, monitoring, or code management.
- Customer service supporting software as chat channels or CRMs – none of the realistically developing companies at the moment shall decide to run business without supporting software as CRMs (software dedicated to customer management) or communication channels to facilitate the exchange of information between the customer/data subject and the company.

first one is dedicated to the entry into possession of personal data, and the latter one is to the change of location of personal data.

[404] According to Gartner Forecasts Worldwide Public Cloud End-User Spending Report software as a service (SaaS) remains the largest market segment with the growth of $117.7 billion in 2021, application infrastructure services (PaaS) is anticipated to grow by a higher margin at 26.6%. Retrieved December 4, 2022 from https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021#:~:text=Worldwide%20end%2Duser%20spending%20on,research%20vice%20president%20at%20Gartner.

- Billing services – on daily basis, the SaaS industry uses third-party providers to facilitate payment. Mostly due to the complexity of banking systems and high standards of protection in this regard, software owners decide to use third party as Braintree or Stripe to facilitate the payment process.

Taking the above into consideration, it remains quite obvious that delivery of SaaS without data transfer is barely possible. In fact, the assumption of the data controller or subprocessor selecting the transfer is a fictional assumption that it is possible to operate in an isolated environment, which remains similar to the assumption that we can currently live without access to any supplier of water, electricity, or municipal waste management. At the same time, the GDPR places some obligation on the data controller to ensure data safety in transfer in line with the requirements of Chapter 5 of the GDPR. To summarize the scope of the responsibility of the data controller, the following may be pointed out:

- responsibility for the selection of processors;
- responsibility for the assessment of the data controller's security measures and the adequacy of such measures;
- assessment of transfer impact;
- liability towards data subject[405].

As quoted above, all responsibilities placed on the data controller refer to the wide scale of all processing activities. Such an approach is dedicated to ensuring reliability for data controllers; nevertheless, there is also the scope of disproportion regarding the proposed construction. In general, providing any IT solution, whether cloud-based or on-site, requires third-party providers. Operating without processors remains a foreign idea that is hardly possible from a purely practical standpoint. As a consequence, while employing the processor, any data controller shall be aware that the scope of such a relationship also includes the use of further third-party providers. Considering the reality of software functioning as “as is” solutions, the factual choice given to the data controller is whether to use or not to use particular data processors. On the other hand, the use of data processors may still indicate that further processing will differ from the processing that happens only on the side of the data processor – including further data transfer.

[405] P. Ticher, *Data Protection and the Cloud: Are the risks too great?*, Cambridgeshire 2015, pp. 22-25.

The transfer itself is regulated by Article 44 of the GDPR; this article may be considered a successor to Article 25 of the DPD; nevertheless, awareness of the need to control data flows dates way back than before the concepts of Article 44 of the current GDPR or the antecedent, Article 25 of the DPD.[406] Looking from a *big picture* perspective, both Article 44 of the GDPR and Article 25 of the DPD have a lot in common; even so, there are some important differences to highlight, namely the allocation of adequacy decisions and an adequate level of protection. While Article 25 of the DPD directly referred to the European Commission's adequacy decisions, for Article 44, such a matter was not covered, and the merit concerning adequacy decisions was solely transferred to Article 45 of GDPR.[407] The idea of transfer impact assessment arose from the requirements of Article 46 of the GDPR, where it is directly stated that:

In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[408]

Article 46 of the GDPR mentions that data transfer is possible as long as the controller and processor, or exporter and importer within the meaning of Standard Contractual Clauses, are able to provide adequate security measures. Such understanding brings us to the question of adequacy within the transfer. Aside from the previously discussed balancing test and the question of proportionality within risks, a new term of art emerged, namely transfer impact assessment (TIA). TIA became frequently used as the outcome of the *Schrems II* judgment. Before 2021, the indications of the TIA are rather limited; nevertheless, para. 134 of the judgment brought certain wording that was further understood as an indication of the TIA.

[406] It constituted one of the objectives of the European Union to open the free flow of data for the purpose of strengthening integration between countries and avoiding any blockades due to non-unified law that requires protection on different levels. One of the examples of such national legislation that sanded against the free flow of data was an Austrian ordinance from 1980 that required prior authorization of the transfer of personal data. Such authorization was issued by the Austrian Data Protection Commission. Austrian legislation or jurisprudence was not the only example of limited data protection flows, such cases were, among others, present in Italy, Germany, or Sweden.

[407] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.,* p. 759.

[408] GDPR, art. 46(1).

In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor ***to verify, on a case-by-case basis*** *and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses*[409]*. (emphasis added)*

This judgment did not itself mention transfer impact assessment; it only mentioned assessment as an instrument in a rather reluctant way. Even so, it is one of the most telling paragraphs from the judgment calls for the possibility of verification of adequacy when it comes to data safety. The requirement to verify, on a case-by-case basis implied or at least suggested that such verification may be of use when conducted in writing. Besides that, in *Schrems judgments*, the TIA still exists only as a newly emerging concept and not as a stated practice. Such a concept is highly supported by prior legislation and its interpretation, for example, Articles 44 and 46. A year after the *Schrems II* judgment came into effect, the European Data Protection Board concluded recommendations on measures to supplement data transfer tools.[410] The recommendation issued by the EDPB brought an important input into the discussion of the data controller's obligation. As suggested by the document, before any transfer actually happens, it should be within the obligation of the transferring party to assess if the circumstances in the receiving country are in line with the requirements of GDPR, and what is further important is if such a transfer may be secured in a way corresponding to the risks and potential mitigations of such risks.

> *You must first assess, where appropriate in collaboration with the importer, if there is anything in the law and/or practices in force in the third country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR transfer tool you are relying on, in the context of your specific transfer. This implies determining whether your transfer falls within the scope of legislation and/or practices which may impinge on the effectiveness of your Article 46 GDPR transfer tool. The assessment required must be based first and foremost on legislation publicly available.*[411]

[409] *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, Case C-311/18, *op.cit.,* para. 134.

[410] European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Brussels*, Brussels 2020.

[411] *Ibid.*, p. 14.

This paragraph summarizes the requirement for verification of the transfer's impact and outcome. Even though, there is no formal indication of TIA in the document itself, and any assessment is, more or less, indicated as *an assessment* and not *the assessment,* there is an underpinning understanding that verification shall be conducted within the scope of risk assessment.[412] Further requirements for transfer impact assessment were also indicated by the newly enacted Standard Contractual Clauses from June 2021. In the module that applies to all possible transfer relations, namely Controller to Processor, Processor to Processor, Controller to Controller, and Processor to Controller, titled *Local laws and practices affecting compliance with the Clauses*, it is indicated that:

> *The Parties warrant that **they have no reason to believe that the laws and practices in the third country** of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities**, prevent the data importer from fulfilling its obligations under these Clauses**. (emphasis added).*

[…]

*(a) The Parties declare that in providing the warranty in paragraph (a), they **have taken due account** in particular of the following elements:*

*(i) **the specific circumstances of the transfer**, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;*

(ii) ***the laws and practices of the third country of destination**– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;*[413]

---

[412] The suggestion of a formal Transfer Impact Assessment is further indicated on pp. 3 of the Recommendation by the following wording: *You should conduct this assessment with due diligence and document it thoroughly. Your competent supervisory and/or judicial authorities may request it and hold you accountable for any decision you take on that basis*.

[413] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this

The scope, as indicated above, refers to the expectation that international data transfer, especially to a third-party country, shall be evaluated, assessed with all potential risks being mitigated before the transfer happens. According to the authorities quoted above, the Transfer Impact Assessment emerged as a term-of-art to formalize the process as the outcome of which the data exporter and the data importer assess the impact on privacy of transmitting personal information from the EEA to a country outside of the EEA that has not been covered by the adequacy decision of the European Commission.

It remains vital to see that the newly emerged requirement, named as a term of art under Transfer Impact Assessment, was never clarified with any indications on how to proceed or conclude such an assessment. At the same time, the obligation of measuring and mitigating risks is already placed upon data controllers or data exporters. Such a lack of clarity when it comes to the required mechanisms and how such mechanisms should be fulfilled leads us to the situation of poor visibility of data controllers' responsibilities and the potential risks of not fulfilling such responsibilities.

1. Question of adequate security measures for data transfer - Standard Contractual Clauses and other safeguards from the perspective of the data controller.

According to Article 44 of the GDPR, the transfer of personal data and the further intention to process personal data as the outcome of the transfer to a third party are possible only if the conditions laid down by the GDPR regarding data safety are obeyed and respected. Article 44 of the GDPR also opens an important chapter V of the Regulation that deals directly with international data transfer. Article 44 of the General Data Protection Regulation plays an important role in safeguarding the privacy and protection of personal data when it is transferred

practical experience is relied on to conclude that the data importer will not be prevented from complying with these Clauses, it must be supported by other relevant, objective elements, and it is up to the Parties to carefully consider whether these elements together carry enough weight in terms of their reliability and representativeness to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

to a third party. The GDPR sets strict conditions that must be obeyed and respected for personal data to be transferred safely to a third party. These conditions are in place to ensure that the personal data is protected from unauthorized access, disclosure, alteration, or destruction. Furthermore, data transfer requirements refer to the capacity to transfer personal data outside of the EU. Chapter V of the GDPR, which is opened by Article 44, is specifically dedicated to regulating the international transfer of personal data.[414] This chapter provides a framework for the transfer of personal data to countries outside the European Economic Area and ensures that such transfers are made only if adequate safeguards are in place.[415] The GDPR requires that the transfer of personal data to a third country comply with several conditions, including obtaining the explicit consent of the data subject or demonstrating that the transfer is necessary for the performance of a contract between the data subject and the data controller. Additionally, the transfer must be made only to countries that provide an adequate level of protection for personal data. In the absence of an adequacy decision, the GDPR allows for the use of specific safeguards such as binding corporate rules or standard contractual clauses. Overall, Article 44 of the GDPR plays a critical role in protecting the privacy and security of personal data when it is transferred to third parties. The GDPR's strict conditions and safeguards ensure that personal data is transferred lawfully and that it remains protected from unauthorized access, disclosure, alteration, or destruction. Compliance with Article 44 is essential for organizations that handle personal data to ensure they are meeting their legal obligations and protecting the privacy rights of data subjects.

Chapter V of the Regulation brought us some important and substantial adjustments when compared with Chapter IV of DPD[416]. The key change that exists between the DPD's way of regulating international transfers and the GDPR lies in the presentation of adequacy. The former content of Article 25 of the DPD was divided into two current articles, namely Article 44 dealing with a general understanding of requirements for data transfer and Article 45

[414] GDPR, art. 44, *Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation*[…].

[415] GDPR, art. 46.

[416] DPD, chap. IV, art. 25-27.

regulating the key element of the transfer regulation, namely adequacy[417]. Aside from Article 44, recitals 6, 101 and 102 serve as guidelines on how to interpret transfer requirements. Recital 6 places an emphasis on the matter of technological growth and the impact of large-scale processing on data safety:

> *Rapid technological developments and* ***globalisation*** *have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities* ***to make use of personal data on an unprecedented scale in order to pursue their activities****. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.*[418] *(emphasis added)*

The above-quoted recital remains of a guiding and abstract character; it emphasizes the importance of new technologies when it comes to data safety but at the same time treats it as the greatest risk. Such an approach filled with risk-based conviction is further loosened up in the Recitals 101 and 102, that refers to a more focused on the substance requirements of the Regulation. Recital 101 states that *A transfer* ***could take place only if****, subject to the other provisions of this Regulation, the* ***conditions laid down in the provisions of this Regulation*** *relating to the transfer of personal data to third countries or international organisations* ***are complied with by the controller or processor***[419].

Recital 101 further discusses that the transfer may be considered lawful only if both the controller and processor are in full compliance with the requirements of the GDPR. It is important to notice that such an understanding directly implies the obligation to meet foreign standards not only by European entities but also by third parties. This view is further supported by Recital 102, which refers back to the need for compliance with EU requirements as laid

[417] Any transfer that is not based on the adequacy decision regarding data safety in the country receiving the personal data will touch upon the question of adequate measures to secure the transfer. It remains a key element for all data controllers to operate on the security measures or other data transfer guarantees that are considered adequate. Among others, one of a formal elements of security data transfer is relying on Standard Contractual Clauses.

[418] GDPR, rec. 6.

[419] GDPR, rec. 101.

down by the GDPR. Furthermore, international data transfer also implies a two-step approach to data transfer.[420] Such a two-step approach can be traced back to the following:

- The controller has to comply with general data processing requirements as laid down by Articles 5 and 6 of the GDPR; and
- The controller has to further satisfy the requirements of data transfer as laid down by Chapter V of the GDPR[421].

It is also worth mentioning that all rules given to us thanks to Chapter V of the GDPR shall be interpreted in the light of the Charter since, as supported by the CJEU, the applicability of EU law entails the applicability of the Charter.[422] The idea that stands behind such understanding is also one of the most important underlying values behind the GDPR, namely the prevention of circumvention of the laws. It is difficult to deny that data protection differs around the world and that, as a consequence, standards of protection of personal data around the world also differ and are otherwise far from being coherent. The term circumvention has never been clarified by the CJEU; nevertheless, as the judicial practice of the CJEU grows, a series of the most important cross-border data transfer judgments arise, namely the *Scherm's cases*, which are all landmark decisions shaping the reality of outside-of-EU data transfer.

Starting with *Schrems*, the practice of the CJEU went in the direction of formalizing relations between the EU and the USA. Even though the relationship between the US and EU is not the main focus of the GDPR at all, the United States remains one of the most influential and important markets for Europe and inevitably one of the fastest growing technological areas of the world.[423] Consequently, it is important to recognize that the European Union and the United States are two coexisting organisms that are bound to cooperate.

---

[420] European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*. Brussels 2018, p. 3.

[421] E. Kosta, R. Leenes, I. Kamara, *Research handbook on EU data protection law*, Edward Elgar Publishing, 2022, Massachusetts, p. 321.

[422] C. Kuner, L. E., Bygrave, C. Docksey, *opt.cit.*, p. 757.

[423] According to the data presented by the European Commission, the EU and the United States have the largest bilateral trade and investment relationship and enjoy the most integrated economic relationship in the world. Although overtaken by China in 2021 as the largest EU import source for goods, the US remains the EU's largest trade and investment partner by far. Source: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en

Taking into account economic, legal, and philosophical considerations, there are a number of reasons why the US and the EU should collaborate on data transfer. Economically speaking, the EU and the US have substantial data flows between them and are big trading partners. The effective interchange of data made possible by data transfer cooperation will promote innovation and economic progress in both regions[424]. From a legal perspective, both the EU and the US have robust data protection laws in place, with the GDPR in the EU and various laws in the US, including the California Consumer Privacy Act (CCPA) and the Children's Online Privacy Protection Act (COPPA). Cooperation on data transfer would help ensure that personal data is transferred safely and legally between the two regions, respecting the privacy rights of individuals and complying with the relevant legal frameworks. Consequently, the high-level approach towards data protection and data safety remains, to the extent possible, coherent, even though both regimes are legally distinct. Moreover, from a doctrinal perspective, the EU and the US share common values regarding the protection of privacy and personal data. Both regions emphasize the importance of individual rights and the need for transparency, accountability, and data protection. Cooperation on data transfer would allow the two regions to align their legal frameworks and create a harmonized approach to data protection, benefiting individuals and organizations alike. In legal terms, cooperation between the US and the EU on data transfer can be achieved through various mechanisms, such as the adoption of standard contractual clauses or the establishment of a framework similar to the EU-US Privacy Shield. Additionally, both regions could work towards an adequacy decision that would recognize each other's data protection laws as providing an adequate level of protection for personal data, facilitating data transfer without additional safeguards. In order to promote secure transatlantic data flows and address the issues raised by the Court of Justice of the

[424] As a proof of political willingness but also real attempts to close the relationship between those countries, below-listed trade and economic initiatives shall be mentioned. The two most important economic agreements between the US and EU are the Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA). The TTIP was a proposed trade agreement between the US and the EU aimed at reducing barriers to trade and investment between the two regions. The agreement would have covered a wide range of sectors, including agriculture, services, and intellectual property. Negotiations for the TTIP began in 2013 but were suspended in 2016 due to public opposition and differences in regulatory approaches. The TiSA is another proposed trade agreement between the US and the EU, along with 22 other countries. The agreement is focused on liberalizing trade in services, including financial services, telecommunications, and transportation. Negotiations for the TiSA began in 2013, but progress has been slow due to concerns about the potential impact on labor and data privacy.

European Union in *Schrems II* from July 2020, the European Commission started the process for adopting an adequacy decision for the EU-U.S. Data Privacy Framework.[425] After President Biden signed an executive order on October 7, 2022, and US Attorney General Merrick Garland issued regulations, a draft decision was made. These two memos formalized the basic agreement reached by Presidents von der Leyen and Biden in March 2022.

Aside from the currently present movement towards a new transfer instrument between the US and EU, cooperation between those two jurisdictions has a long-standing history of failed concepts that ended up in the invalidation of the agreements between the EU and the USA with regard to data transfer security. As is currently recognized, cooperation between the US and EU requires formal guarantees that ensure the facilitation of data transfer between those regions[426]. Starting with *Scherms I,* which invalidated Safe Harbors, and then with Scherms II, which brought the final decision about no formal guarantees regarding data transfer, exchanging data between the EU and USA remains a gray area for data controllers. In a judgment dated July 16, 2020, the CJEU found that the Privacy Shield does not provide adequate protection of personal data in a third country, as stated in Article 45(2) of the GDPR. The assessment of the adequacy of protection should be resolved in terms of compliance with the content of Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union. These provisions guarantee the right to respect for private life, the right to protection of personal data, and the right to an effective remedy before a court when these rights (freedoms)

[425] European Commission Press Release, *Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US*, Brussels 2022. Retrieved March 5, 2023 from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631.

[426] There have been two agreements between the US and the EU that have been invalidated: the Safe Harbor Agreement and the EU-US Privacy Shield. (1) Safe Harbor Agreement: The Safe Harbor Agreement was a framework for data transfers between the EU and the US that was in place from 2000 to 2015. In October 2015, the Court of Justice of the European Union (CJEU) invalidated the Safe Harbor Agreement in the case of *Maximillian Schrems v. Data Protection Commissioner (Case C-362/14),* citing concerns over US government surveillance practices and the lack of redress for EU citizens. EU-US (2) Privacy Shield: The EU-US Privacy Shield was a framework for data transfers between the EU and the US that replaced the Safe Harbor Agreement in 2016. However, in July 2020, the CJEU invalidated the Privacy Shield in the case of *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Case C-311/18),* citing similar concerns over US surveillance practices and lack of redress for EU citizens. It is important to note that both agreements were invalidated due to concerns over US government surveillance practices and the lack of redress for EU citizens. The invalidation of these agreements has significant implications for businesses that transfer personal data between the EU and the US and has resulted in increased scrutiny over data transfers and privacy practices.

have been violated.[427] As a consequence of the Court's decision, the transfer of personal data to the US remains unsafe as long as it is not secured with proper and adequate security measures on the side of the data controller, with further restrictions on the use of the Standard Contractual Clauses. In response to the Irish authority's preliminary question, the CJEU clarified that the standard clauses' purely contractual nature, and thus their inability to bind public authorities in third countries (which are not parties), does not undermine the effectiveness of the Commission's decision. Indeed, the validity of the decision depends on an assessment of whether the decision contains effective mechanisms to ensure that the processing of data (after transfer to a third country) complies with the level of protection required by European Union law, as well as to halt the transfer of personal data in the event of a breach of the conditions set forth in the standard clauses or the inability to comply with them in the third country.

At this point, it is important to remember that the mechanisms offered by the GDPR when it comes to security measures are of an abstract nature, and furthermore, there is no one coherent mechanism on which to rely. It remains within the discretionary power and responsibility of the data controller to analyze risks and, based on such assessments, provide security measures.

[427] First, although the rights to privacy and protection of personal data are not absolute rights and may be restricted, for example, for reasons of national security interests, such restrictions must be narrowed to cases of absolute necessity. According to the principle of proportionality, this means that restrictions may be imposed only if they are necessary and genuinely meet objectives of general interest recognized by the European Union or the need to protect the rights and freedoms of others" (Article 52(2) of the Charter). This requirement is not met by the existing laws in the United States under which the intelligence surveillance programs operate, i.e., the Foreign Intelligence Surveillance Act (FISA), Executive Order 12333, and Presidential Policy Directive 28 (PPD-28). Indeed, these laws do not contain clear and precise rules governing the scope of application of the established restrictions on the rights of personal data subjects; in particular, they do not indicate the scope of the restriction, as well as under what circumstances and conditions data can be processed for intelligence purposes. Thus, the condition of limiting interference with the right to privacy and data protection to situations of absolute necessity is not fulfilled. Furthermore, internal U.S. legislation regulating the use of personal data for intelligence purposes does not guarantee data subjects an adequate opportunity to challenge decisions made in this regard before the courts. Not in every case of electronic surveillance carried out by US authorities are the persons concerned granted such rights. This is crucial, since the right to judicial review of possible violations of rights (freedoms) is explicitly guaranteed by Article 47 of the Charter. At the same time, the Court stressed that the institution of Privacy Shield Ombudsperson, introduced in the Privacy Shield, does not compensate for the above-mentioned protection deficiencies, especially since this body does not have the characteristic of adequate independence; nor has it been shown that it can issue decisions that bind the intelligence services. Consequently, Decision No. 2016/1250 on the recognition of Privacy Shield as meeting the condition of adequate protection was deemed null and void.

Prior to *Scherms II*, the Standard Contractual Clauses were acknowledged as the most trustworthy and established contractual norm for data controllers and/or data processors to implement in order to ensure transmission. Even though, GDPR attempts to list some of the appropriate security measures as SCCs, codes of conduct, or a set of technical types of measures suggested by the SCCs, the final use of the security measures is within the undefined scope of selection of the data controllers. The document also assumes that under special circumstances, additional safeguards may in fact be compensation for the change of purpose[428]. The CJEU ruling was particularly momentous for US-EU relations, as the United States is an important economic partner of EU member states, and the permissibility of seamless data transfer is an important element of economic circulation. Equally important, as the US is home to numerous companies providing popular cloud computing services (for example Microsoft, Google, along with many other relevant though less well-known IT providers). The main disruption around *Scherms II* and the conflict on the ground of EU-USA transfer arose from surveillance law. Under certain circumstances, cloud service providers are being asked by government authorities as part of criminal investigations to provide them with relevant information stored in their data centers. In March 2018, the U.S. Congress ratified the Clarifying Lawful Overseas Use of Data Act (*CLOUD Act*) for this purpose. This law regulates the transfer of data to U.S. authorities, even if the data is not stored in the U.S. but, for example, on servers in the European Union.[429] So the question now is whether, and if so how and on what basis, personal data can be transferred from the EU to the US - so as not to expose oneself to allegations of violating the provisions of the GDPR and the associated potential and severe financial consequences. The assessment of transfer mechanisms is regulated in a number of places across GDPR as an act:

- **General Prohibition of Transfer** is first introduced in previously quoted articles 44 and 45 and recitals 101, which state that the transfer of personal data to non-EU countries shall be subjected to limitation and exclusion unless there is a ground for such

[428] *Data Protection Working Party, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, 00569/13/EN WP 203,* p. 26. *Retrieved April 31 July, 2022 from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.*

[429] The CJEU pointed out in the Schrems II ruling that in certain circumstances, further measures, in addition to standard contractual clauses, are necessary to establish an adequate level of data protection in a third country.

transfer ensured when it comes to data security and such transfer is absolutely necessary.[430] Such understanding remains consistent with the DPD Directive;

- **Transfer to a Country with an Adequacy Decision Issued** – the European Commission has the right to issue an adequacy decision based on the predefined criteria.[431] When such a decision is issued by the Commission, the transfer shall not require any additional guidelines.[432] The Commission may declare third countries (or territories, a specified sector, or an international organization) to be covered by the Adequacy Decision.
- **Agreements Between Public Sector Bodies** – according to Article 46(2)(a) and 46(3)(b):

  The appropriate safeguards referred […] may be provided for, without requiring any specific authorisation from a supervisory authority, by: a legally binding and enforceable instrument between public authorities or bodies[433]. Furthermore, *Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: […] provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.*[434]

- **Binding Corporate Rules** – according to the GDPR it is possible to facilitate data transfer between a corporate group that includes cross-border transfer with the mechanism of corporate rules. Such rules shall be approved by a relevant data protection authority nationally (while being assessed by a member state country and

[430] Article 45, Article 46 and Recital 101 of the GDPR.

[431] According to Article 45 (2), such criteria includes: the rule of law, the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, and the international commitments the third country or international organization concerned has entered into.

[432] Article 45 (1) A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory, or one or more specified sectors within that third country, or the international organization in question, ensures an adequate level of protection. Such a transfer shall not require any specific authorization.

[433] GDPR., art. 46(2)(a).

[434] GDPR., art. 46(3)(b).

being subjected to a member state country law)[435]. Furthermore, binding corporate rules as a mechanism have to be specific in purpose and define the transfer scope.

- **Model Clauses** – Cross-border transfer is deemed to be permitted if the relationship between the controller and processor is covered by model clauses along with appropriate safeguards. The Commission is entitled to create new clauses and to adjust currently existing ones.[436] According to recital 81, *The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission.*[437] Further, the GDPR defines that the contract between the controller and processor may implement the Standard Contractual Clauses so as to facilitate the transfer, the act implies such understanding in the following wording of Article 28(6): *Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses*. Clauses shall also be implemented by the independent supervisory body on the territory of a member state country.[438] The use of Standard Contractual Clauses as a facilitating mechanism for data transfer was also the subject of discussionin in the above-mentioned Scherms II judgment.[439]
- **Codes of Conduct** – similarly to binding corporate rules it remains possible for an entity to facilitate data transfer based on the Code of Conduct that is approved as enough

[435] GDPR., rec. 108, rec. 110; art. 4(20), art. 46(2)(b), art. 47 and Guidelines of Working Party Article 29 - BCR Guidance (WP256, WP257).

[436] Furthermore, Recital 109 lays the background for the use of Standard Contractual Clauses: *The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.*

[437] GDPR, rec. 81.

[438] GDPR, art. 57 (j) and ®.

[439] The question of the validity of SCCs has been raised, as has the question of whether the clauses themselves may be enough to facilitate the transfer.

transfer security together with binding and enforceable commitments to provide appropriate safeguards.[440]

- **Legal obligations** – the GDPR places some additional mechanisms facilitating transfer in the case of court order or administrative arrangements.[441]

The list of possible transfer mechanisms shows the perspective of the data controller on the available options. For large entities and for internal transfers (transfers within the organization), binding corporate rules and codes of conduct come in handy. The transfer that happens as the outcome of the business activity of a medium or small enterprise is because those enterprises uses other tools to deliver a product or service. Furthermore, the only regulated and defined form of security measures that are formalized as Standard Contractual Clauses. Those clauses come in a defined form from the Commission and have an unchanged structure. Consequently, the eagerness to rely on the only known and predictable security measure was widely recognized among entrepreneurs. The solution, even though supportive for the entrepreneurs, was widely limited by the *Schrems II* judgment and changes to the understanding of Standard Contractual Clauses. In fact, all *Schrems judgments* may be viewed as landmark cases that substantially affected the way we understand data privacy transfer mechanisms and verification of data processing.[442] The reasoning behind the Schrems judgments was to expose the current vulnerabilities of the data transfer mechanisms. With *Schrems II*, aside from the Facebook infringement assessment, the focus of the audience was placed on the validity of Standard Contractual Clauses. It is important to mention that SCCs were never granted absolute power to ensure data processing security while data was in transfer, as SCCs were the only fully described and regulated form of transfer security mechanisms that were widely used by data controllers.

[440] Article 46(2)(e) of the GDPR reads as follows: *an approved code of conduct pursuant to Article 40, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.*

[441] GDPR, rec. 108; art. 46(3)(b), (4), and 63 of the for administrative decisions; and GDPR, rec. 115 and art 48 of the for the third-party court orders.

[442] In case C-362/14 Schrems (CJEU, Opinion of Advocate General, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, September 2015, ECLI:EU:C:2015:627) it was stated that the transfer based on the adequacy decision with respect to the protection of privacy and fundamental rights must be examined with a due diligence.

After Schrems, the discussion about what is right or wrong when it comes to the use of SCCs begun[443]. The CJEU confirmed the validity of the SCC but ruled that organizations transferring data must verify (on a case-by-case basis) whether the law in force in the country to which the personal data is transferred provides an adequate level of protection for personal data transferred under the SCC, and if the level of protection is not adequate, the organizations must either provide additional safeguards or suspend the transfer. The judgment requires EU data protection authorities to suspend the transfer of personal data in those cases where an adequate level of protection cannot be ensured. Consequently, after the Schrems II judgment, it remains within the scope of the data controller responsibility to follow the pattern of:

- **Analysis of the guidelines of the supervisory authorities** – from the currently known practice, the available guidelines remain fully supplementary, and all responsible offices reply on case-by-case assessments;
- **Evaluation of Data Transfer** – based on previously mentioned risk assessments or transfer impact assessments, the benchmark remains undefined here and is located somewhere between balancing test and case-by-case impact on individual assessments; and
- **Development of a Data Transfer Risk Assessment Model** – based on the previous point referring to the risks and mitigation models available.

All of the above shall aim to exceed the scope of risks brought by transfer. From a purely formal perspective, the assignment of responsibility for data transfer to the data controller seems intuitive; nevertheless, once we head towards practical implementation, the factual situation shows that there is no possibility to exclude transfer in general. As described in subchapter B(2)(ii), there is a narrow possibility to exclude transfer at all, and the mechanism to impact the assessment is, from a purely practical perspective, difficult because the actors delivering the services are usually suppliers of water, electricity, or municipal waste management rather than the controller relying on their services.[444] Consequently, it is inevitable to see the

[443] Historically speaking, the latest ruling is tied to a 2013 case in which Maximillian Schrems filed a complaint with Ireland's Data Protection Commissioner, claiming that the transfer of personal data under the *Safe Harbour* program for EU-US data exchange poses dangers to data protection. In the landmark judgment in Case C-311/18: (*Data Protection Commissioner v. Facebook Ireland Limited* and Maximillian Schrems, *op.cit.)*, handed down on July 16, 2020, the CJEU ruled that, in principle, the SCCs are valid, while it declared the *Privacy Shield* invalid.

[444] Subchapter B(2)(ii) mentions service providers such as Amazon, IBM, Braintree, Stripe, or Google. Respectively, Amazon's market share fluctuates around 25%, IBM around 4%, Braintree is owned by PayPal, one

disproportion between the data controllers and vendors used to deliver the service. Even more important is the fact that almost every market leader transfers personal data to third party countries, especially the US.

The lack of an adequacy decision towards the US creates a fallacy of law in action, as it renders the General Data Protection Regulation only a law in books. This is particularly relevant given the extensive geolocation of major IT companies in the US.[445] The GDPR is a fundamental data protection framework that aims to safeguard the privacy of EU citizens and protect their personal data against unauthorized access and misuse. However, the GDPR's effectiveness is hampered by the absence of a viable mechanism for data transfers between the EU and the US. In the absence of an adequacy ruling, personal data transmitted from the EU to the US may be vulnerable to US government monitoring methods that violate EU privacy rules. This raises worries about the preservation of basic rights and liberties, as well as the possibility of data breaches and exploitation. From a political and legal aspect, this dilemma demonstrates the discrepancy between the law in books and the law in practice, as expressed by Justice Holmes and Pound. The law in books refers to the formal legal rules and frameworks created by the government and judiciary, whereas the law in action refers to how these laws are applied in society. The lack of an adequacy decision towards the US creates a gap between the law in books and the law in action, as it hinders the practical application of the GDPR in the context of transatlantic data transfers. This gap undermines the legitimacy of the GDPR and creates a

of the biggest market providers when it comes to payment with a total market share of around 32%, Stripe with around 19% market share, or Google with the monopoly on a set of products starting from search engines, through payment methods, data storage, website analytics, and adding towards the product placement. Data based on the reports available via *Datanyze software*. Retrieved December 4, 2022 from https://www.datanyze.com/.

[445] The assertion that many significant IT companies have their headquarters in the US is well-supported by a variety of sources. For instance, six out of the top ten technological corporations are headquartered in the US, according to the *Forbes Global 2000* list of the largest public companies in the world (Retrieved March 5, 2023 from https://www.forbes.com/lists/global2000/. Apple, Microsoft, Alphabet (the parent company of Google), Facebook, Cisco Systems, and Intel are some of these businesses. Several additional IT firms, like Amazon, Twitter, and Salesforce, to name a few, are headquartered in the US in addition to these top firms. Additionally, a large number of these businesses operate and process data in the EU. For instance, Google maintains offices and data centers throughout the EU, notably in Ireland, Finland, and Belgium. Amazon has built multiple data centers across the EU, while Facebook has a sizable data center in Sweden. Since this impacts the ability of these enterprises to transfer personal data from the EU to the US while adhering to EU data protection regulations, the problem of transatlantic data transfers and the absence of an adequacy judgment towards the US become especially pertinent.

situation where the law in action deviates from the law in books, which may lead to a loss of public trust and confidence in the legal system. From a doctrinal perspective, this issue highlights the need for a more nuanced approach to the concept of law, which takes into account the complexity of the modern world and the interplay between different legal systems and jurisdictions while at the same time, considering the possibility of applying the law in practice. The legal doctrines of Justice Holmes emphasize the importance of understanding the social and economic context of the law and recognizing the limitations of formal legal rules in addressing complex societal problems. A similar approach and dedication to discussing the matter of right in practical application were further discussed by Pound – quoted in the prior chapter of this thesis. Lack of such a corresponding approach between social reality and law makes law only a concept present in books and not applied in practice[446]. The lack of an adequate decision towards the US illustrates the need for a more dynamic and flexible legal framework that can adapt to the changing realities of the global digital economy and ensure the protection of fundamental rights and freedoms in a rapidly evolving technological landscape.

Deriving from the doctrinal and legal evaluation, one conclusion remains extremely visible - currently, on the grounds of the above-described *Schrems judgment*, there is no privacy agreement between the US and EU that may facilitate the data exchange. In such circumstances, it seems non-excessive to say that every SaaS, PaaS, or cloud-based provider transfers personal data, and most likely, such a transfer will happen outside of the Member States. This factual situation, combined with the perspective on the responsibility of data controllers and the approach – controller always being in charge of data processing, leads us to the difficult conclusion that even though there is a responsibility for data controllers, their factual decision-making is very limited, making their ability to realistically rely on legislation only mediocre.

[446] Justice Holmes stated in one of his dissenting opinions that *The prophecies of what the courts will do in fact, and nothing more pretentious, are what I mean by the law*. This quote originates from a dissenting opinion in the case U.S. Supreme Court, *Northern Securities Co. v. United States*, 193 U.S. 197, no. 277, March 1904, here Holmes elaborates on the idea that the law is ultimately shaped by the actions of judges and other legal actors, rather than by abstract legal principles or theoretical frameworks. Holmes was convinced that the practical outcomes of legal decisions are the real backbone of what is law and, in fact, are more important than any theoretical or doctrinal considerations, and that judges should be guided by the practical realities of the cases before them. This approach to the law is relevant to many different areas of legal practice, as it emphasizes the importance of taking into account the real-world consequences of legal decisions and frameworks, rather than relying solely on abstract legal reasoning and seems to be extremely up to date with regard to the GDPR.

The question of data processing adequacy or the adequacy of security measures is of an abstract character, and from a philosophical perspective, it should remain on an abstract level, to firstly define the aim of protection and then navigate through the possibility to protect individual rights in practice. Nevertheless, what is still missing is reliability and the option to decide about actions based on an understanding of their effect. Such an ability to foresee the effects of actions and consequences is, in my opinion, narrowed down and limited when it comes to the GDPR and the liability placed upon data controllers. The most important actors in the path of data processing are, looking from the perspective of this legal act, forced to be in a position of the doctrinal *bad guy* focused only on consequences because the consequences are of a great scale and limited explanation.

2. The right to be forgotten from the perspective of CJEU requirements.

The idea of the *right to be forgotten* has drawn a lot of attention recently, especially in the area of internet privacy. The Court of Justice of the European Union (CJEU) developed explicit guidelines for the right to be forgotten in 2014. The concept of the right to be forgotten is often viewed as a right; nevertheless, from a critical analysis, it is possible to evaluate it as a social value or a legal policy of behavior[447]. Hence, although it may be thought of as a legal right (*de lege lata* or *de lege ferenda*), it can also be considered a value or interest deserving of protection or a goal of policy that must be attained by all means necessary, including through the use of legislation or other regulatory mechanisms.[448] The right to forget represents another important psychological dimension, especially while considering the aspect of privacy and the desire to control information about oneself, namely, it uses the first-person perspective because it is equally crucial to be able to forget your own past, unlike the right to be forgotten, which takes

[447] For example, J-F Blanchette and DG Johnson, in their publication titled *Data Retention and the Panoptic Society: The Social benefits of Forgetfulness*, 2002, p. 18 The Information Society, pp. 33-45 discussed the *social value of forgetfulness*. Furthermore, M Dodge and R Kitchin at *Outlines of a World Coming into Existence': Pervasive Computing and the Ethics of Forgetting*, 2007, 34 Environment and Planning B: Planning and Design, ppp. 431-445 viewed the right to be forgotten as a matter of ethical policy.

[448] B. J. Koops, *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice*,SCRIPT ed: A Journal of Law, Technology & Society 2012, vol. 8, p. 3. Retrieved April 17, 2023 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719.

the viewpoint of third parties who should be allowed to forget about your past. This has social and legal ramifications instead of being primarily psychological in nature (since forgetting is typically presented as a normal function of the human brain that does not need reinforcement as such): the right to avoid being confronted with your past (which you have forgotten or would like to forget yourself). Being forgotten and forgetting both fall under the umbrella term of *forgetfulness,* or the French word *oubli*.

From a purely academic perspective, the right to be forgotten has been the underpinning element of the European data protection and data privacy laws, which was, among others, highlighted by European Commissioner Viviane Reding. In her major policy proposal for the review of the Data Protection Directive (95/46/EC), European Commissioner Viviane Reding mentions the right as a component in the following wording:

> *[…] strengthening the so-called "right to be forgotten", i.e. the right of individuals to have their data fully removed when they are no longer needed for the purposes for which they were collected or when he or she withdraws consent or when the storage period consented to has expired*[449].

The idea of the right to be forgotten as presented above may be viewed as a philosophical question; in fact, what it means to delete the data, and to what extent the data should be deleted. Along with technological growth, the potential and practical dimensions of data removal change. In fact, to what extent do data controllers have to sacrifice their business capabilities to remove the data? Victor Mayer Schönberger, who has provided one of the most thorough analyses of the right to be forgotten in academic literature to date, has a perspective that is essentially in accordance with emphasis on data-deletion duties. His key suggestion is to *bring the concept of forgetting in the digital era through expiration dates for information*, in addition to current systems that stimulate forgetting, in order to recalibrate the shifting balance between memory and forgetting.[450] Also, two other perspectives that cast forgetting in a slightly different light can be seen in the literature. The first places special emphasis on the connection with the notion of a *new start* or *clean slate,* which has long been a component of various legal systems designed to promote societal forgetting, including bankruptcy law, juvenile criminal law, and credit reporting. It should be noted that under Swiss law, guarantees that a person can

[449] V. Reding, *The Upcoming Data Protection Reform for the European Union*, 2011, 1 International Data Privacy Law, pp. 3-5;

[450] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age,* Princeton, 2009, p. 198.

prevent others from recognizing her in connection with her criminal past.[451] This focuses more on controlling the use of data than it does on data deletion[452].

While reviewing the examples presented above, it becomes obvious that the right to be forgotten may be traced back either to its narrow scope of understanding as currently shaped by the data protection laws or may be treated in a broader manner as a right, social concept providing safety, or a legal policy that ensures individuals have control over the information shared about them. To properly evaluate the right to be forgotten in the light of current legal challenges and new technologies, it remains important to focus on the modern understanding of the right. The GDPR, enacted by the European Union in 2016 and going into force in 2018, is where the history of the right to be forgotten begins. The GDPR-established right to erasure allows users to request that their personal data be deleted in certain circumstances.

In the case of *Google Spain,* the European Court of Justice expanded on this right by declaring that people have the right to ask search engines to remove links to information about them, the information being unreliable, insufficient, irrelevant, or excessive.[453] The right to privacy and the right to data protection are two more legal notions that aim to preserve people's privacy and are closely related to the right to be forgotten. These ideas are reflected in a rising understanding of the significance of protecting personal information in an increasingly digital society. They are codified in numerous international treaties and national legislations.[454]

---

[451] B. J. Koops, *opt.cit.* pp. 5-6.

[452] *Ibid.*

[453] Consequently, interest in the right to be forgotten finds its underpinning value not only in the ability to shape the information but also in the principle of quality and accuracy, as further highlighted by the GDPR.

[454] The Universal Declaration of Human Rights (UDHR), which was approved by the United Nations General Assembly in 1948, is a prime illustration of a multinational treaty that enshrines the right to privacy. No one *should be subjected to arbitrary interference with his privacy, family, home or communication, nor to attacks upon his honor and reputation*, according to Article 12 of the UDHR. Since then, this principle has been confirmed and expanded upon in various international agreements, including the European Convention on Human Rights and the International Covenant on Civil and Political Rights (ICCPR) (ECHR). Many nations have passed laws protecting the right to privacy and personal data under their own national laws. Many nations have passed laws protecting the right to privacy and personal data under their own national laws. For instance, the Privacy Act of 1974 in the United States regulates the gathering, use, and disclosure of personal data by federal entities. The General Data Protection Regulation (GDPR) in the European Union lays out detailed guidelines for how businesses and organizations may process personal data. Similar regulations exist in other nations as well, such

The right to be forgotten, however, also raises significant concerns about how to strike a balance between personal privacy and freedom of expression, as well as the practical difficulties of putting such a right into effect. For instance, there is disagreement over how to define the parameters of the right to be forgotten, how to evaluate erasure requests, and how to strike a balance between the interests of individuals and those of the public. Notwithstanding these difficulties, the right to be forgotten has recently received a lot of attention and support, both within the EU and outside of it. Many supporters contend that it is a vital instrument for preserving individual privacy and giving people control over their own personal data. But the idea also continues to draw criticism and skepticism from some places, especially in light of its possible effects on free speech and the public's right to information. In general, the legal idea of the right to be forgotten is still complex and developing, and it will be discussed and improved throughout time.

The specific guidelines for the right to be forgotten have been included in the landmark 2014 CJEU ruling in *Google Spain*.[455] In this case, the CJEU established that, under certain circumstances, individuals have the right to request that search engines such as Google remove links to personal information that is "inaccurate, inadequate, irrelevant, or excessive" from search results. The CJEU also outlined criteria that search engines must consider when evaluating such requests, including the public's interest in accessing the information and the individual's right to privacy. These guidelines have since been referenced and expanded upon in subsequent cases and regulatory frameworks, both in the EU and beyond. Since then, these guidelines have shaped legal frameworks and discussions all over the world. These specifications, which call for balancing the rights to privacy and information, have significant ramifications for people, businesses, and governments. This subchapter examines the standards set forth by the CJEU for the right to be forgotten, its implications for personal data privacy and free speech, and the current difficulties in implementing and upholding this right.

In addition to the landmark 2014 CJEU ruling in the *Google Spain* case, there have been several other significant cases related to the right to be forgotten. One such case was the 2018 Supreme

as the Personal Data Protection Act (PDPA) in Singapore and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. These rules are made to safeguard people's right to privacy and control how their personal information is used in different situations.

[455] *Google Spain …,* C-131/12, *op. cit.*

Court of Canada ruling in *Google Inc. v. Equustek Solutions Inc.*[456] This case involved a lower court decision that ordered Google to remove search results worldwide related to the sale of products that were the subject of intellectual property infringement. The Supreme Court upheld this decision, expanding the scope of the right to be forgotten beyond personal data to include other types of information. Another notable case was the 2019 CJEU ruling in *Google LLC v. Commission nationale de l'informatique et des libertés* (CNIL).[457] In this case, the CNIL had ordered Google to remove links not just from its European domains, but from all domains worldwide.[458] The CJEU clarified that the right to be forgotten is not absolute but applies globally when a search engine processes personal data for EU residents.

From these cases, it can be concluded that the right to be forgotten is a complex and evolving legal concept that involves balancing individual privacy rights with other fundamental rights and interests, such as freedom of expression and access to information. While the right to be forgotten is not absolute, it can apply globally when search engines process personal data for EU residents. Additionally, the right to be forgotten can apply not just to personal data but also to other types of information. Other cases related to the right to be forgotten include the 2020 CJEU ruling in *A v. Google LLC*, which established that the right to be forgotten does not apply to information related to criminal proceedings that resulted in an acquittal.[459] In 2019, a French court ordered Google to pay a fine of €50 million for failing to properly implement the right to be forgotten, in what was seen as a significant enforcement action. The case of *NT1 and NT2 v. Google LLC*, which was heard by the UK Court of Appeal in 2019, involved individuals

[456] Supreme Court of Canada, *Google Inc. v. Equustek Solutions Inc*., 2017 SCC 34.

[457] CJEU, Judgement, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, September 2019. ECLI:EU:C:2019:772.

[458] The case from the Canadian Supreme Court touches on different approaches towards the right to be forgotten or the actual right to forgot/erase certain sets of data. While the right to be forgotten initially focused on personal data, some cases have expanded its scope to include other types of information as well. For example, in the 2018 Supreme Court of Canada ruling in *Google Inc. v. Equustek Solutions Inc*. (SCC, Judgments, *Google Inc. v. Equustek Solutions Inc*., SCC 34, [2017] 1 S.C.R. 824, June 2017.), the court granted an injunction ordering Google to remove search results worldwide related to the sale of products that were the subject of intellectual property infringement. This case expanded the scope of the right to be forgotten beyond personal data to include other types of information. Even though Canadian jurisdiction remains distinct from European jurisdiction, Canada as a country covered by the adequacy decision represents an interesting comparative jurisdiction that discloses the potential expansion of the shape of right to be forgotten.

[459] CJEU, Judgement, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, September 2019. .

seeking to have links to past criminal convictions removed from Google search results.[460] The court ruled against the individuals, finding that the public had a legitimate interest in accessing the information. Overall, these cases demonstrate the ongoing challenges and complexities of implementing and enforcing the right to be forgotten, as well as the need for careful consideration of the various rights and interests at stake.

With regard to the technological dimension, the right to be forgotten requires certain investments and may call for the total reconstruction of the infrastructure. There are various specifications for actual databases that have an immediate impact on the issue of data removal. In most cases, they are referred to as ACIDs, which stands for atomicity, consistency, isolation, and durability. These terms are described as follows: atomicity, consistency, isolation, durability, ability to perform rollbacks, replication, and back-ups and many more[461]. The main aim of any principle standing against the right to be forgotten depicts the challenge that the data controller shall face upon implementing a potential request to permanently remove the data while at the same time being obliged to show due care about the consistency and safety of other personal data stored in the same database or a cluster of databases.

The right to be forgotten not only came as a break-through element included in the GDPR and further evaluated by the European Court of Justice, but it also gave a rise to the new tendency of *arising laws* that entered the discussion, especially when it comes to the area of new technologies and broadly understood IT. One of these newly arising interpretations of what is included in the GDPR, aside from the right to be forgotten, is the newly invented *right to explanation*. It is claimed that the GDPR contains a provision known as the *right to explanation* that allows anyone to request an explanation of an algorithmic judgment that has been made about them.[462] The right to an explanation or the *right to know* are common names for this privilege. The right to explanation, however, is a contentious idea that some contend is a fallacy with regard to interpretation. The right to explanation crosses paths with the right to be

[460] UK, Court of Appeal, *NT1 and NT2 v. Google LLC*, HQ15X04128, HQ15X04127 [2018] EWHC 799 (QB). April 2018 and UK, Court of Appeal, *A Local Authority v A Mother and Others*, B4/2019/0291 [2019] EWCA Civ 799, May 2019.

[461] T. Li, E.F. Villaronga, P. Kieseberg, *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, Computer Law & Security Review 2018, vol. 34, no. 2, pp. 304-313.

[462] The idea of right to explanation gained attention, among others, after the publication of the workshop by Bryce Goodman and Seth Flaxman: *Eid., EU Regulations on Algorithmic Decision Making and "a Right to an Explanation"*. AI Magazine 2017, vol. 38 no. 3, pp. 50-57. Retrieved April 17, 2023 from https://ojs.aaai.org/aimagazine/index.php/aimagazine/issue/view/219.

forgotten and, at the same time, steals some attention from the directly disclosed right included in Article 17 of the GDPR. The right to explanation seems to overlap and mutually affect the right to be forgotten when it comes to the algorithms' functioning. From a purely social perspective, it seems logical to first understand the conclusion taken by the algorithm before making the decision to request the removal of certain findings or suggestions made by it. One of the biggest objections to the right to explanation in this regard is that it presupposes algorithms can always give simple, understandable justifications for their choices. In fact, many algorithms are so intricate that it is challenging, if not impossible, to explain how they came to a certain conclusion. In other instances, the algorithm's justification might not be adequate to completely comprehend why a certain choice was taken[463]. At the same time, a further layer of challenge has been placed on the right to be forgotten by the current development of artificial intelligence, especially with regard to openAI and *chat.openai.com*, which have become two of the most influential AI processing machines.[464] A legal principle that has gained significance in the digital age is the right to be forgotten, but should it change or even become void under the challenges of AI processing?

It is likely that as AI technology develops, so will the methods used to implement and uphold the right to be forgotten. The management and storage of data is one of the most significant ways that AI may have an impact on this right. The automatic detection and removal of personal information from online sources can be programmed into AI systems. As a result, people may be able to exercise their right to be forgotten more quickly and easily. Even if they are not immediately obvious to humans, an AI system may search a website or database and find all

[463] Some contend that by concentrating on the right to an explanation, we are neglecting other crucial privacy rights, such as the right to be forgotten. Individuals have the option to ask data controllers to delete their personal information under the right to be forgotten. This is a crucial right because it enables people to manage their own data and restricts the amount of private information that is publicly accessible online. Yet, because it requires data controllers to locate and erase every piece of personal information they have about a person, which can be a laborious undertaking, the right to be forgotten can be hard to enforce. The right to explanation, in comparison, is quite simple to implement because it only calls for data controllers to give a justification for an algorithmic choice. This could result in a situation where businesses prioritize adhering to the right to explanation above the harder and more expensive process of adhering to the right to be forgotten.

[464] Open to the public model available to the public that is free of charge as of March 11, 2023 is available via https://chat.openai.com/chat. The solution proposed by OpenAI retrieves the data based on the ChatGPT models (currently available to the public is both API and interface operated modules that are based on ChatGPR-2 and ChatGPT-4). Microsoft Azure is currently working on the release of ChatGPT-4 to open it to the companies/vendors who successfully pass the application to their program.

instances of personal information that need to be deleted. This could make it possible to preserve people's privacy rights more effectively than if people had to actively look for and delete personal information. At the same time, AI-based processing of personal data will make targeting information about individuals even more accessible and faster than before.[465] Regarding AI and the right to be forgotten, openness and information freedom are two other crucial factors to take into account. Due to the fact that it entails erasing material from the public domain, the right to be forgotten may significantly affect these principles, mostly because AI does not forget in a way that was, until now, understood by human-mind focused thinking-[466] It will be crucial to strike a balance between people's right to privacy and the public's right to access information as AI systems increasingly adopt the right to be forgotten. In order to prevent the right to be forgotten from unreasonably restricting access to information, there may be a requirement to create AI systems that can recognize and delete personal information while leaving other information untouched.

For a variety of reasons, applying the right to be forgotten to AI models can be more difficult than applying it to search engines and other conventional methods. Initially, a lot of data, including a plethera of personal data, is used to train AI models. The accuracy and performance of the model may be impacted if this data is eliminated from the training set. Personal data like credit ratings, insurance quotations, and employment suggestions can be used to inform AI models' decision-making and output generation. In certain circumstances, eliminating personal information from the model could lead to skewed or incorrect judgments, which might be challenging to fix without retraining the model. Lastly, because AI models can be implemented across a variety of systems and platforms, it may be challenging to guarantee that all copies of the model have been created with all personal data totally erased.
In conclusion, carrying out the right to be forgotten for AI modules necessitates careful evaluation of the potential effects on the model's precision and efficacy, as well as the moral and legal ramifications of removing personal data from the model's training data and decision-making processes.

[465] AI, meanwhile, has the potential to be abused in order to violate the right to be forgotten. For instance, someone may use AI to saturate databases and search engines with removal requests, making it challenging for real removal requests to be handled. This could result in the removal of information from the public domain, even if it is pertinent and significant.

[466] T. Li, E.F. Villaronga, P. Kieseberg, *opt.cit*, pp. 304-313.

At the end of the evaluation of the broad analysis of the right to be forgotten in the light of CJEU judgments, it remains important to observe the timeline. The most representative judgment referring to the right to be forgotten is dated 2014[467]. At the same time, technology has jumped incredibly far from the reality of 2014. On the one hand, the right to be forgotten interferes with one of the most fragile elements of the IT system infrastructure, namely data storage, and at the same time is considered to be one of the least re-visited issues by the legislative bodies. Consequently, execution of the right to be forgotten for the data controllers may be extremely challenging due to a lack of new guidelines and a technological reality that goes through the same turning points as does the ChatGPT release.

Yet, it should be emphasized that the right is merely an *a posteriori* band-aid fix. The right can only stop further (harmful) processing and dissemination because it only arises after the collection. Attacking the problem's source is required for a lasting solution. Over the years, numerous solutions have been put forth. In this regard, it is important to emphasize anonymization, transparency, encryption, clearer privacy notices, data minimization, awareness-raising, and other important concepts that, though unclear, may provide better privacy protection. Each of these steps aims to stop the spread of information that could be damaging in the first place.

[467] *Google Spain SL…,*C-131/12, *op.cit.*

C. Implementation challenges in SaaS online operating software.

1. Third-party processors and data transfer at SaaS products.

Software as a Service (SaaS) is a software delivery paradigm in which a third-party provider hosts a software application and makes it available to clients through the internet. Customers can access software using a web browser rather than installing and maintaining it on their own PCs or servers. SaaS providers typically charge customers a subscription fee for access to the software and handle the maintenance, security, and support of the software on their own servers. SaaS is a popular option for businesses because it allows them to access software applications without the need to invest in expensive infrastructure and IT staff to maintain it. It also allows for easy scalability and flexibility, as users can easily add or remove users and access the software from any device with an internet connection. Some examples of SaaS applications include customer relationship management (CRM) systems, project management tools, and office productivity software. It is difficult to determine the exact market share percentage of SaaS as a software delivery model, as it depends on the specific market or industry being considered. Additionally, the market for SaaS is constantly evolving and growing, making it challenging to accurately measure market share. However, SaaS has become a widely adopted model for delivering software, particularly for business-oriented applications. According to a report by Grand View Research, the global SaaS market was valued at $106.3 billion in 2018 and is expected to reach $223.8 billion by 2025, growing at a compound annual growth rate of 10.7%.[468] This expansion is being driven by the increasing adoption of cloud computing and businesses' desire to reduce IT costs and improve efficiency. In general, as more firms switch to cloud-based solutions, SaaS is likely to acquire market share in the software sector. SaaS enterprises and companies that expand on this model are one of Europe's most important business divisions. In general, Europe has a thriving SaaS industry, with many successful companies offering a wide range of software applications as a service. Some examples of well-known SaaS companies based in Europe include Zendesk, UiPath, and DocuSign. The market for SaaS in Europe is expected to continue to grow in the coming years,

[468] GVR Report cover SaaS Market Size, Share & Trends Report SaaS Market Size, Share & Trends Analysis Report By Type (Enterprise Software, Productivity Software), By Region (North America, Europe, APAC, Central & South America, MEA), And Segment Forecasts, 2022–2028, Retrieved December 30, 2022 from https://www.grandviewresearch.com/industry-analysis/saas-market-report.

driven by the increasing adoption of cloud computing and the desire of businesses to reduce IT costs and improve efficiency.

There are several reasons why companies may choose to use SaaS (Software as a Service) instead of other software delivery models:

- Cost: SaaS can be more cost-effective than other options, as it allows companies to access software applications without the need to invest in expensive infrastructure and IT staff to maintain it. SaaS providers typically charge customers a subscription fee for access to the software, which can be more predictable and easier to budget for than the upfront costs associated with other delivery models.[469]
- Maintenance and updates: SaaS providers handle the maintenance, security, and updates of the software on their own servers, which can be a significant burden for companies that have to manage these tasks themselves.
- Scalability and flexibility: SaaS allows for easy scalability and flexibility, as users can easily add or remove users and access the software from any device with an internet connection.
- Time to deployment: SaaS can be deployed more quickly than other delivery models, as there is no need to install software on individual computers or servers.
- Integration with other tools: SaaS products often have APIs (application programming interfaces) that allow them to easily integrate with other tools and systems, which can improve efficiency and streamline workflows.

Overall, companies may use SaaS to reduce IT costs, improve efficiency, and access the latest software applications and features without the need for a significant upfront investment. On the other hand, because SaaS companies are one of the most rapidly growing industries in the IT environment, the challenges arising from implementing the GDPR in this area are even more vital. On the other hand, looking from a purely practical perspective, IT industries, including SaaS and PaaS, process personal data on the largest scale. As a consequence, the potential risk of infringing upon data safety grows linearly. To depict the risk-based scale of data processing, the following data leaks related to the IT industry, narrowed down to SaaS companies, shall be listed:

[469] J. Grabski , *Valuation Techniques and the Economics of Software as a Service* [In;] *SSRN* [online]. Retrieved December 30, 2022 from https://ssrn.com/abstract=3509782.

- In 2020, hackers accessed the data of millions of users of the SaaS platform Zoom, including names, email addresses, and other personal information.
- In 2019, the SaaS company MongoDB had a data leak that exposed the personal information of millions of users, including names, email addresses, and passwords.
- In 2018, the SaaS company Exactis suffered a data leak that exposed the personal information of nearly 340 million individuals, including names, addresses, phone numbers, and other sensitive data.
- In 2017, the SaaS company OneLogin had a data leak that exposed the personal information of millions of users, including names, email addresses, and passwords.

The scale of the revealed data shows the day-to-day scope of data processing by SaaS service providers. Once there is a clear picture of the size of the industry and the potential impact of SaaS providers when it comes to data processing activities, it remains important to tie it up with the idea of legal responsibility and the challenges that arose after the GDPR emerged.

The General Data Protection Regulation (GDPR) imposes a number of requirements on organizations that process personal data of individuals in the European Union (EU). These requirements can pose significant challenges for software as a service (SaaS) providers, who often process large amounts of personal data on behalf of their customers. One challenge for SaaS providers is the need to ensure that they have appropriate technical and organizational measures in place to protect personal data from unauthorized access, use, disclosure, or destruction. This includes implementing appropriate safeguards to protect personal data from cyber threats and data breaches. Another challenge for SaaS providers is the need to comply with the data subject rights provisions of the GDPR. These provisions give individuals certain rights in relation to their personal data, including the right to access their personal data, the right to rectification, the right to erasure (also known as the *right to be forgotten*), the right to restrict processing, and the right to data portability. SaaS providers may need to implement systems and processes to enable them to respond to these rights in a timely and effective manner.

A further challenge for SaaS providers is the need to ensure that they have a legal basis for processing personal data under the GDPR. This may require SaaS providers to enter into contracts with their customers that set out the terms under which personal data will be processed. Lastly, the use of data providers is an inseparable element of SaaS operations; consequently, the ability to exclude data transfer remains a fiction and difficult to apply in

practice. Overall, the GDPR presents a number of challenges for SaaS providers, who must ensure that they have the necessary technical and organizational measures in place to protect personal data and comply with the requirements of the GDPR. Implementation of the GDPR at any IT company, including SaaS companies, may be traced back to three major areas:

- Internal valuation: this area aims to assess internal data flow and further assign risks and potential data flaws in internal software construction. At the moment when GDPR came into force, as described beforehand, SaaS as a market segment was already a long-standing industry; consequently, implementation of the GDPR happened mostly on already existing software.
- External valuation: this area aims to define how data is being shared externally to third-party vendors, who, from a purely legal perspective, stand as data processors or controllers that further process the data on a particular company's behalf.
- Product development phase: this area focuses on the way new software pieces are crafted and how data privacy is being implemented in the day-to-day process of the developer's craftsmanship.[470]

While assessing the implementation challenges in this thesis, the main focus shall be placed on external valuation, referring to data transfer, with some mentions of the internal valuation phase. An average SaaS, while delivering the service (that is, product access), uses at least the following types of software that support product delivery:

- task management tool[471];
- CRM[472];

[470] Product development stage shall be further supported by the understanding of how the software is being crafted. As rightly highlighted by Chong Ee in the book titled *Configuring Internal Controls for Software as a Service: Between Fragility & Forgiveness* on p. 320, product backlogs and product development is usually organized around two-week scrum-based sprints, and the auditing process, and well as measure implementation shall be customized to fit into this process. Consequently, the old form of auditing that assumes phase when the product is considered to be *done* fails when it comes to SaaS. By definition, SaaS is constantly changing and evolving and there is no phase of *done* consequently, the environment to which we apply legal measures changes all the time.

[471] As an example, Jira has a brief 40% market share, Asana has around 15% market share, and Basecamp has 5% of the market share.

[472] Customer Relationship Management (CRM) software is used by organizations to manage their interactions with customers, clients, and other stakeholders. There are many CRM tools available on the market, and the most popular ones vary depending on the specific needs and requirements of different organizations. Salesforce is generally considered to be one of the leading CRM platforms in the market, with a strong presence in the enterprise segment. According to a report by Gartner, Salesforce had a 20.8% market share in the CRM software market in

- data storage center (virtual databases) and physical machines supporting virtual databases[473];
- database management system[474];
- version control system[475];
- payment collection system[476].

2020. Hubspot is also a well-known CRM platform, particularly in the small and medium business (SMB) segment. According to a report by Gartner, Hubspot had a 2.5% market share in the CRM software market in 2020. Zoho CRM is a popular CRM platform, particularly for SMBs. According to a report by Gartner, Zoho had a 1.4% market share in the CRM software market in 2020.

[473] When it comes to the database, there are a plurality of vendors that provide such a service, including IBM, OVH, or Amazon (AWS). According to a report by Gartner, IBM had a 3.2% market share in the global public cloud infrastructure as a service (IaaS) market in 2020. IBM is also a major player in the enterprise software market, with a 2.7% market share in the application platform as a service (aPaaS) market in 2020. According to a report by Gartner, AWS had a 32.4% market share in the global public cloud infrastructure as a service (IaaS) market in 2020. This made AWS the largest provider of IaaS in the market, ahead of other major players such as Microsoft Azure (18.9% market share) and Google Cloud Platform (8.5% market share).

[474] Postgres, MongoDB, or ElasticSearch are some of the more frequent examples of database management systems. One SaaS provider may need to use more than one database management system, which may further increase the potential for data transfer. MongoDB is a popular open-source database management system that uses a document-oriented model to store data. It is designed to be scalable, flexible, and easy to use, and is often used to store large amounts of data in a variety of formats, including structured, semi-structured, and unstructured data. PostgreSQL, or Postgres, is a popular open-source object-relational database management system (ORDBMS). It is known for its robustness, reliability, and flexibility, and is often used for mission-critical applications. Postgres is designed to be highly extensible, with a wide range of features that support a variety of data types, index types, and programming languages. It is implemented using the SQL (Structured Query Language) standard, which makes it easy to use and integrate with other systems. Lastly, Elasticsearch is a search engine based on the open-source Lucene library. It is designed to be scalable, flexible, and easy to use, and is often used to index, search, and analyze large volumes of data quickly and in near real-time. Elasticsearch is implemented using a distributed architecture, which allows it to scale horizontally across a large number of servers. It is designed to handle a wide range of data types and formats, and can be easily integrated with other systems and tools.

[475] Version control systems are software tools that allow users to track and manage changes to files, typically in the context of software development. They allow developers to collaborate on code and keep track of different versions of files, making it easier to identify and resolve conflicts, roll back changes, and maintain a history of the codebase. Other popular solutions in this regard are Git, Microsoft Team Foundation Server (TFS) or Mercurial.

[476] Payment collection systems are designed to collect the payment on behalf of the company. In most of the relationships, payment systems are treated as separate data controllers, and contrary to the other vendors listed,

The above-listed software constitutes only a bare minimum of services used to deliver SaaS to the customer. What is not included is all the customer care systems, such as ChrunZero, Intercom or LiveChat, along with analytics tools such as FullStory, Google Analytis, or even marketing software such as MailChimp.

Based on the above-listed types of software necessary to build a SaaS product, it remains important to contrast this against the GDPR challenges. In previous parts of this thesis, it was discussed that the controller remains in a position of responsibility for the data processing and selection of the processors. Consequently, it is right to treat the majority of vendors as processors and intuitively assign the responsibility for such vendors to the data controller. To clarify the implementation challenge of the requirements as posted by the GDPR, one may need to analyze the statements of the Data Processing Agreements of the listed examples of vendors to name the possibility of ongoing data transfer that the controller in fact cannot limit or affect. As a consequence of the fact that all software intermediaries need support from third-party vendors, the practical possibility of excluding data transfer outside of the EU remains only a wish. To provide further support for such a statement, one may review the privacy policies of leading market solutions from the list enclosed above.

According to Atlassian terms of service that applied to Jira[477]:

> *International transfers within the Atlassian Companies: To facilitate our global operations, we transfer information globally and allow access to that information from countries in which the Atlassian owned or operated companies have operations for the purposes described in this policy. These countries may not have equivalent privacy and data protection laws to the laws of many of the countries where our customers and users are based. When we share information about you within and among Atlassian corporate affiliates, we make use of standard contractual data protection clauses, which have been approved by the European Commission to safeguard the transfer of information we collect from the European Economic Area, the United Kingdom (the "UK"), and Switzerland.*
>
> and
>
> *International transfers to third parties: Some of the third parties described in this privacy policy, which provide services to us under contract, are based in other*

they are acting on a set of data that is not fully accessible to the SaaS provider (credit card numbers). Among others, important providers of payment systems include Stripe, Square, Braintree, or Amazon Payments.

[477] Jira is one of the most recognized products of the company Atlassian. Atlassian is a publicly traded company, and as of 2021, it has a market capitalization of over $50 billion. The company is headquartered in Sydney, Australia, and has offices around the world. In addition to its core products, Atlassian also offers a range of services, including consulting, training, and support.

> *countries that may not have equivalent privacy and data protection laws to the country in which you reside. When we share information of customers in the European Economic Area, the UK, or Switzerland, we make use of the European Commission-approved standard contractual data protection clauses, binding corporate rules for transfers to data processors, or other appropriate legal mechanisms to safeguard the transfer.*[478]

In both sections of Atlassian's Privacy Policy, there is a clear statement of onward data transfer. The privacy policy constitutes an integral part of the agreement between the customer and the company. As a consequence, it becomes binding upon the use of the application, and the application is, as in the case of all SaaS products, delivered as-is. From there, customers of Atlassian, who in the vast majority of cases stand as data controllers, have to per se accept the transfer of personal data outside of the EU. At this point, it remains crucial to highlight the total market share currently enjoyed by Atlassian, which was previously quoted, and the fact that Jira, along with other Atlassian flag products such as Confluence, remains one of the most recognized software products in its category.

A similar approach has been taken by the other SaaS providers in the same product category as Asana, that in its Privacy Policy directly states:

> *When you use our products and services, information about you will be transferred to the United States where the majority of Asana's data processing occurs. We may also transfer information that we collect about you to third party processors across borders from your country or jurisdiction to other countries or jurisdictions around the world. Asana uses appropriate technical and operational safeguards for cross-border transfers of personal data collected in the European Economic Area (EEA), United Kingdom, Switzerland, and Japan as required by applicable local law, including the Standard Contractual Clauses*[479].

The approach presented by Asana remains coherent with the approach taken by Atlassian – the onward transfer is natural to those companies, and there is no technical or organizational possibility to exclude it.

To prove that the approach becomes a market standard, the next important market player, in another segment, that shall be taken into account, is Salesforce. Salesforce is one of the world's leading CRMs, and in the Privacy Policy, which, as always, constitutes a binding element of

[478] *Atlassian Privacy Policy*. Retrieved December 30, 2022 from https://www.atlassian.com/legal/privacy-policy#how-we-transfer-information-we-collect-internationally.

[479] *Asana Privacy Policy*, Retrieved December 30, 2022 from https://asana.com/terms#privacy-statement.

the agreement between the customer and the company, it states: how does Salesforce legalize, and also help its customers legalize, transfers of personal data outside of Europe?

> *In Europe, the "appropriate safeguards" that permit cross-border data transfers include the following transfer mechanisms: ○ Binding Corporate Rules for processors ("BCRs"): these are company-specific, group-wide data protection policies approved by data protection authorities to facilitate international transfers of personal data from Europe to organisations that are located in third countries that have not been deemed adequate by the relevant regulators. For more information, see "What are BCRs?" below. ○ Standard Contractual Clauses ("SCCs"): legal contracts entered into between contracting parties who are transferring personal data to third countries. The most recent set of SCCs are those pursuant to Regulation 2016/679 and were released in 2021 ("2021 SCCs"). For more information, see "What are the Standard Contractual Clauses?" below. Salesforce is in the unique position of being able to offer these transfer mechanisms to its customers, each of which is, by itself, sufficient to legalize transfers of personal data outside of Europe. Salesforce has both the BCRs and the 2021 SCCs incorporated into its Data Processing Addendum ("DPA")*[480].

The language selected by Salesforce differs from the formulation used by both Asana and Atlassian, and yet it leads one to a similar conclusion, namely, that the onward transfer is unavoidable. Due to the size of the company, the mechanisms for binding corporate rules differ, but the nature of processing with a necessity to transfer remains the same.

Lastly, once evaluating the MongoDB Privacy Policy, one can end up with a similar conclusion, as this agreement states as follows:

> *Your personal information may be transferred and stored in countries outside the EU, that are subject to different standards of data protection. MongoDB will take appropriate steps to ensure that transfers of personal information are in accordance with applicable law and carefully managed to protect your privacy rights and interests, including through the use of standard contractual clauses. Additionally, MongoDB uses a limited number of third-party service providers to assist us in providing our services to customers. These third parties may access, process, or store Personal Data in the course of providing their services. MongoDB obtains contractual commitments from them to protect your Personal Data.*[481]

---

[480] *Salesforce Data Transfer Mechanisms Policy*. Retrieved December 30, 2022 from https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-transfer-mechanisms-FAQ.pdf.

[481] *MongoDB Privacy Policy*. Retrieved December 30, 2022 from https://www.mongodb.com/legal/privacy-policy.

By analyzing the last quoted privacy policy, one may arrive at the conclusion that the information about the lack of possibility to exclude personal data transfer to third-party countries remains a market standard. Having that in mind, it remains important to come back to previously discussed requirements of data transfer under EU law. Under the GDPR, personal data can only be transferred to a country or territory outside of the EU/EEA if that country or territory ensures an adequate level of data protection[482]. The European Commission has determined that certain countries, such as Canada and Switzerland, provide an adequate level of data protection, and personal data can be transferred to these countries without additional safeguards. If a country or territory has not been determined by the European Commission to provide an adequate level of data protection, personal data can still be transferred if the company transferring the data has put in place appropriate safeguards, such as standard data protection clauses adopted by the European Commission, binding corporate rules, or approved codes of conduct.

Additionally, personal data can be transferred to countries outside of the EU/European Economic Area if the data subject has given explicit consent to the transfer, if the transfer is necessary for the performance of a contract between the data subject and the data controller, or for the implementation of pre-contractual measures taken at the data subject's request.[483] In fact, the GDPR poses an essential challenge from a purely logical and practical perspective. The act mentions the relation between the data subject and data controllers as a relation where the data controller shall ensure that the obligation towards informed consent has been met while at the same time taking up full responsibility for data processing. At the same time, as we have seen, the practical impact of data controllers on the practices of other market vendors is limited, especially when it comes to data transfer. Let’s imagine a simplified and artificial situation where, as a SaaS product delivery company, we use MongoDB as a database provider.

[482] The European Commission has the authority to determine whether a country or territory provides an adequate level of data protection. If a country or territory is determined to provide an adequate level of data protection, personal data can be transferred to that country or territory without the need for additional safeguards. As of 2021, the following countries and territories have received an adequacy decision from the European Commission: Andorra, Argentina, Canada (commercial organizations), the Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland. It is worth noting that adequacy decisions are reviewed periodically and can be withdrawn if the European Commission determines that the level of data protection in the country or territory has changed.

[483] Furthermore, the performance of a contract may not be made dependent upon consent to process further personal data, which is not needed for the performance of that contract.

From a purely practical perspective, in a computer system, a database is a structured collection of data that is stored and organized in a specific way, typically in order to facilitate retrieval, insertion, modification, and deletion of the data. Databases are used to store and manage a wide range of data, including text, numbers, images, and other types of data. The role of a database in a system can vary depending on the specific system and the needs of the users. Some common roles of databases in systems include: (1) storing and organizing data: databases are used to store and organize data in a structured way, which makes it easier to access and manipulate the data. (2) Facilitating data retrieval: databases are designed to allow users to retrieve specific data quickly and efficiently, using a variety of search and filter criteria, (3) ensuring data integrity: databases often include mechanisms to ensure the integrity of the data, such as constraints and triggers, which can help prevent data corruption or inconsistencies, (4) enabling data analysis: databases can be used to perform complex data analysis and generate reports, providing insights and business intelligence to users and (5) Enhancing security: databases can include various security measures, such as access controls and encryption, to protect the data from unauthorized access or tampering. Overall, the role of a database in a system is to store and manage data in a structured and efficient way, provide a range of capabilities to users, and support a wide range of applications and business processes. The importance of the database and, at the same time, the difficulty of any changes that may arise in this regard depend on the software architecture[484]. For database-centric systems there is a technological need to rely on the predefined solutions to preexisting challenges due to limited capacity to interfere with the database architecture or excessive cost and effort toward such an

[484] For example, the meaning and difficulty arising from any change to database-centric software remain key elements that define the possibility of the company to change the model of work. Database-centric software is software that is designed to work closely with a database management system (DBMS) and relies on a database to store and manage data. Database-centric software typically includes features and functions that allow users to interact with a database, such as the ability to create, read, update, and delete data in the database. Examples of database-centric software include database management systems, database development tools, and database-powered applications. Database management systems are software programs that are designed to create, manage, and maintain a database. These systems provide a range of features and functions for managing and manipulating data, including data modeling, data storage, and data access. Database development tools are software programs that are used to design, implement, and maintain a database. These tools often include features such as database design and modeling tools, data migration tools, and database management tools. Database-powered applications are software programs that use a database to store and manage data. These applications often rely on a database to function and may include features such as data input, data retrieval, and data analysis.

activity.[485] On the other hand, using the information-centric database model brings distinct yet relevant technical challenges.[486] In both cases, the possibility of transferring one database management system to another requires a rebuild of the application. Consequently, there is no possibility to customize the use of core providers as database management systems, payment intermediaries, or other core providers in a narrow timeframe. To fully navigate through the challenge of personal data management in software companies, there were attempts to provide a comprehensive framework that was supposed to support the application of processing standards. As an example, the Data Protection and Cloud Computing Framework may be mentioned. The framework aims to navigate through a number of obligations that rely on the controllers while processing personal data and using typical solutions necessary to deliver software. It goes beyond the very generic terms such as *privacy by design* or *privacy by default*.

[485] G. Phillips-Wren, N. Ichalkaranje, L. Jain, *Intelligent Decision Making: An AI-Based Approach*, Studies in Computational Intelligence, Berlin 2008, p. 61.

[486] An information-centric database model is a type of database model that is designed to store and manage data in a way that reflects the relationships and connections between different pieces of information. This model is based on the idea that data is interconnected and that the relationships between data are as important as the data itself. In an information-centric database model, data is organized into logical groups called "information models," which are used to represent the structure and relationships between different pieces of data. Information models are typically hierarchical in nature, with data at the top level representing the most general concepts and data at lower levels representing more specific concepts. One of the key features of an information-centric database model is that it is designed to be flexible and adaptable, allowing data to be added or removed as needed without requiring significant changes to the underlying database structure. This makes it well-suited for managing large, complex datasets that may change over time. Information-centric database models are often used in applications that require the ability to store and manage large amounts of interconnected data, such as knowledge management systems, data warehouses, and business intelligence systems.

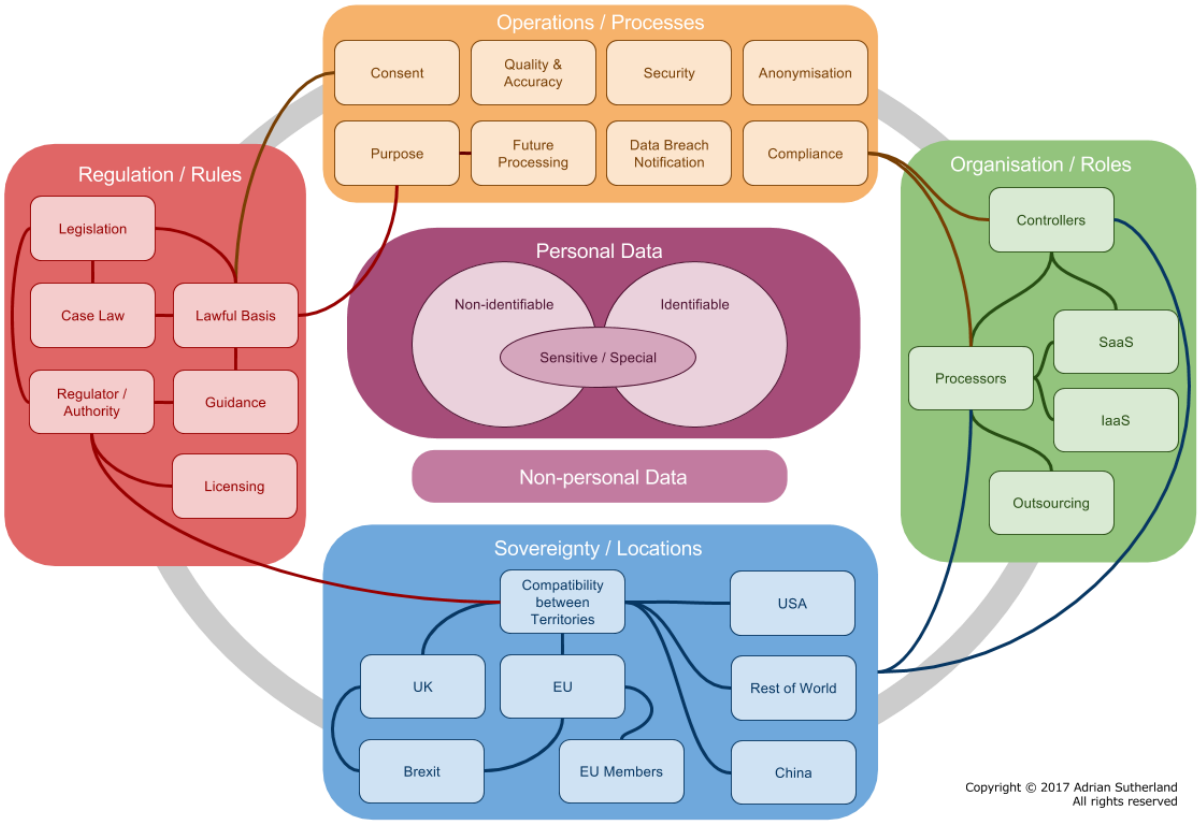


Figure 3: *Data Protection and Cloud Computing Framework*[487].

The presented flowchart depicts that the initial division of personal data focuses on personally identifiable information and non-identifiable information, further narrowing down the scope of sensitive/special categories of personal data. While focusing on personal data as the centric element of data architecture, the controller shall consider the matter of operations taken on the particular data set and its further compliance with the applicable data protection laws. In such a determination, the data controller shall take into account the role that it has under the organizational standards, namely, if the entity serves as a data controller or processor, and if it serves as a processor, is there any further outsourcing process? All of the above has to be viewed in the light of data processing location, namely compatibility of laws across countries, including vastly different requirements in the EU, US, or China, and taking into account changes in local contexts such as Brexit. Lastly, the controller has to evaluate the applicable standards that shape the reality of processing activities and, among others, define the basis for personal data processing and risk evaluation. As presented by the example framework, a real assessment of the impact of data processing and the scope of such activities is extensive and,

[487] *Data Protection and Cloud Computing Framework*. Retrieved March 24, 2023 from http://architectureportal.org/data-protection-and-cloud-computing-framework.

even though framework as the above-presented ones exist across technical practice, there is no guarantee or confirmation that any selected framework would meet the requirements of the GDPR. Consequently, the main use of available frameworks is to depict the complexity and scope of responsibility of the controller, especially while transferring the data to jurisdictions not covered by the adequacy decision.

At the same time, the GDPR focuses on the possibility for data subjects to immediately receive a remedy for data processing and the data controller to take full responsibility for the actions taken on the data subjects' data. As a consequence, the practical situation with which the data controller is dealing, taking into account the following analysis, is as follows:

- A data controller accepts full responsibility for the processing of the data subject's personal data;
- A data controller, from a practical standpoint, is unable to process personal information or deliver the product without external vendors;
- A data controller shall be responsive to requests from data subjects to affect data transfer.

The above-presented assumptions exclude one another to some extent. From a purely practical perspective, GDPR requires from data controllers a level of control that is impossible from a practical perspective. The previously described limitation on data transfer to the US further expands the stalemate that data controllers are in as the vast majority of software, including SaaS products, transfers data to the US based on the employed processors or sub-processors. The lack of a successor to the Privacy Shield and the uncertainty of Standard Contractual Clauses as a guarantee make GDPR a challenging piece of legislation to implement, mostly because of the uncertainty because there is no successor of the Privacy Shield.

2. Technical limitations to the execution of the right to be forgotten.

It remains impossible to obey the law that does not meet the criterions of the quality of law as discussed by L.L. Fuller[488]. This statement suggests that the law will be deemed to be in effect so long as it is consistent with what Fuller considers to be morality. No matter how Fuller

[488] L. L. Fuller, *op.cit.* p. 33.

defines morality, the message still feels very relevant to today's problems. Any type of legal act that is too foreign from practice is exposed to fail when it comes to the practical implementation. Fuller or Llewellyn observed the question of the quality of the law. From a purely practical perspective, the law has never encountered such a rapidly growing opponent as it has now. Lack of direct correspondence between law and practical implementation in the past was less visible than now, mostly because now one instant action may lead to mass data processing that may stand as a direct violation of law.

Unnerving interconnections between the government and corporations have been shown by recent discoveries of widespread data gathering and processing. As a result, the national bodies and big Internet and telecommunications companies have been the main targets of the movement for surveillance reform. The matrix of organizations that promote and carry out development and welfare around the world, however, poses major challenges to privacy and other civil liberties. One of the most strenuous elements and the crucial objection with regard to the technical challenges of the right to be forgotten v. technological practice is the definition of data itself. As one may currently assume, personal data is everything that leads to the identification of an individual. Starting from name and surname, across to email and phone number, and eventually arriving upon macID, IP address, or individual system verification token. The GDPR approaches the definition of personal data broadly. The GDPR defines personal data as *any information relating to an identified or identifiable natural person.*[489] This broad interpretation includes not only direct identifiers, such as names and addresses, but also indirect identifiers, such as location data, online identifiers (e.g. IP addresses), and even factors such as physical, physiological, genetic, mental, economic, or cultural identity. The European Court of Justice has also confirmed that dynamic IP addresses can constitute personal data under certain circumstances, further highlighting the expansive nature of the GDPR's definition of personal data.[490]

[489] GDPR, art. 4(1).

[490] The European Court of Justice (ECJ) ruled in *Patrick Breyer v. Germany* (C-582/14), a decision from 2016, that dynamic IP addresses might, under some conditions, be considered personal data. The court found that dynamic IP addresses, which change each time a user connects to the internet, can be considered personal data if the website operator holding the data has legal access to additional information that links the IP address to an identifiable individual. The case involved a challenge to the retention and use of IP addresses by the German Federal Government. This ruling highlight how broadly the GDPR interprets *personal data*, which includes both direct and indirect identifiers.

On the other hand, the Internet's architecture is mirrored in the data ecosystem. No one entity has control over or a comprehensive perspective on the information flow taking into account its complexity. The fact that data is tracked as it changes hands and contexts also implies that no one organization is responsible for data quality.[491] Data-driven companies such as Facebook, Google, Acxiom, and others are expanding their own data processing engines. They are making every attempt to ensure privacy and security while also keeping ownership of their most precious assets, namely personal data. They are not, however, held accountable for the ads that users choose to target on their platforms, or for the secondary uses of data that occur after it leaves their domain[492]. Consequently, the scope of the right to be forgotten gains more potential areas to be controlled than the legislator may initially assume.

From a purely practical perspective, the execution of the right to be forgotten is mostly about data removal. Consequently, from a technical perspective, the question of the right to be forgotten usually implies the ability to remove the data from the service provider's data storage or the layer of the business logic that functions as a separate element. Of course, the construction of the database and its technical logistics differ when it comes to database-centric software or domain-driven architecture.[493] A typical role of a database in a system can be traced back to a few core elements that are further important from the perspective of the practical performance of the right to be forgotten.

- Data storage: The database stores data in an organized manner that makes it easy to retrieve data upon request. A database has its own architecture that determines the scope of processing that is performed in the area of data and that further affects the flexibility of operations performed on it.
- Data retrieval: The database allows users to quickly access the data they need without having to search through large amounts of unorganized data. Depending on the type of database and use case, the main objective of the database's existence is to enable fast, cheap, and efficient access to information at the granularity level expected by the user.

[491] U. Gasser, J. Zittrain, R. Faris, R. Heacock Jones, *Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse*, Berkman Center Research Publication 2014, no. 2014-17, pp. 70-71, 20. Retrieved March 11, 2023 from https://cyber.harvard.edu/publications/2014/reflections_on_the_digital_world.

[492] *Ibid.*

[493] C. Babers, *Architecture Sourcebook Vol.2: Data Centric Architectures*, Morrisville 2007, pp. 8-10.

- Data manipulation: The database allows users to add, modify, and delete data upon request. From the perspective of the GDPR, data manipulation constitutes a necessary element for the performance of the right to correct personal information.
- Data security: The database ensures that data is secure and protected from unauthorized access or modification due to storage in isolated infrastructure. Data security enshrined in the database may further create some obstacles for data modification and potential removal.
- Data integrity: The database ensures that data is accurate and consistent, by enforcing data constraints and data validation rules.
- Data backup and recovery: The database provides mechanisms for backing up data, so that in the event of a system failure, data can be restored to a previous state. Consequently, the database is the central element of every disaster recovery process and a vital element of risk assessment.
- Data sharing: The database can be shared by multiple users and applications, allowing for collaboration and integration of data across different systems.

Based on the above, generic explanations of the functionalities of databases, it remains crucial to understand that the right to be forgotten in a practical dimension cannot be analyzed without a practical assessment of how to perform or execute the removal of data affecting or implementing the aforementioned right. While performing the right to be forgotten, understood as the removal of data, the data controller has to be aware of the risks that must be balanced against the performance of such a right, which may in fact affect the rights of other data subjects having personal data processed by the same storage unit.

First of all, it's crucial to mention the atomicity of data. Atomicity describes a set of operations as being performed either entirely or not at all. For example, when inserting a data record, the entire record must be added; adding only half of the record is unacceptable[494]. The same is true for adding or removing entire sets of records. This is particularly intriguing when it comes to database crashes that occur in the middle of use; in these cases, methods must be in place to undo the incomplete transactions and return to a previous state. *Rollback* is the term used for this type of operation. The next challenge to be faced by the data controllers with regard to the performance of the right to be forgotten while executing data removal is *consistency*. The

[494] B. Kemme, R. Jiménez-Peris, M. Patiño-Martínez, *Database Replication*, Waterloo 2010, pp. 9-13.

database needs to be in a consistent state, again, after an operation, which calls for normalizing it and making sure all relations in the database structure are clear and well-maintained.

The next element of the database architecture to be taken into account refers to the isolation of data. In the case of parallel transactions, the database must ensure that they do not interfere with each other. This is typically done via *locking*, i.e., the data to be changed is marked as locked and cannot be touched by other operations until the first operation is finished. The expectation is to properly isolate subsets of data to ensure higher durability for potential data loss or infringement.[495]

With regard to data consistency while operating on data removal, the consistency remains important to durability of the data storage. Data must be kept in the database continuously, especially in the event of server or system failure. Data loss or inconsistent results must be avoided, especially during crashes. This requirement is often met by mechanisms like transaction logs.

Following them, databases are said to be ACID-compliant[496]. All significant databases in use today are ACID-compliant. Yet, in order to create a functional environment, users of databases often require the database to include extra functions. Core elements of the ACID framework further imply that the next element of database maintenance and management must be implemented in order to ensure data safety and consistency[497].

Furthermore, to better understand the clash between the technology and how it operates in practice within the context of the requirements of the GDPR, the primary technique of deletion must be investigated, leaving the question of internal mechanisms aside since it is always debatable whether complying with the GDPR entails keeping the deleted information safe against retrieval in prominent forensic investigations focusing on unstable internal mechanisms.[498] In fact, when a record is deleted using the (SQL) interface, it is just marked as deleted and removed from the search indexes, not replaced with other data, or having its

[495] D. Feng, *Data Deduplication for High Performance Storage Sy*stem, Wuhan, 2022, pp. 83-84.

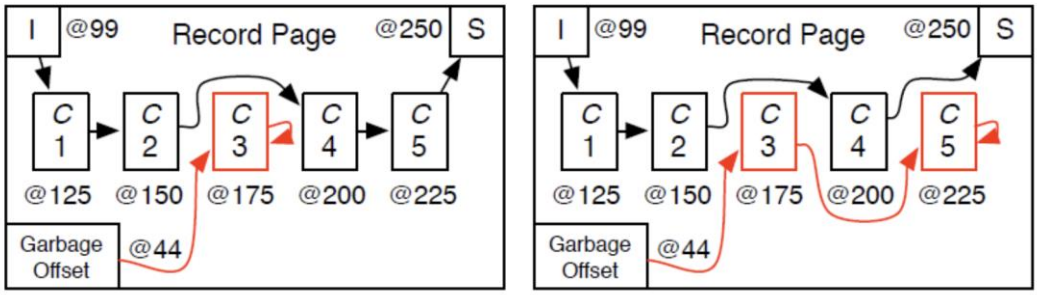
[496] ACID is an acronym that stands for Atomicity, Consistency, Isolation, and Durability. These are the four key properties that ensure the reliability and consistency of transactions in a database.

[497] The mentioned additional elements to be taken into account while drafting the scope of technological challenges for the right to be forgotten include intended rollbacks, audits and control sets, replication and backup management.

[498] T. Li, E.F. Villaronga, P. Kieseberg, *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, *op.cit.*, p. 10.

occupied space filled with zeros or the like. This brings up performance concerns again; in reality, removing and overwriting space would require a significant amount of additional work and have a negative influence on speed (it would mean that a delete request would be more expensive than numerous data insertions). The matter of removing the data after it is marked as deleted is one of the biggest implementation challenges for personal data storage vs. the right to be forgotten. In fact, it seems to be the most natural and obvious interpretation of the requirements by the European Court of Justice to remove such data or data indexes from any potentially owned resources, while at the same time, the removal of personal data struggles with a different practice that is safer from the perspective of data controllers and still more affordable.

To further explain the matter, the below included illustration shall serve as an example:



(a) One deleted record (b) Two deleted record

***Figure 4**: Deletion of a data set from the MySQL database type. Example mirrors the "mark as deleted" instead of physical deletion of data*[499].

The above-presented example guides one through the process of marking datasets as deleted instead of the functional deletion of data as such. Element (a) of Figure 4 depicts the database's condition just before deletion. While the majority of the image is provided for correctness, the five data records located in places C1 through C5, as well as the beginning (I) and ending (S) of this section of the database, are crucial for the deletion. The picture also displays a single deleted record at C3 that is connected by the so-called *Garbage Offset* a group of deleted and now vacant spaces. This graphic only displays a portion of the search tree, or what is known as a *page* in order to simplify complexity. When a database searches for information, it finds the

[499] P. Fruhwirt, P. Kieseberg, E. Weippl. *Using internal MySQL/InnoDB B-tree index navigation for data hiding*, [In:] *Advances in Digital Forensics XI: 11th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 26-28, 2015*, G. Peterson, S. Shenoi (Eds.), Cham 2015, pp. 179-194.

page inside the search tree where the required data must be located. It begins at node I inside the page and moves down the arrowed path until it finds the needed information. The data was not found if the search returns to node S with no results. In our example, the task is to delete the data kept in C5. The database explores the tree until it finds C5 and looks for the data in C5. It has been *marked for deletion* at this time. The physical operation of data removal in this case does not refer to the permanent extraction of data but to the change of its location. At the same time, the presented scheme is, among others due to ACID requirements, one of the most widely recognized and applied.

For a variety of reasons, data controllers may opt to label data as *erased* rather than actually deleting it. They could need to preserve a record of the data for legal or regulatory reasons, which is a frequent justification. They might occasionally also want to keep the data for commercial or historical purposes. Yet, the data controllers may also run into problems if they maintain the data designated as removed but do not actually remove it. Data breaches or unauthorized access to erased data are two serious risks. Even though the data has been declared erased, it may still be accessible to hackers or other bad actors who can access it by abusing system flaws. Data inconsistency is another issue. Data backups may still contain deleted data if it is not physically removed, which could result in inconsistent data when the backup is restored. This could lead to issues with data analysis, decision-making, and compliance with data protection laws.

Keeping deleted data, including personal data that has been flagged, might also cause storage and management problems because the data takes up space in the system and is still present. Costs associated with managing and storing data may rise as a result. Overall, data controllers should carefully consider the risks and benefits of marking data as deleted but not physically removing it. They should weigh the potential legal and business benefits of retaining the data against the risks of data breaches, data inconsistency, and storage challenges. If they decide to keep the data marked as deleted, they should ensure that appropriate security measures are in place to protect the data against and otherwise prevent unauthorized access. At the same time, the existence of a practice that stands apart from the pure legal requirements shows that the implementation of the right to be forgotten in its straight-forward form may not only cause other risks for data subjects that are stored in the same infrastructure but also become an

expensive and advanced technological challenge to be faced by data controllers often lacking in specifically defined responsibility and/or authority to carry out the same.[500]

3. Challenges for data controllers in light of the growing popularization of artificial intelligence models.

Even though data processing remains one of the most modern challenges of legal practice with regard to data processing, it is extremely difficult to avoid the feeling that with the popularization of artificial intelligence, the question of *standard* data processing has become or is quickly becoming outdated. Starting in 2016, one has been witnessing the AI-popularization revolution. The question of the adequacy of legal conventionalism in this regard (and why it fails) seems to be the right one to ask. The term *legal conventionalism* refers to a group of much debated legal theories that use the *conventional rule of recognition* to explain the existence of law. Some of them strive to be *fully fledged theories of law* and use the same fundamental, accepted fact to explain how laws are normative.[501] Ultimately, the fundamental criticisms can be framed in terms of the dichotomy between substantial and instrumental reason.[502] Similar to the previously discussed theories of Pound and Holmes, in every area of law, the potential for addressing social needs remains vital from the perspective of the real quality of law. At the same time, the question of the foreseeability of the law remains one of the most important requirements and challenges for data controllers, at least from the perspective of day-to-day operations. Consequently, the fact that language models are

[500] At this point, it is worth underlining that data controllers are obliged by law to maintain backups, as under the requirements of the GDPR, they have to ensure data consistency and clarity. They should also employ all necessary security measures and control means to ensure data consistency and availability. For that reason, every data controller provides a backup infrastructure for the data, including personal data. Backups are kept by data controllers for a variety of reasons. Disaster recovery is one of the key factors. Backups offer a way to retrieve data in the event of a disaster, such as a hardware failure, natural catastrophe, or cyberattack. Businesses can restart operations and reduce downtime by using backups to restore data if the original data is lost or corrupted. To maintain business continuity is another justification. Even in the event of an unanticipated loss or downtime, backups can assist in ensuring that crucial data and apps are always accessible. This aids businesses in maintaining operations, keeping consumers happy, and preventing any harm to their reputation.

[501] A. Dyrda, *Why legal conventionalism fails?*, Archiwum Filozofii Prawa I Filozofii Społecznej 2015, no. 1(10). Retrieved April 30, 2023 from https://doi.org/10.36280/AFPiFS.2015.1.14, pp. 14-15.

[502] As J. Coleman (and J. Dickson after him) point out, it is typical of modern legal positivists that they all acknowledge that the standards of legality are traditional. Such an understanding of the "practice theory of rules," which is the Hartian account of social rules, as the customary nature of the ultimate rule of recognition, is inextricably linked.

becoming ever more popular supports the reality that data controllers are facing new and not properly vetted laws and regulations requiring the data controllers responsible implementation.

From a practical perspective, standards for data processing as defined by the GDPR are newly created. Yet, in 2022, a careful observer may find the outbreak of the language model revolution with the possibility to process data, including personal data, on a scale that hasn't been known before and what made know GDPR rules already outdated when it comes to the clash with new technologies. Neural networks, rule-based systems, fuzzy logic, machine learning, expert systems, adaptive systems, genetic algorithms, multi-agent systems, etc. are some of the several methods used to create AI-based solutions. All of these methods aim to create models that can deal with complex systems that sequential algorithms cannot (or do not know how to) handle. These challenges could be brought on by the difficulty of modeling a behavior that depends on a number of factors, dealing with nonlinear interactions (impossible to achieve using linear methods), and even changing over time. Machine learning is one of the AI disciplines that has seen the most success in business applications. It creates prediction models by analyzing an original collection of data, seeing or sensing patterns, and modeling links between the variables. The last of the listed techniques is responsible for the currently popularized AI-based chat models.

Undoubtedly, the turning point in AI processing and the general accessibility of AI technology to the public came with the release of ChatGPT. The development of ChatGPT is an element of OpenAI's bigger family of GPT (generative pre-trained transformer) models. The first model in the GPT model family, known as GPT-1, was initially introduced by OpenAI in 2017. This model learned to generate text by identifying patterns and structures in the data, without any explicit instructions or supervision, throughout the unsupervised learning process that it underwent to train on a sizable corpus of text data. An improved version of the GPT model known as GPT-2, which was trained on an even larger dataset and had substantially higher performance than its forerunner, was made available by OpenAI in June 2018. GPT-2 gained notoriety for its remarkable capacity to produce writings that appear human, raising questions about how such technology might be abused. 2020 saw the release of GPT-3, the largest and most sophisticated model in the GPT series to date GPT-3 has 175 billion parameters and was trained on a massive dataset of over 45 terabytes of text data. It is possible to employ ChatGPT, a GPT-3 variation, in chatbot applications since it has been expressly taught to produce human-like responses to conversational queries. The core architecture of ChatGPT is identical to that

of GPT-3, but it has been tweaked using a particular set of data to enhance conversational capabilities. What is more, further developments in this regard are planned by OpenAI. From a technical perspective, artificial intelligence models may require the interception of personal data at the following stages:

- Training: Personal data may be utilized in the building of an AI model, such as one based on machine learning (ML). In other circumstances, such as with a training system built on gathering knowledge from an expert, it can be thought that no personal data processing activities are being done. When processing personal data is necessary for the training stage, that processing is regarded as personal data processing in and of itself.[503]
- Validation: When employing information that reflects the real present state of a processing activity to assess the suitability of the experimental model, this stage may involve processing personal data. If present and if employing personal data, this dataset could be distinct from those used in the training phase, and it might even be performed by a third party for model certification or auditing purposes. This stage may also be further completed by other analytical methods.
- Deployment: in case the AI-based solution becomes effectively used for a broader audience, then it may re-process personal data upon its deployment.
- Operation: it is possible that AI models may require access to, modification of, and further operation on personal data in order to remove them, while such models interfere with the user to deliver the requested result or to perform any decision making process.

It is important to remember that not all AI-based solutions process personal data throughout their life cycles or base all of their choices on automated processing that affect real people.[504] Because of the popularization of the AI technologies, the European Parliament urged the Commission in Resolution 2017 to investigate, analyze, and take into account the potential effects of legal solutions, particularly those that might eventually provide robots with a distinct

[503] Agencia Española de Protección de Datos, GDPR compliance of processings that embed Artificial Intelligence An introduction, 2020. pp. 12-13. Retrieved April 30, 2023 from https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf.

[504] There could be significant legal repercussions if decision-making in a financial environment is based on AI as for example liability for automated decision making issued by the AI.

legal status[505]. It is important to remember that from a European legal perspective, one operates within the regime of Article 2 TFEU and in the Charter of Fundamental Rights, such as human dignity, equality, justice, and equity, non-discrimination, informed consent, private and family life, and data protection; it should also be based on other underlying principles and values of EU law, such as non-stigmatization, transparency, autonomy, individual responsibility, and social responsibility, and on existing ethical practices and codes. At the same time, we operate under the regime of Article 6 of the GDPR, where some direct rights stand for the protection of the right to privacy of individuals, is binding upon all EU member states. Resolution 2017 aspiring to address early notions of AI use required the protection of the safety, health, and security of human beings, as well as their freedom, privacy, and integrity, which remains consistent with both previously legislated Article 2 of the TFEU and prior GDPR. Even though, the act has also recommended some technical means for realizing these general principles, such as robot registers, compensation funds, individual registration numbers for robots, and compulsory insurance, the European Commission admits that there is no relevant legislation that may serve the process of popularizing AI use.[506]

These approaches would at the very least give the most advanced autonomous robots the status of electronic persons responsible for repairing any harm they may cause, and they might even apply electronic personalities to situations in which robots interact with third parties independently or make autonomous decisions.[507] At the same time, the question of the status of AI in data processing and how it fits within modern processing activities remains inevitable. The popularization of AI means that the processing conducted by the centralized language models will become present in daily activities, starting with household appliances to every-day software. The fundamentals remain the same: Internet of Things technologies considerably

[505] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), point 59(f).

[506] *Commission Staff Working Document Impact Assessment, Accompanying The Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts 21.4.2021 SWD(2021) 84 final*, Brussels, p. 5. Retrieved April 30, 2023 from .https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence.

[507] It is worth noticing that Regulation 2017 is purposiveli limited to intelligent robots what implies at one side self-consciousness and ability to take up decisions and at the same time at least minimum of physical support what leads to the conclusion that relation between the AI as is understood now and intelligent robots remain unclear.

increase and facilitate the possibilities of gathering personal data, but the legal framework in this area is unchanged. Simply using a smart system does not give the user more freedom than using more conventional methods; rather, because the system can more quickly and effectively collect personal information, the user comes under more pressure than ever to make sure that their actions are legal and in accordance with those individuals' rights, particularly their right to privacy[508].

It remains important to highlight two elements that shape the impact on data processing with regard to artificial intelligence: the aspiration to control the reasoning of AI by individuals; and the functioning of the AI model once it becomes personalized. For that reason, from the very early stage, the European approach towards AI in all dimensions of law was to fit this new technology into already known, existing legal canons of law. In this regard, the European Data Protection Supervisory (EDPS) emphasizes the significance of a future convention fully respecting the EU acquis in the area of personal data protection given that data, including personal data, are frequently the fundamental predicate for autonomous decisions that will inevitably affect individuals' lives at various levels[509]. The EDPS acknowledges that the convention's scope and the proposed AI Act's overlap, as stated in Directives (6) and (12), and it supports the Commission's goal to ensure that the convention is in line with the proposed AI Act while also taking into account future developments in the legislative process[510].

The growing use of AI in the field of software is a fact, and the processing of personal data by language models remains an inevitable element of this growth. At the same time, the problem of challenges posted by the AI processing of personal data has already been discussed in the literature and among others, including lack of privacy, misuse of personal data, security problems, lack of quality data, lack of accuracy of data, problems of integrity, lack of accountability and liability, lack of transparency, bias and discrimination, lack of accuracy of

[508] P. Księżak, S. Wojtczak, *Towards a Conceptual Network for the Private Law of Artificial Intelligence*, Cham 2023, p. 177.

[509] European Data Protection Supervisory, *Opinion 20/2022, Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence (AI), human rights, democracy and the rule of law ('the convention'), pursuant to Article 218 TFEU*, p. 8. Retrieved April 28, 2023 from https://edps.europa.eu/system/files/2022-10/22-10-13_edps-opinion-ai-human-rights-democracy-rule-of-law_en.pdf.

[510] *Ibid.*

predictive recommendations, and lack of accuracy of non-individual recommendations[511]. Having in mind these risks, it remains vital to bring any degree of transparency and reliability from AI actions into the light of law. Especially from the perspective of current data controllers who are struggling with the fact that language models are usually delivered by third-party vendors and at the same time constitute a complex system that processes personal data, it is challenging to agree to have the responsibility for such processing. As a consequence, the perspective of data controllers is that the use of language models will become a basic element of day-to-day operations. At the same time, it remains possible to question if the rise of popularized personal models will not create a new category of personal data, in particular, if the model based on personal actions will become a set of personal data. As it is already known, language models may be fed with data, behavior, or observations of one individual. In such circumstances, it is likely that the model itself will be considered personal data. The question of whether a customized AI, which functions as a kind of user's shadow (silhouette), qualifies as a unique legal good that is partially of a personal character, must be answered. It is crucial to understand that the issue at hand is not whether the AI would save any personally identifiable information on and/or of the user, but rather whether it might change how it is organized so that it becomes tailored to the user during interaction. It will make decisions based on a user's profile and preferences that are unique to them[512]. In such circumstances, it is possible to claim that trading in such AI should be governed by different legal regulations.

It should be noted that machines that aren't fully autonomous carry and mimic the user's intent since it's been written (programmed) into them. Regarding continued operation after the user's passing, specific issues arise in the case of autonomous AI, i.e., those that can replicate the user and learn to carry out the user's hypothetical will. In this situation, the user's hypothetical will refers to what he or she would likely want to do or would want to do if he or she gave it any thought. This is different from the *per se* expressed will of the person, and as a consequence, there is no current classification of such action on the grounds of personal data processing, including phenomena such as a valid consent statement that is vital part of the legal basis for

[511] B. C., Stahl, *Artificial intelligence for a better future: an ecosystem perspective on the ethics of AI and emerging digital technologies*, Cham .2021, p. 49. Retrieved April 30, 2023 from https://doi.org/10.1007/978-3-030- 69978-9.

[512] P. Księżak, S. Wojtczak, *op. cit.*, p. 186.

data processing[513]. Machines can act on behalf of a deceased person as if they were still alive, which raises an interesting question regarding personal data operations and the potential succession of such rights that arise from data processing that remains unknown from the perspective of current legal practice[514].

As pointed out above, the area of data processing by artificial intelligence models places new, unknown challenges on data controllers. At the same time, the approach of risk-balancing seems to be one of the most rarely used by European practice and further leaves data controllers with an unproportionate burden of responsibility for the processing activities while using providers that use AI, which becomes a market standard. It is important to mention that in the *Working Paper Laying down Harmonized ruled on Artificial Intelligence and Amending Certain Union Legislative Acts*, the person who uses an AI model to process personal data is directly pointed out as the person who decides about the scope and means of data processing (consequently acting as a data controller)[515]. Yet the working paper recognizes that the risks standing from the use of language models as AI may lead to the arbitrary use of algorithmic tools give unprecedented opportunities for indiscriminate or mass surveillance, profiling, and scoring of citizens. The fact that small and medium enterprises have no practical impact on processing by market leaders remains omitted almost fully by the research. It remains important to perceive responsibility for particular processing activities from the perspective of their real impact on the processing, popularization of AI makes the practical impact that controllers may have even smaller, with no further guidelines on the possible legal safeguards that are available for the controllers to ensure processing activities are in line with the GDPR but with no need to isolate from the market.

Undoubtedly, AI models that will imitate individuals and assist them in any actions, including those implying data processing, will place individuals in the position of data controllers [516].

---

[513] In simple terms, the question would be, if AI model can give a valid consent on behalf of individual or time withdraw it if the scenario of higher decisiveness of language models will be fulfilled.

[514] In fact, it remains important to remember that the potential AI model may imitate the will of individual and further likely comply with the initial will of the deceased at the same time leaving the question of potential validity of such decisions.

[515] *Commission Staff Working Document Impact Assessment…*, *op. cit.*, p. 6.

[516] It is also worth noticing that the model of individual may be understood and constitute a personal, biometric data. Any information relating to a physical or behavioral trait that can be used to identify a person is referred to as biometric data. Biometric information examples include iris scans, facial recognition, DNA, and fingerprints. Data obtained from a person's behavior, such as voice patterns, typing habits, and search history, may be included

Consequently, from the perspective of the GDPR, the use of AI solutions in day-to-day life by both individuals and enterprises may lead them to become data controllers, not necessarily with the full understanding that the processing of personal data happened. For example, tools that will support calendar organization or grocery shopping may lead to broader data processing that was not fully purposeful by the user (acting as a controller) but was a necessary condition for the AI model to fulfill certain actions. The question that the law shall be challenged with in the near future is how to treat the assistant service provider processing with the use of AI in such a setup. Looking intuitively towards the future from the standpoint of current experience, such AI personal assistants should be treated on par with the person for whom they work—as one legal entity. Following that, the legislator must establish a separate law to treat it not as a tool used by humans but as an integral part of their following. This concept strictly implies the inviolability that such an AI assistant and its actions may be treated collectively as the actions of the person who delivered the data or personal profile to the AI. Its examination (e.g., by law enforcement agencies) will have to be treated as questioning the person it serves (perhaps a new type of privilege, similar to that of a lawyer, may be necessary to cover the functioning of an AI assistant). At the same time, if actions of AI may be attributed to the person who uses it, then the concept strongly affects the currently existing concept of controller and further knows aspects of privacy. As an example, the model that imitates individual behaviors of a person shall be considered personal data, and as an outcome, in the case of execution of the right to be forgotten, such a model shall be erased, or partially erased, what may permanently impair the functioning of such a model. Furthermore, the aspect of data erasure may arise after the death of an individual, and in such circumstances, the question of the succession and after-death management of such a model arises as an unknown in the light of personal data processing.

Processing personal data by AI models opens up an extensive and unknown scope of data protection challenges, and it further places responsibility on data controllers that may become even more blurry than it is at the moment. Having that in mind, the question of the reliability of the law arises again.

in a personal AI model. A customised profile that can be used to identify the person may be constructed using these data points. The personal AI model could be viewed in this way as a type of biometric information.

D. Search for the impossible solution – lack of real possibility to exclude data transfer and to provide full execution of the right to be forgotten. Thoughts on the role of the law in the light of technological challenges.

Previous chapters directly referred to the day to day challenges of the data controller's role with regard to factual capability to control the process of the activities performed on data. As discussed above, both the transfer of personal data to a third-party country and the technical possibility to execute the right to be forgotten seem to be unavoidable elements of the day-to-day operation of companies related to new technologies, especially for online-operating software. Is there a solution that, on the one hand, guarantees an acceptable dose of accuracy and reliability for the controllers and, on the other, efficiently protects the rights of individuals? On the surface, such a rhetorical inquiry appears to be a search for the impossible, as those two desires appear to be diametrically opposed, at least to some extent. The issue of conflict between data subjects' rights and data controllers' rights, or rather, responsibilities, is a well-known legal dilemma. The GDPR places a lot of emphasis on concepts such as consent and legitimate interest, but in practice, both concepts do not evolve as quickly as practice, particularly with regard to technological contracts that are written in the same way for all customers and further postpone the issue of pre-trial or pre-acquisition [517]. The question of fiduciary duty has been present for a while in the world of technology and challenges the data controllers while balancing the rights of data subjects against their business interest[518]. As an example, according to the GDPR, data controllers must obey the limitation of purpose, data collected for purpose A shall never be used for purpose B without obtaining the consent of the

[517] *Data Governance in AI, FinTech and LegalTech Law and Regulation in the Financial Sector*, A. Darbellay, J. Lee (Eds.), Cheltenham 2022, p. 47.

[518] Fiduciary duty refers to the legal obligation that one person or entity has to act in the best interest of another person or entity. This duty arises when one party is in a position of trust, confidence, and responsibility for the other party. For example, a financial advisor has a fiduciary duty to act in the best interest of their clients when providing investment advice or managing their clients' assets. This means that the financial advisor must put their clients' interests ahead of their own and avoid any conflicts of interest that may harm their clients.

data subject again[519]. While such stands clear in theory, practice of data retention may differ[520]. Data retained in the database may be reused, from time to time, with lesser risk than removal and re-gaining of such data, even if, such approach goes against a direct requirement of the GDPR and, ironically, at the same time, is in favor of practical protection of an individual's rights once viewed from a practical perspective.

The GDPR offers a simple approach to balancing – it claims that the interest of the data subject must be balanced against certain risks, such as interference with data, illegitimate use. At the same time, GDPR leaves a massive scope of uncertainty for the controllers. In accordance with Article 35 of the GDPR, where there is a danger or a high chance of violating an individual's rights, it is mandatory to conduct a data protection impact assessment. Such an approach shall be taken both in the case of data processing in general and in the case of data transfer. In fact, according to the currently available knowledge of the DPIA requirement, every business using new technologies and operating in an online environment processes personal data to a degree that necessitates a risk assessment. With the implementation of the GDPR, data controllers' obligations and practical actions must be evaluated from the perspective of any real harm that a loss of processed data might do to the data subject while the data is being processed or transferred. It should be highlighted that just 14 nations outside of the EU member states were evaluated as complying with the requirements imposed by the GDPR, indicating that the level of security demanded by the European Commission is among the greatest in the world. There are no additional security precautions needed to reduce the danger of such a transfer when sending personal data to the nations covered by the so-called adequacy judgment. Transfer to any other region, however, necessitates the deployment of additional security measures. Any

[519] This ethical question of fiduciary duty was also discussed by Balkin who questioned the overuse of patients' data when such use in the favor of the development of knowledge and medicine. J. M. Balkin, *Information fiduciaries and the First Amendment*, U. C. Davis Law Review, 2016, vol. 49, p. 1183, and J. M. Balkin, *The fiduciary model of privacy*, Harvard Law Review Forum 2020, vol. 134, p. 11.

[520] Recital 39 of the GDPR reads as follows: *Any processing of personal data should be lawful and fair. 2It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed*.

other transfer issued by the data controller or data processor based on the territory of the EU will be further followed by an assessment of the risks associated with such a transfer. Since 2020, the adequacy decision has also covered the US, and the adequacy decision thereto is known as Privacy Shield. At that time, subjects that went through the right certification were assigned to the list of data subjects complying with the Privacy Shield requirements[521]. Such self-certification was treated as the equivalent of European standards, and as a consequence, data transfer to such organizations was justified on the grounds of Article 45 of the GDPR. Nevertheless, as the outcome of the Privacy Shield invalidation by Schrems II judgment[522], transferring personal data to the US requires additional measures that align with the requirements of Article 46 of the GDPR[523]. What is even more important, the court stated that the use of the most popular Standard Contractual Clauses as a mechanism may not be enough and shall be subjected to evaluation each time upon transfer. According to the CJEU, transferring personal data to a country not covered by the adequacy decision requires a balancing test each time to check for risks and mitigate them. Furthermore, neither Schrems II nor any other judgment or decision provided a list of universal criteria for the controllers to rely on. According to the ruling, the data controllers shall each time verify the practice and law applicable in the state where the personal data are being transferred[524]. As a consequence, the principle of accountability for the data controllers extends to the transfer and full responsibility of evaluation of foreign law and practice. It is further worth mentioning that the main focus of interpretation of the GDPR provided by the Schrems II and further interpretations of the EU Commission focuses on the effective execution of security for personal data. It seems more than obvious that none of the industries were prepared to manage the scope of requirements as drawn by the GDPR. Transferring personal data to the US has been one of the most frequently relied upon by data controllers, especially in the internet-operating software industry. It became

[521] Self-assessment for the Privacy Shield is still available. Retrieved March 24, 2023 from https://www.privacyshield.gov/PrivacyShield/ApplyNow.

[522] *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, Case C-311/18, *op.cit.*

[523] Article 46(1) of the GDPR states that: *In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available*.

[524] The main challenge regarding this high-level suggestion refers to the costs of such evaluation and sometimes practical difficulty requiring knowing the environment of not only foreign legal systems but also the practice present there.

obvious that data controllers and, in general, any entity transferring personal data shall need the merit-based support from the side of the EU to manage TIA. The hope was seen in the Recommendation 01/2020 which was further revised in 2021[525]. The recommendation focused on the main principles of the legality assessment; nevertheless, it clearly left the responsibility for the documentation and transfer impact assessment with the data exporter. According to the Recommendation there are six main steps of the assessment of processing activities, namely: mapping the processing activities, verification of the legality basis, assessment of the effectiveness of the tool used to transfer based on the analysis of the receiving state law and practice, definition and application of supplementary measures, procedural steps; and finally re-assessment[526]. Consequently, to begin with the controller must be aware of the transfer of personal data to the third country. In fact, even this simply and obvious element may bring some challenges when it comes to the realistic accountability because, in the case of software providers, especially those originating from the cloud environment, there is a challenge to the chain of providers necessary to deliver the software to the client. Consequently, the data controller, while appointing any data processor, shall take a deep dive not only into the practical use of the provider but also into the potential for further transfer. The next step requires defining the legal basis for such processing. In the case of a transfer that requires data processing outside of the European Economic Area with no adequacy decision, it remains within the scope of responsibility of the data controller to provide compliance with the requirements of Article 46 of the GDPR. It is further worth mentioning that all measures that are listed by Article 46 focus mostly on the formal, contractual safeguards and that they further limit their scope of application to the parties to the agreement; consequently, the data exporter has to evaluate the environment of the country where the data are being exported and supplement the measures. If the formal check of practice and law in a third country is completed positively (individuals can rely on the same set of rights as within the EU), the exporter may supplement the measures and proceed with the transfer. Lastly, the re-evaluation shall ensure that the durability of guarantees provided for particular transfers remains in place. Even though Recommendation 01/2020

[525] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021. Retrieved March 24, 2023 from https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[526] *Ibid.*, p. 10-23.

made some attempt to clarify the core element of TIA, the assessment of risks remains a limbo that each entity taking part in data processing must address themselves.

The recommendation provides beneficial advice on how to carry out a transfer effect assessment, but it has come under fire for not going into enough detail in this area. Particularly, several experts have pointed out that the guideline does not offer precise standards or a thorough framework for evaluating the risks connected with the transfer of personal data to foreign countries. One crucial step in the transfer impact evaluation process is evaluating the legal system in the third-party country where the transfer of personal data is taking place. Any transfer of personal data to a third country is required under the GDPR to be subject to sufficient controls that provide an adequate degree of data protection. This means that the third nation must have laws and regulations governing data protection that are identical to or comparable to those in the European Union. However, recommendation 01/2020 does not provide specific guidance on how to assess the legal framework in the third country. This means that any entity responsible for transferring personal data may be left alone with the challenge of determining whether the legal framework in the third country meets the appropriate safeguards required by the GDPR[527]. The lack of specific guidance in the recommendation can make it challenging for organizations to perform a transfer impact assessment that is fully compliant with the GDPR. As an effect, Recommendation 01/2020 left the controllers with the same dose of uncertainty and may increase the risk of non-compliance, leading to significant penalties and reputational damage. To address this issue, organizations should seek legal advice from experts in data protection law to ensure that they are properly assessing the legal framework in the third country where personal data is being transferred. They may also need to conduct their own research on the data protection laws and regulations in the third country and seek additional guidance from supervisory authorities to ensure that they are meeting the appropriate safeguards required by the GDPR. At this point, it is worth mentioning that the standard of risk assessment as promoted by the GDPR is, to some extent, more challenging than similar

[527] CJEU decision in the Schrems II case in July 2020 has further complicated the transfer of personal data to third countries. The ECJ invalidated the EU-US Privacy Shield framework, which had previously been used by organizations to transfer personal data from the EU to the US. The court also raised concerns about the use of standard contractual clauses (SCCs) as a means of ensuring an adequate level of protection for personal data transferred to third countries. The decision requires organizations to undertake additional measures to ensure that any transfer of personal data to a third country meets the GDPR's requirements for appropriate safeguards. As a result, the transfer impact assessment process has become even more complex, and organizations must carefully consider the legal framework and risks associated with any transfer of personal data to a third country.

standards regarding data processing[528]. As an example, for legal acts such as HIPAA or CCPA, which both deal with personal data processing, the requirements of accountability and obligation to document are more generic, which in fact, leaves more space for individual assessment for the data controllers[529]. Under the GDPR, the level of legal certainty remains low but is, however, not followed by practical guidelines. At that point, it is worth coming back to the question, that was already asked by, among others, Roscoe Pound, namely, what the task of law in the light of social engineering and law in practice is[530]. Pound observes the phenomenon that was previously discussed by Jhering, namely that the law does not shape its own interests, it meets the interests of the society when the society starts to demand certain

[528] Under the GDPR, impact assessments (DPIA) are mandatory for certain types of processing activities that are likely to result in a high risk to the rights and freedoms of individuals. DPIA, which stands for the impact assessment requires any processing entity to identify and assess the risks associated with the processing activity and to implement appropriate measures to mitigate those risks. The DPIA must also be documented and made available to supervisory authorities upon request. The GDPR's DPIA process is considered comprehensive and effective. It usually requires external support from lawyers or technological field experts. HIPAA, on the other hand, requires covered entities and business associates to perform a risk analysis, which remains a concept similar to DPIA, to identify and mitigate risks to the confidentiality, integrity, and availability of electronic protected health information (ePHI). The risk analysis process is not as comprehensive as the GDPR's DPIA process, and it does not require organizations to document or submit their risk analyses to a regulatory authority. However, HIPAA does require covered entities and business associates to implement reasonable and appropriate safeguards to protect ePHI, based on the results of the risk analysis. Furthermore, the CCPA, which applies to certain businesses operating in California, requires organizations to perform a risk assessment to identify and mitigate risks related to processing personal information. The CCPA's risk assessment process is less prescriptive than the GDPR's DPIA process and does not require organizations to document or submit risk assessments to a regulatory authority. However, the CCPA does require organizations to disclose certain information about their data processing activities to individuals upon request and to implement certain security measures to protect personal information.

[529] HIPAA's risk analysis is outlined in 45 CFR § 164.308(a)(1)(ii)(A), which requires covered entities and business associates to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Similarly, the CCPA's risk assessment is outlined in California Civil Code § 1798.150, which requires businesses to assess the risks associated with their processing of personal information and to implement reasonable security measures to mitigate those risks.

[530]The main focus of the question of law in books was presented by Roscoe Pound in his book titled *Law in Books and Law in Action*, (American Law Review 1910 , vol. 44, no. 1, pp. 12-36) but further the evaluation of the task of law was discussed in his other publication titled *Task of Law* (*Task of Law:The North Law Lectures*, Lancaster 1944.)

protection[531]. It remains the obligation of the law to recognize such interests and navigate through them[532].

As a consequence, one may ask a vital question – if this is within the scope of interest of society, namely entrepreneurs, to be able to rely on law to avoid uncertainty of whether processing of personal data may be processed or not, and at the same time the support for such legal obligations remains limited, what does that say about the quality of law? GDPR remains one of the most important regulations in the history of data processing, but at the same time, it remains the one with the biggest amount of uncertainty because of the gap between practical implementation and legal requirements when it comes to the transfer and obligation to rely on the undefined source of transfer impact assessments.

A similar challenge, or phenomenon, is visible with regard to the right to be forgotten. As a one of the key elements of the GDPR, the right to be forgotten and its execution remain a blurry area for internet-operating software. As discussed before, current modeling of data removal remains distinct from the classic, legal, understanding of what it means to remove personal data – consequently, one can currently observe a distinction between what we have required by law and what we meet in action. The right to be forgotten was a subject of discussion both in legal actions as well as in the media regarding some errors and misinterpretations of how the law works. For example, in 2014, Google received a request from a person to remove links to a news article that contained information about his financial past. Google initially removed the links, but the publisher of the news article challenged the removal, arguing that it was an infringement of freedom of expression. In 2018, the European Court of Justice ruled that Google was not required to remove the links globally but could be required to remove them within the EU[533]. In fact, Google, as one of the biggest data processing search engines, has been challenged about the right to be forgotten a couple of times. In 2016, the company received another request from a businessman to remove links to news articles that contained information about his past criminal convictions. Google initially refused to remove the links, arguing that the information was in the public interest and, as a consequence, believed to be exempted[534]. However, the businessman challenged the decision in court, and in 2018, the UK High Court ruled that Google was required to remove the links. At the same time, pure practice

[531] R. Pound, *Social Control Through Law*, New Haven, London, 1942, pp. 64-65.

[532] *Ibid*. p. 68.

[533] Google v. CNIL, Case C-507/17, European Court of Justice, 2018.

[534] NT1 and NT2 v. Google, EWHC 799 (QB), UK High Court, 2018.

about the execution of the right to be forgotten has also been challenged[535]. In 2019, Google was fined by the French data protection authority (CNIL) for failing to comply with the right to be forgotten[536]. The authority found that Google had not sufficiently delisted links to sensitive personal data from its search results and had not notified publishers of the removals.

As a consequence, there is a practical challenge in the implementation of the right to be forgotten, that, due to the way practice works, may lead the data controllers to be assessed as non-complying with the data processing requirements of the GDPR. In fact, one may ask the question, is full compliance with the requirements of the GDPR always in the best interest of the data subjects, and what is more, is this compliance possible with such a dose of uncertainty and difference in application across all EU countries?

Although the Global Data Protection Regulation is intended to protect the unique rights of data subjects, there are worries that its actual implementation may be ambiguous. It went into effect in May 2018. For instance, the obligation for transfer effect assessments, which is meant to ensure that personal data is moved to third countries only if sufficient protection is in place, has not yet been adequately explained. The legal obligations outlined in the GDPR and the actual protection provided to individuals may differ as a result of this lack of clarity. Because of the degree of uncertainty, it is possible that the GDPR will just serve as a set of regulations on paper rather than providing the actual protection of individual rights, which affects the possibility for individuals to factually rely on those laws. At the same time, it vastly exposes the controllers to undefined risks.

[535] The accuracy of how data are being removed has been also discussed by the media, removal of personal data from the extensive data resources places certain dose of risks on the processing entities. For example, due to previous decisions on the geolocation of the data covered by delisting there was an accusation towards Google that the company uses their geolocation feature to hide links from the search listing. More details in: F. Lardinois, *Google now uses geolocation to hide 'right to be forgotten' links from its search results TechCrunch, 4 Mar. 2016*. Retrieved March 24, 2023 from https://techcrunch.com/2016/03/04/google-now-uses-geolocation-to-hide-right-to-be-forgotten-links-from-its-search-results.

[536] *Google LLC v. CNIL*, No. 16/00196, French data protection authority, 2019. *Cf. :* CJEU, Judgement, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, September 2019. ECLI:EU:C:2019:772.

Conclusion

Data processing laws have grown to be one of the most influential and challenging for the practical application of the law. We are currently living in an era of inevitable change where personal data becomes one of the most valuable units and where technological growth usually leaves changes in the law behind. At the same time, the phenomenon that we observe is the question of the reliability of the law and the possibility to base our actions on it, the capacity to foresee its outcomes, and the trigger of avoidance of the law due to an outdated approach if the law does not fit the reality[537]. There is no doubt that by incorporating non-normative instruments into the jurisprudential field, we are situating legal research in a considerably bigger and quite distinct field. Advocates of a shift in emphasis from *law* to *regulation* may encounter criticism, but at least most regulatory theorists view regulation as normative and beginning with the establishment of standards. This idea of *regulation* would still be limited to normative signals if the *regulatory environment* embraced it, which may be acceptable to many lawyers. Yet, we are not concerned about the comfort of the judges. The emergence of a pervasive risk management attitude and the perceived transition to technological management are the topics of our cognitive attention[538]. The purpose of this is to channel human behavior, which is considerably different from typical legal strategy and legal thinking[539]. To understand what is happening with regard to the channeling of conduct within jurists' own narrowly circumscribed domain, they have to expand their horizons, regardless of how uncomfortable it may be. Modern legal systems, to be able to catch up with the constantly developing world of technologies has to be able to challenge itself and produce solutions that are usable, reliable, and, at the end of the day, possible to implement in practice. A good summary of the approach

[537] One of the legal thinkers who discussed the idea that a law that cannot be effectively enforced is not a subject of the quality of law was the American legal philosopher and jurist Lon L. Fuller. In one of his famous, previously quoted, works titled *The Morality of Law* (1964), Fuller argued that for a law to be legitimate, it must meet a set of criteria, including the requirement that it be possible for people to comply with it. Fuller's idea was that if a law is so vague, contradictory, or incomprehensible that people cannot reasonably understand how to comply with it, then it cannot be considered a valid law. He called this the principle of legality and argued that it is essential to the rule of law. Other legal thinkers who have addressed the concept that an unenforceable law is not meeting the threshold of being a law include H.L.A. Hart and Ronald Dworkin, both of whom were also influential in the field of legal philosophy.

[538] xxxx

[539] Similar view was presented by Karl N. Llewellyn in his writing *The Normative, the Legal, and the Law-Jobs: The Problem of Juristic Method*, Yale Law Journal, 1940, vol. 49, p. 1355.

of jointly-influencing arts was proposed by Lobel. According to Lobel, in many areas of competition and innovation, informal limitations imposed by foreground social norms are more significant than formal restraints (if any) found in background regulations. *Competitive environments from fashion to magic, comedy to cuisine have managed to protect the process of innovation without resorting to the most restrictive controls. The distinction between control and freedom does not have to be a binary one, that is, one of negative spaces free of controls contrasted with formal legal systems saturated with the big sticks of protections and restrictions … In every industry, we find practices of self-imposed confidentiality alongside practices of openness and sharing; we find places where norms substitute for law. Reputation replaces litigation*[540]. The above presented quote exposes the need for distinction between control and freedom as well as the need for every industry, in my opinion, including law, to self-impose the openness to understand other industries that it aims to regulate and to cooperate on the solution that may appeal to the social need. At the beginning of this thesis, the assumption of a relationship between privacy and data processing law was made. Privacy and the aim to protect it have been doctrines for a remarkable period of time, and the natural desire to shape information about ourselves and project the way we are seen stands as the underpinning values for such need[541]. In fact, modern developments in data protection laws, such as the GDPR, have privacy as underpinning value as well. One of the most significant data privacy regulations in history, the GDPR has received accolades for its extensive reach and considerable influence on how businesses manage personal data. It has, nonetheless, drawn flak for being convoluted and ambiguous in several places. The GDPR's legal language is frequently ambiguous, which has caused misunderstanding and inconsistent application. Compliance is a demanding task for firms of all sizes since its standards are frequently challenging to put into practice. As a result, the GDPR is regarded as both an important advancement in data protection and a complicated piece of legislation.
The GDPR came with a vast impact on the ability of data controllers to operate on data. The industry that may be said to be most affected by the legislation is the area of widely understood IT. The GDPR has had a significant impact on the IT industry, as it has forced companies to

[540] O. Lobel, *Talent Wants to Be Free: Why We Should Learn to Love Leaks, Raids, and Free Riding*, New Haven, 2013, p. 239.

[541] Early case example of previously quoted UK, Judgement, *Southey v Sherwood And Others*, [1817] EngR 351, (1817) 2 Mer 435, (1817), 35 ER 1006, March 1817. Retrieved December 13, 2021 from https://vlex.co.uk/vid/southey-v-sherwood-and-805313089.

fundamentally change how they collect, store, and process personal data. This has affected a wide range of businesses, including tech companies, social media platforms, online retailers, and more. One of the most significant ways in which the GDPR has affected the IT industry is through the requirement for explicit consent from individuals for their data to be collected and used. This has led to changes in the way companies design their user interfaces and obtain consent, as well as changes in the way they handle and store personal data. For example, companies like Google and Facebook have had to update their privacy policies and provide more transparency around data collection and usage. Other companies have implemented measures like pseudonymization and encryption to protect personal data. Additionally, the GDPR has introduced hefty fines for non-compliance, which has forced companies to take data protection seriously and invest in compliance efforts. Overall, the GDPR has had a significant impact on the IT industry and has forced companies to prioritize privacy and data protection in ways that were previously uncommon. Consequently, online-operating software remains one of the best litmus tests to assess the implementation of this regulation in practice. One of the main underpinning values of the GDPR is the protection of privacy and individual rights. Such an understanding of the role of the right to privacy and data protection with regard to one of two key elements of this evaluation, namely data transfer rights and the right to be forgotten, has been mentioned numerous times across EU legislation. One of the most important agreements between the European Commission and the biggest economy in the world, namely the United States of America, directly recalled the protection of privacy as the value that processing data stands for. Further decisions of the European Court of Justice invalidating every agreement between those two actors were also grounded on the fact of privacy infringement. In the final report after Safe Harbour invalidation, we can read as follows: *[…] the Court finds that the Safe Harbour Decision denies the national supervisory authorities their powers where a person calls into question whether the decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals*[542]. The fact that privacy is the value and the right that motivates all rights included in the GDPR further referred to under Articles 5-11 of the GDPR, seems very natural and obvious. Of course, none of the rights included in the GDPR stand as absolutes, and even the right to privacy as a fundamental right is frequently balanced against other rights. Having this in mind, any actor engaged in the processing of personal data focuses on the determination of the scope and limits

[542] Court of Justice of the European Union PRESS RELEASE No 117/15 Luxembourg, 6 October 2015 Judgment in Case C-362/14 *Maximillian Schrems v Data Protection Commissioner, op.cit.*

of legal actions that may be taken during data processing. Especially in the field of software technology, personal data are a day-to-day subject of work, and the processing of such data is the core element of business operations. Consequently, industry and law face the challenge of strong social demand to clearly regulate the boundaries of law and take into consideration the practical aspect of law – *law in action*[543]. GDPR aimed to be very generic to tackle the challenge of a fast-changing environment, but does this complexity reflect the real social need? This question, of a philosophical nature, has already been asked in the past by, among others, R. Pound and W. O. Holmes – they questioned the quality of law when it did not reflect the real social need. Similarly, as at the time of R. Pound, we can observe some reluctance to bring clear solutions – Schrems I and II judgments cut a line between prior relations between the US and EU but bring no direct solution on how to facilitate the transfer. This action seems to ignore the fact that the US-EU transfer is one of the most vital for internet operation and that almost every SaaS, PaaS, software, or platform development depends on this transfer. With this uncertainty, the GDPR places disproportionate responsibility on the data controllers, pointing them out as the ones to be blamed for. From a formal perspective, such a placement of blame is reasonable, but does it factually reflect the need for data protection and accountability for data infringement? Taking into consideration the fact that the controller of personal data does not need to have legal personality thanks to the broad definition included in the GDPR, the ability for the data subject to unconditionally rely on a law that guarantees accountability is failing[544]. At the same time, disproportion between the assumption that we can exclude personal data and the practice places the data controller, as a bad guy interested only in the consequences, in a very disadvantaged position. The law currently states that the data controller is in charge of security measures, that the controller is the entity that defines the aim and

[543] This directly refers to the question of the quality of law, as further recalled in prior parts of this thesis with regard to the legal thought of Fuller and the question of how the law fits the social demand as discussed by Pound.

[544] GDPR, art. 4(7) reads as follows: 'controller' means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;. This directly states the possibility of a non-legal person being the data controller, which causes discussed difficulty. Furthermore, the fact that a non-legal, public body may be considered a data controller also brings formal challenges. For example, a school is considered to be the data controller of students' data. At the same time, schools cannot be sued in a simple term or held liable. Therefore, there is a lack of enforceability for violations when there is a lack of accountability in the personal data controller.

purpose of processing, and that the controller is in charge of the broadly understood quality of processing. Lastly, the controller is considered the entity to issue instructions to the processor ordering how the processing shall be performed[545]. The definition included in Article 28 implies that there is a superiority relation of the controller and the processor and the factual impact on data processing[546]. Nevertheless, the reality stands in opposition to the law in books in this regard – usually controller shall, at some point, use third-party vendors to deliver the product. The presence of market leaders with no considerable alternatives, such as Google analytics or Google Adds, Amazon, or Facebook, limits the ability of data controller to use or not to use the services necessary to deliver or maintain the final product. From a purely practical perspective, the challenge is not only because of the presence of market monopolists, but also because of the practical dimension of how the software development works. Once the infrastructural elements, such as the database or architecture is being developed the amendment of crucial operational elements would be equal with a decision to shut down the project and develop it from scratch. As a result, a significant part of the expected changes or adjustments that may be ordered by the controller cannot be implemented in practice because they interfere too much in the operation of the systems[547]. The legal regulation (*law in books*) expects from the data controller to be in charge of data transfers, places responsibility for the transfer and suggest the instrument as Transfer Impact Assessment at the same time invalidating the most reliable and important transatlantic agreement that facilitated the transfer of personal data necessary for the industry. Furthermore, invalidation itself as issued by the European Court of Justice, is broader than the standard understanding of GDPR, what brings even more uncertainty into the equation. Schrems II judgment stated that the surveillance laws on the territory of the US, especially regarding the FISA act and programs as PRISM, extends the

[545] Article 28 of the GDPR states that the Processor shall process personal data in line with the following: *processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.*

[546] Such understanding is further supported by the Audit rights included in article 28(3)(h) of the GDPR.

[547] One of such examples may be data retention and data removal from back-ups. The ability to amend the backup is limited in the majority of databases; nevertheless, we cannot guarantee that the processing shall be absolutely excluded if the data are being stored in back-ups due to broad definition of what we consider as data processing.

scope of US government beyond what is proportionate and necessary[548]. At the same time, it is important to ask the question what rights this collision of law balances. On one side, we have the FISA act and US surveillance laws that are dedicated to tackle threats to national security, and on the other data processing safeguards that originates from the act that itself list threat to public security as exception to the processing requirements[549]. Furthermore, under such circumstances, according to Scherms judgment and the European Court of Justice created two controversial assumptions, namely (1) extended the jurisdiction of GDPR and by its mean its own jurisdiction to the country that is not a member state of the European Union and (2) that acts such as FISA that are directed towards the protection of mutual benefit of combating terrorism and ensuring national security[550]. GDPR by its nature is EU law applicable in two dimensions – to EU territory (member states) and to the processing of the personal data of European citizens. While the first criterion raises no questions or doubts in the majority of interpretations, the latter one, further supported by the jurisprudence of the ECJ is difficult from a practical perspective. Under currently known practice, especially grounded in previously quoted Schrems judgments, the applicability of the GDPR standards of processing and responsibility of data controllers to exclude, control and limit the transfer to third party countries is promoted[551]. It further extends such responsibility to the scope that goes beyond the GDPR itself and aims to include that the data controller and EU supervisory authority shall

[548] Para. 184 of Schrems II judgment reads as follows: *It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.*

[549] Among others such interpretation is supported by Recital 19 of the GDPR and Recital 73 of the GDPR.

[550] The Focus on terrorism and national security was included in the initial draft of FISA dated 1978, further The Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, amended the definition of "agent of a foreign power" in FISA (50 U.S.C. § 1801(b)(1)), to add a new category to address the lone wolf by its provision (individuals, exceeding the definition of Agent by FISA, that are acting alone but their actions is targeted against national security).

[551] *Maximillian Schrems…*, Case C-362/14, *op. cit.*, p. 28, *On 25 June 2013 Mr Schrems made a complaint to the Commissioner by which he in essence asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA').*

ensure that there would be no interference with such processed data confidentiality at all cost even once weighting is against the public security. For the purpose of thought experiment let's imagine a situation that is fully grounded on the European level, in the situation of one EU member state officially asking the other member state to permanently abandon the idea of public security and the use of national surveillance the likelihood of the acceptance of such a proposal boarders with the absurd. National security remains one of the most important underpinning values from national perspective and under regular circumstances, there is no possibility of such exclusion. What is more, the GDPR itself mentioned as one of the exemptions the public interest included in Article 6 of the GDPR and further in Article 49(1)(d)[552]. Among others, for that reason the global encryption standards have been unified for commercial use on the level of recommendations, and the recommendation is in general to apply such standards that would enable the national authority to access encrypted data in the case of national security threat[553]. Lastly, with the arguments raised in the Schrems judgment that raise the objections towards the data transfer to the US wherein the argument against such transfer is grounded mostly on the ability of national intelligence to access the data, the CJEU questioned the underpinning values of military pact between the EU and USA. Assuming that the public interest is insufficient value to exclude application of GDPR, we further we are undermining the value of the NATO alliance, which is designed to focus on stabilizing the military situation with the participation of EU member states and the US, and promotes the common interest of these countries. Such orthodoxic interpretation of the GDPR in my opinion, constitutes an overinterpretation of the provisions directly derived from the law and introduces the factor of lack of real enforceability of the law. Currently existing tendency in interpretation of this act also raise the question of balancing rights. From a purely practical perspective, the interpretation of the GDPR limits the aspect of freedom to undertake business activity, narrow down the scope of decisiveness of entrepreneurs while at the same time assigning them with a broader scope of responsibility. As a side note, from a purely constitutional perspective one may also ask the question of least restrictive mean employed to achieve the goal brought into life by the GDPR, namely protection of privacy and hypothetical lose that may be drawn from it based on risk assessment hypothesis versus the real and tangible limitation of

[552] Article 49 of the GDPR directly states the exemption of the applicability of legal act in case where *the transfer is necessary for important reasons of public interest*.

[553] Such codification attempts were developed, among others, by Advanced Encryption Standard (AES) where it specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data.

entrepreneurship.

Under the treaties that establish the European Union (EU), the EU has exclusive competence in certain areas, including the protection of personal data[554]. This means that the EU has the exclusive authority to legislate and adopt binding acts in these areas, and member states are required to adopt and implement EU legislation in these areas. However, the EU's competence in the area of personal data protection is not absolute, and there are certain exceptions and limitations to the EU's authority. One of these exceptions is the exclusion of activities related to the national security of member states from the scope of EU data protection law. The exclusion of activities related to national security from the scope of EU data protection law reflects the fact that member states have primary responsibility for the protection of their national security and that the EU's competence in this area is limited. This exclusion is reflected in various provisions of EU data protection law, including the General Data Protection Regulation (GDPR). One of these exceptions is the exclusion of activities related to the national security of member states from the scope of EU data protection law. This exclusion is reflected in various provisions of EU data protection law, including the General Data Protection Regulation (GDPR), article 3 which reads as follows:

[554] According to the Treaty on the Functioning of the European Union (TFEU), the EU has exclusive competence in the following areas: Customs union: "The Union shall have exclusive competence in the following areas: (a) the establishment and functioning of the internal market; (b) the customs union." (Article 3(1) TFEU) Monetary policy: "The Union shall have exclusive competence in the following areas: (a) the conservation of marine biological resources under the common fisheries policy; (b) the economic, social and territorial cohesion of the Union; (c) the common commercial policy; (d) the common agricultural policy; (e) the common transport policy; (f) the common energy policy; (g) the common foreign and security policy; (h) the area of freedom, security and justice; (i) the competition rules necessary for the functioning of the internal market; (j) the non-discrimination and equality between men and women; (k) the company law, in so far as it relates to the creation and functioning of the internal market; (l) the protection of consumers; (m) the interpretation and application of the agreements and association of the Union with third countries and the bodies representing the interests of these countries." (Article 3(2) TFEU) Foreign and security policy: "The Union shall have exclusive competence in the following areas: (a) the common commercial policy; (b) the common agricultural policy; (c) the common transport policy; (d) the common energy policy; (e) the conservation of marine biological resources under the common fisheries policy; (f) the common foreign and security policy; (g) the area of freedom, security, and justice." (Article 3(3) TFEU).

This Regulation shall apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

This Regulation shall apply to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union[555].

Furthermore, GDPR as a regulation is not intended to apply to the processing of personal data: (1) by the Member States when carrying out activities that fall within the scope of Chapter 2 of Title V of the TFEU, which relates to the common foreign and security policy[556]; (2) by a natural person in the course of a purely personal or household activity; (3) by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security[557]. This demonstrates that activities related to the national security of member states are excluded from the scope of the GDPR. The issue of the inadmissibility of including the sphere of national security in EU regulations as an area excluded from EU competence under the treaties has been the subject of debate and legal challenges. Some have argued that the exclusion of activities related to national security from the scope of EU data protection law may conflict with the fundamental rights of individuals and undermine the EU's commitment to the protection of personal data. Others have argued that the exclusion is necessary to ensure that member states have the necessary flexibility to

[555] GDPR, art. 3.

[556] Chapter 2 of Title V of the Treaty on the Functioning of the European Union (TFEU) deals with the common foreign and security policy (CFSP) of the European Union (EU). The CFSP is the EU's framework for cooperation in the fields of foreign and security policy, and it is designed to help the EU speak and act as a single entity in international affairs. The TFEU sets out the general principles and objectives of the CFSP, as well as the competences and powers of the EU in this area.

[557] GDPR, rec. 19.

protect their national security interests. Consequently, it becomes clear and visible that the judgment of Schrems aims to regulate the scope that remains outside of the regular EU jurisdiction, and it raises the issue of the inadmissibility of including the sphere of national security in EU regulations as an area excluded from EU competence under the treaties. The perspective of the GDPR with broad definitions and high expectations places two important questions that, in my opinion, remain unanswered: (1) what rights we aim to protect with the GDPR and moves to treat it as absolute and imposable on external countries as the US, are those rights the one listed directly in the GDPR or the one derived from this legal act based on the understanding of the right to privacy, and (2) how we could rely on law and believe in the practical protection of rights of individuals and just consequences for data controllers with all disproportions that are currently built and further expanded by the interpretation of the GDPR. Those practical questions are further underpinned by the philosophical question of whether we can apply the law with such a dose of uncertainty or whether an unenforceable law is a law. There is no clear and defined answer, and the line of reasoning presented in the doctrine supported by thinkers such as Holmes or Pound proves that the reliability and foreseeability of the law remain one of the most vital questions about the nature of law. Such a question becomes even more vivid in the time of technological growth, AI, big data and mass processing that we can observe at the moment. This time in the history of legislation posts one of the most undefeated questions about the ability to apply law in practice mostly due to the high technological complexity that is full to dependencies and corner cases. Ignorance towards such corner cases or simplification in the placement of responsibility as we see now through the scope of responsibility placed upon data controllers shall emphasize the divergence between law and practice and thus will bring us renewed questions about the nature, role and nature of law. The best real test for the above questions will certainly be the upcoming decisions of the ECJ as well as the European Commission in terms of the development of law in the area of data protection nevertheless without real changes we will reach a point when the shortcoming will be so far and different from the book expectation that a real conflict of law in books v. law in action will be visualized.
One of the imaginable solutions for the challenges brought by the GDPR into life may be the certification that covers the questionable areas of law. There is no official certification for compliance with the General Data Protection Regulation (GDPR). The GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It sets out specific requirements for the processing of personal data and applies to all companies that process the personal data of individuals in

the EU/EEA, regardless of where the company is located. Companies are responsible for ensuring compliance with the GDPR, and failure to comply with the GDPR can result in significant fines and penalties. The GDPR includes provisions for the enforcement of compliance, including the authority of data protection authorities to investigate and impose fines for non-compliance. Controllers had to face an even more challenging processes with the rise of artificial intelligence models becoming more popular. With regard to the right to be forgotten and audits in particular, the emergence of AI poses significant difficulties for GDPR compliance. Due to the effect that erasing data may have on AI models, the right to be forgotten may need to be revised. For instance, eliminating data from a dataset could make an AI model less accurate, which might lead to bias and mistakes. The requirement to preserve the accuracy and efficacy of AI models must thus be weighed against the right to be forgotten. Furthermore, because AI is a complex system, auditing AI systems comes with its own set of difficulties. It's possible that the conventional auditing techniques that were previously employed before AI won't be enough, and new auditing procedures must be established to account for the particular issues presented by AI. Furthermore, worries about the potential exploitation of personal data have been raised by AI's capacity to analyze enormous amounts of data and spot patterns. With AI acting as a super-censor that might be used to influence and control vast amounts of data, George Orwell's vision of rewriting history in "1984" could come to pass. This authority has the potential to be misused to invade people's privacy and facilitate widespread surveillance. Therefore, new laws must be passed to guarantee that AI is applied morally and that people's privacy rights are upheld. AI poses additional difficulties for GDPR compliance, necessitating changes to the right to be forgotten and auditing procedures. It's critical to strike a balance between the necessity to preserve AI's efficacy and accuracy and the right to be forgotten. Furthermore, ethical guidelines must be established to guarantee that AI is applied in a way that respects people's right to privacy and averts power abuse. If this is not done, there may be possible privacy rights breaches and greater surveillance of people.
There must be a tighter synergy between social/market goals and the legal requirements if the IT sector is to successfully comply with GDPR. Both conventional data processing and AI-based procedures exhibit this. The GDPR offers a framework for protecting personal data, but it can be difficult for data controllers to execute because the EU frequently provides little help or advice in this area. Existing recommendations, such as those created by the Working Party group, for instance, might not be appropriate for the situation at hand or might be too general to offer useful advice. Because of the absence of thorough instructions and assistance, data controllers may find it difficult to comply with GDPR. There is a need for particular rules and

best practices to be created because of the growing dependence on AI-based systems so that these systems can adhere to GDPR. Furthermore, traditional auditing measures might not be enough to ensure GDPR compliance because AI-based systems are inherently more complex than conventional data processing systems. This demonstrates the necessity of developing more creative auditing methods to guarantee adherence to GDPR rules. Additionally, promoting a culture of data privacy and security within the IT industry is a crucial part of GDPR compliance. In order to help data controllers traverse the complexity of GDPR, the EU should endeavor to build a tighter interaction between regulators and data controllers as well as offer more precise and useful information. By doing this, the EU may support the establishment of a GDPR-compliant, more accountable, and transparent data processing strategy. The emergence of AI is likely to result in a fundamental change in the currently existing norms, including those relating to data protection. With the increasing role of AI in both administrative and daily life, there is a growing recognition that individual rights may need to be balanced against the wider societal good. The use of AI-based systems presents a number of challenges for data protection, particularly in terms of the right to be forgotten and the need for auditing measures that are appropriate for these systems. Additionally, AI-based systems have the potential to redefine moral and ethical standards. The idea of the common good might override individual rights if AI becomes more commonplace, especially in situations involving public health or national security. Important problems concerning how to strike a balance between individual rights and group interests and how to make sure that the usage of AI-based systems complies with GDPR's guiding principles are raised by this. As a result, continuing discussion and debate concerning the effects of AI on privacy and individual rights are necessary. This entails examining the possible effects of AI on current norms and values as well as formulating plans for striking a balance between people's individual rights and broader community objectives. By participating in this discussion, we can guarantee that the development and implementation of AI-based systems are consistent with the principles of GDPR and advance a responsible data processing culture that puts both individual rights and the welfare of the community first.

There are, in my opinion, only two ways to proceed to provide alignment between the law and practice: (1) the interpretation of the GDPR becomes more responsive towards market reality, and the way companies operate at the moment, especially about the data transfer via third party providers. What shifts the focus from the formalistic approach of no transfer, and total responsibility on data controllers into the allowability of transfer with realistic requirements, (2) European Commission should invest in the certification process that guarantees compliance

with legal norms that are currently expected by the orthodox interpretation of the GDPR as promoted by the CJEU. Such a corresponding interpretation shall not only take into account the technological aspect but also name the corresponding value of cost and the possibility of implementation of particular solutions. Furthermore, from the perspective of the current interpretation of the CJEU, the IT industry would expect the solution to a currently deliberately overlooked problem to be the transfer of data to the US and the fact that, from a practical perspective, the majority of online-operating software providers have no practical possibility to affect data processing by market giants while at the same time being unable to use the solutions that require data transfer to the US, or perhaps other *silicon valley*s of the world such as India. In such a case, the solution does not have to be a necessary, passive auditing process, as we know from standards such as SOC or ISO. Modern technology allows us to develop complex and reliable self-assessment tools to audit security standards and measures. Such a practice has been proven right for the private sector. As an example, Google has closed API access and conducted one of the most restrictive policy launches towards scopes of API consumption that one could observe on the market ever[558]. As an outcome, any vendor that assesses Google API scopes classified as sensitive or restricted had to undergo the audit to comply with security standards[559]. As Google's customer base constantly grows, the provider has developed a self-assessment schedule that enables the company to conduct objective and reliable security checks using self-triggered algorithms and applications. At the same time, the future of data processing has to be built in alignment with and as a response to the revolution of artificial intelligence and the growing accessibility of this technology to the public. The key is mostly a corresponding measure between the law and practice, or even more between the law and reality. The IT industry continues to be one of the most significant challenges to GDPR compliance, and using outdated methods like classic audits to keep up with change may only get us to the next stage of the law's appearance in practice while making it impossible for data controllers to achieve or maintain the practical aspect of applied standards. While observing

[558] Details of the Google API use standards available on the official Google website. Retrieved December 30, 2022 from https://support.google.com/cloud/answer/9110914?hl=en.

[559] *Google Restricted Scope Policy for developers*. Retrieved December 30, 2022 from https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification;

the CJEU's increasingly restrictive interpretations of the GDPR, it is important to consider the purpose of protected data as well as the actual risk to data privacy.

Bibliography

Adequacy decisions. Retrieved March 24, 2023 from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents.

Advances in Digital Forensics XI: 11th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 26-28, 2015, G. Peterson, S. Shenoi (Eds.), Cham, 2015.

Agencia Española de Protección de Datos, GDPR compliance of processings that embed Artificial Intelligence An introduction, 2020. Retrieved April 30, 2023 from https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf.

Alderman E., Kennedy C., *The Right to Privacy*, New York 1995.

Allen S., *Remembering and Forgetting – Protecting Privacy Rights in the Digital Age*, European Data Protection Review 2015, vol. 1(3), pp. 164-177, Retrieved June 13, 2021 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2776048.

Annual Institute on Privacy Law: Strategies for Legal Compliance in a High Tech and Changing Regulatory Environment. Vol. 1 : Practicing Law Institute, Indiana 2011.

Aristotles, *Politics*, Kitchener 1999.

Asana Privacy Policy, Retrieved December 30, 2022 from https://asana.com/terms#privacy-statement.

Atlassian Privacy Policy. Retrieved December 30, 2022 from https://www.atlassian.com/legal/privacy-policy#how-we-transfer-information-we-collect-internationally.

Babers C. , *Architecture Sourcebook Vol.2: Data Centric Architectures*, Morrisville 2007.

Bajac Q. , *The Invention of Photography: The First Fifty Years*, London 2002.

Balkin J. M., *The fiduciary model of privacy*, Harvard Law Review Forum 2020, vol. 134, p. 11.

Balkin J. M., *Information fiduciaries and the First Amendment*, U. C. Davis Law Review, 2016, vol. 49, p. 1183.

Bartoletti I., *An Introduction to the GDPR: Your Rights as a Data Subject*, CPO Magazine May 14, 2018. Retrieved July 20, 2021 from https://www.cpomagazine.com/data-protection/introduction-gdpr-rights-data-subject/.

Barzun C.B., *Three forms of Legal Pragmatism*, Washington University Law Review 2018, vol. 95, no. 5, pp. 1003-1034. Retrieved April 17, 2023 from https://openscholarship.wustl.edu/law_lawreview/vol95/iss5/5/.

Benohr I., *EU Consumer Law and Human Rights*, Oxford 2013.

Beverley-Smith H., Ohly A., Lucas-Schloetter A., *Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation*, Cambridge 2005.

Blackstone W., *Commentaries on the Laws of England* dated, Oxford 1766-1767.

Brownsword R., *Law, Technology and Society. Re-imagining the regulatory environment*, New York, 2019.

Bygrave L. A., *Data Privacy Law: An International Perspectiv*e, Oxford 2014

Bygrave L. A., *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements (June 20, 2017)*, Oslo Law Review 2017, vol. 4, no. 2, pp. 105–120. Retrieved March 18, 2021 from https://ssrn.com/abstract=3035164.

Carr H., Goosey D., *Law for Social Workers.* 15th edition, New York 2019.

Castells M., *The information age. Vol. 1. : economy, society and culture : the rise of the network society*, Oxford 1996.

Castells M., *The information age. Vol. 2 : economy, society, and culture : The power of identity.* Oxford 1997.

Castells M., *The information age. Vol. 3. : economy, society and culture : end of millennium.* Oxford 1998.

Chong E., *Configuring Internal Controls for Software as a Service : Between Fragility and Forgiveness*, Boca Raton 2019.

Cooley T. M., *Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*, Chicago, 1879.

Coppel P., *Information Rights. A Practitioner's Guide to Data Protection, Freedom of Information and other Information Rights*, Edition 5, Oxford 2020.

Council Framework Decision 2008/977/JHA. Retrieved April 17, 2023 from https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng .

Craig T., Ludloff M. E., *Privacy and Big Data: The Players, Regulators, and Stakeholders*, Sebastopol 2011.

Commission Staff Working Document Impact Assessment, Accompanying The Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules

On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts 21.4.2021 SWD(2021) 84 final, Brussels 2021, p. 5. Retrieved April 30, 2023 from https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence.

Data Governance in AI, FinTech and LegalTech Law and Regulation in the Financial Sector, A. Darbellay, J. Lee (Eds.), Cheltenham 2022.

Data Protection and Cloud Computing Framework. Retrieved March 24, 2023 from http://architectureportal.org/data-protection-and-cloud-computing-framework.

Data Protection and Privacy: Data Protection and Democracy, D. Hallinan, R. Leenes, S. Gutwirth (Eds.), Oxford 2020.

Datanyze software. Retrieved December 4, 2022 from https://www.datanyze.com/.

Dijk K. van, Böröcz G., Mantovani T., *Data Protection Impact Assessment in the European Union: Completing the New Legal Framework towards a more robust protection of individuals*, d.pia.lab Policy Brief 2017, no. 1. Retrieved June 25, 2022 from https://osf.io/preprints/lawarxiv/b68em/download.

Dorsen N., Rosenfeld M., Sajo A. [et al.], *Comparative Constitutionalism. Cases and Materials*, Saint Paul 2003.

DPC 2020 Annual Report [online], Dublin, Data Protection Statement, 2020. Retrieved April 17, 2023 from www.dataprotection.ie/en/resources/tuarascalacha-reachtula/annual-report-1-january-2020-31-december-2020.

Drexl J., *Data Access and Control in the Era of Connected Devices Study on Behalf of the European Consumer Organisation BEUC*, Brussels 2008.

Dróżdż A., *Protection of Natural Persons with Regard to Automated Individual Decision- Making in the GDPR*, Alphen aan den Rijn 2020.

Dworkin R., *Imperium Prawa*, Warszawa, 2006.

Dwyer J. G., *The Oxford Handbook of Children and the Law*, New York 2020.

Dyrda A., W*hy legal conventionalism fails?*, Archiwum Filozofii Prawa I Filozofii Społecznej 2015, no. 1(10). Retrieved April 17, 2023 from https://doi.org/10.36280/AFPiFS.2015.1.14, pp. 14-15.

El-Gazzar R., Stendal K., *Examining How GDPR Challenges Emerging Technologies*, Journal of Information Policy 2020, vol. 10, pp. 237-275. Retrieved April 18, 2021 from https://www.jstor.org/stable/10.5325/jinfopoli.10.2020.0237.

Elliott M., Thomas R., *Public Law*, Fourth Edition, Oxford 2020.

European Commission, *Commission Staff Working Paper Impact Assessment on the Proposal for a General Data Protection Regulation, accompanying the document Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final*, Brussels 2012. Retrieved January 10, 2023 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072.

European Commission Press Release, *Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US*, Brussels 2022. Retrieved March 5, 2023 from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631.

The European Data Protection Board (EDPB) Retrieved February 24, 2023 from: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201901_on_the_processing_of_personal_data_under_article_6_1_b_of_the_gdpr_in_the_context_of_the_provision_of_online_services_to_data_subjects_en.pdf.

European Data Protection Supervisory, *Opinion 20/2022, Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence (AI), human rights, democracy and the rule of law ('the convention'), pursuant to Article 218 TFEU*, p. 8. Retrieved April 28, 2023 from https://edps.europa.eu/system/files/2022-10/22-10-13_edps-opinion-ai-human-rights-democracy-rule-of-law_en.pdf.

Feng D. , *Data Deduplication for High Performance Storage Sy*stem, Wuhan, 2022.

Forbes Global 2000. Retrieved March 5, 2023 from https://www.forbes.com/lists/global2000/.

Foulsham M., HitchenB., Denley A., *GDPR: How To Achieve and Maintain Compliance*, New York 2018.

Frantziou E., *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, Human Rights Law Review 2014, vol. 14, no. 4, pp. 761–777. Retrieved June 9, 2021 from https://doi.org/10.1093/hrlr/ngu033.

Freund P. A., *On Law and Justice*, Cambridge, 1968.

Frosio G., *Oxford Handbook of Online Intermediary Liability*, Oxford 2020.

Fuller L. L. , *The morality of Law.* Revised edition, London 1963.

Fuller L. L., *Positivism and Fidelity to Law: A Reply to Professor Hart*, Harvard Law Review 1958, vol. 71, no. 4, pp. 630–672. Retrieved April 17, 2023 from https://www.jstor.org/stable/1338226.

Fuller L. L., *The morality of law*, New Haven 1964.

Fuller L. L., *The Morality of Law*, New Haven 1969.

Fuller, The Morality of Law in 1964;

Gagarin M. , *Early Greek Political Thought from Homer to the Sophists*, Cambridge 1995.

Gal C. S., Kantor P. B., Lesk M. E., *Protecting Persons While Protecting the People: Second Annual Workshop on Information Privacy and National Security ISIPS 2008*, New Brunswick 2008.

Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021 [online]. Retrieved December 4, 2022 from https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021#:~:text=Worldwide%20end%2Duser%20spending%20on,research%20vice%20president%20at%20Gartner.

Gasser U. , Zittrain J., Faris R., Heacock Jones R., *Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse*. Berkman Center Research Publication 2014, no. 2014-17, pp. 70-71, 20. Retrieved March 11, 2023 from https://cyber.harvard.edu/publications/2014/reflections_on_the_digital_world.

Gavison R., *Privacy and the Limits of Law*, The Yale Law Journal 1980, vol. 89, no. 3, pp. 421-471. Retrieved April 19, 2020 from http://www.jstor.org/stable/795891.

Gawroński M., *Guide to the GDPR*, Alphen aan den Rijn, 2019.

Gellert R., *The Risk-Based Approach to Data Protection*, Oxford 2020.

Goffman E., *The Presentation of self in everyday life*

Goodman B., Flaxman S., *EU Regulations on Algorithmic Decision Making and "a Right to an Explanation"* . AI Magazine 2017, vol. 38 no. 3, pp. 50-57. Retrieved April 17, 2023 from https://ojs.aaai.org/aimagazine/index.php/aimagazine/issue/view/219.

Google Cloud Data Processing Addendum (Customers). Retrieved June 20, 2022 from https://cloud.google.com/terms/data-processing-terms .

Google Restricted Scope Policy for developers. Retrieved December 30, 2022 from https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification.

Grabski J., *Valuation Techniques and the Economics of Software as a Service* [In;] *SSRN* [online]. Retrieved December 30, 2022 from https://ssrn.com/abstract=3509782.

Grafenstein, von M., *The Principle of Purpose Limitation in Data Protection Laws*, Baden-Baden 2018. Retrieved March 18, 2021 from https://www.jstor.org/stable/j.ctv941v5w.5.

Grama J. L. , *Legal and Privacy Issues in Information Security*, Third Edition, Burlington, 2020.

Guide to the General Data Protection Regulation (GDPR) [online]. Retrieved February 16, 2021 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/.

Halperin J. L., *Law in Books and Law in Action: The Problem of Legal Change*, Meine Law Review 2011, vol. 64, no. 1, pp. 45. Retrieved November 21, 2021 from https://digitalcommons.mainelaw.maine.edu/mlr/vol64/iss1/4.

The Hart-Fuller Debate in the Twenty-First Century, P. Cane (Ed.), Oxford 2010.

Hart, H. L. A., *The Concept of Law,* 3rd edition, Oxford 2012.

Hart, H. L. A., *The Morality of the Law [Book Review]*, Harvard Law Review 1965, vol. 78, pp. 1281-1295.

Hart, H. L. A., *Positivism and the Separation of Law and Morals*, Harvard Law Review 1958, vol. 71, no. 4, pp. 593–629. Retrieved April 17, 2023 from https://www.jstor.org/stable/1338225.

Hirshleifer J., *Privacy: Its Origin, Function, and Future*, The Journal of Legal Studies 1980, vol. 9, no. 4, pp. 649-666.

Hoeren T., Kolany-Raiser B., *Big Data in Context: Legal, Social and Technological Insights*, [S.l.], 2017.

Holmes O. W., *Common Law*, New York 1991.

Holmes O. W., *The Path of the Law* (1897) Harvard Law Review 1897, vol. 10, no. 8 (March. 25, 1897) https://www.jstor.org/stable/1322028

Information Commissioner's Annual Report and Financial Statements 2019-20, London 2020. Retrieved June 9, 2021 from https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

Informational Commissioner's Office, *International transfers* [In:] *Guide to the General Data Protection Regulation (GDPR)* [online]. Retrieved December 4, 2022 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.

Irvine A. A. M. , *Human Rights, Constitutional Law and the Development of the English Legal System*, Portland 2003.

Jain V., Chaudhary G, Cengiz M., *Advances in Data Sciences, Security and Applications: Proceedings of ICDSSA 2019*, Singapore 2020.

Jhering R. von, *Der Kamph ums Recht*, Paderborn 2013.

Kelleher D., Murray K., *IT Law in the European Union*, London 1999.

Kelsen H., *General Theory of Law and State*, A. Wedberg (Transl.), Clark 2011.

Kelsen H., *Pure Theory of Law*, M. Knight (Transl.), 2nd print., Berkeley 1970.

Kemme B., Jiménez-Peris R., Patiño-Martínez M., *Database Replication*, Waterloo 2010.

Kerr I., Kerr I. R., Steeves V. M., [et al.], *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York 2009.

Kettemann M. C., T*he Normative Order of the Internet: A Theory of Rule and Regulation Online*, New York 2020.

Klamert M., Kellerbauer M., Tomkin J., *Commentary on the EU: Treaties and the Charter of Fundamental Rights*, Oxford 2019.

Kołodziej M., *Ochrona danych osobowych w marketingu internetowym po zmianie przepisów*, Warszawa, 2016.

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom 1. Komentarz do artykułów 1–18, L. Garlicki (Ed.), Warszawa 2010.

Koops B. J. , *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice*, SCRIPTed: A Journal of Law, Technology & Society 2012, vol. 8,

pp. 1-28. Retrieved April 17, 2023 from https://papers.ssrn.com/sol3/ papers.cfm?abstract_ id=1986719.

Kościuk D., *General Data Protection Regulation (GDPR) – The EU Law Strengthening the Information Society in Poland*. Białostockie Studia Prawnicze 2018, vol. 23, no. 2, pp. 139-148.

Krzysztofek, M. *GDPR: General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union,* Alphen aan den Rijn, 2019. Retrieved April 20, 2023 https://transparencyreport.google.com/.

Kuner C., Bygrave L. E., Docksey C., *The EU General Data Protection Regulation (GDPR). A Commentary,* Kettering 2018.

Kuner C., Bygrave L. E., Docksey C., *The EU General Data Protection Regulation (GDPR). A Commentary,* Oxford 2020.

Lambert P., *Understanding the New European Data Protection Rules*, Boca Ratón 2018.

Lasswell H. D., Macdougal M. , *Jurisprudence for a Free Society: Studies in Law, Science, and Policy,* New Haven, 1992.

Leszczyński L., Liżewski B., *Ochrona praw człowieka w Europie – szkic zagadnień podstawowych*, Lublin 2008.

Li T., Villaronga E.F., Kieseberg P., *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, Computer Law & Security Review 2018, vol. 34, no. 2, pp. 304-313. Retrieved April 17, 2023 from https://doi.org/10.1016/j.clsr.2017.08.007.

Liptak A., *An Exit Interview With Richard Posner, Judicial Provocateur*, New York Times 2017, vol. 11, September 12, p. A18. Retrieved November 28, 2021 from https://www.nytimes.com/2017/09/11/us/politics/judge-richard-posner-retirement.html.

Litwiński P., Barta P., Kawecki M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w swobodnym przepływem takich danych. Komentarz,* Warszawa 2018.

Llewellyn K. N., *The Normative, the Legal, and the Law-Jobs: The Problem of Juristic Method*. The Yale Law Journal 1940, vol. 49, no. 8, pp. 1355–1400. Retrieved April 17, 2023 from https://www.jstor.org/stable/792545.

Llewellyn K. N., *The Normative, the Legal, and the Law-Jobs: The Problem of Juristic Method*, Yale Law Journal, 1940, vol. 49, p. 1355.

Lloyd I. J., *Information Technology Law*. 9th edition, New York 2020.

Lobel O., *Talent Wants to Be Free: Why We Should Learn to Love Leaks, Raids, and Free Riding*, New Haven 2013.

Lohsse S., Schulze R. , Staudenmayer D., *Data as Counter-Performance - Contract Law 2.0?*: *Münster Colloquia on EU Law*, Baden-Baden 2020.

Lynskey O., *The Foundations of EU Data Protection Law*, Oxford 2016.

Mayer-Schönberger V., *Delete: The Virtue of Forgetting in the Digital Age*, Princeton 2009.

Mehrotra A. K., *Law and the "Other": Karl N. Llewellyn, cultural anthropology, and the legacy of The Cheyenne Way*. Law & Social Inquiry 2001, vol. 26, no. 3, pp. 741-775.

Mendel T., Puddephatt A., Wagner B. [et al.], *Global Survey on Internet Privacy and Freedom of Expression*, Paris 2012.

Mill J. S. , *On Liberty*. London, New York, [189-?].

MongoDB Privacy Policy. Retrieved December 30, 2022 from https://www.mongodb.com/legal/privacy-policy.

Moore A. D., *Defining Privacy*, Journal of Social Philosophy 2008, vol. 39, no. 3, pp. 411-428. Retrieved July 11, 2021 from https://ssrn.com/abstract=1980849.

Murray M., *Information Technology Law: The Law and Society*, Glasgow 2016.

Neier A., *The International Human Rights Movement: A History*, Princeton 2012.

Nielsen A., *Practical Fairness. Achieving Fair and Secure Data Models*, Sebastopol 2021.

Parent W. A., *Privacy, Morality, and the Law*, Philosophy & Public Affairs 1983, vol. 12, no. 4 , pp. 269-288. Retrieved August 7, 2021 from www.jstor.org/stable/2265374.

Patterson A., *A Companion to Philosophy of Law and Legal Theory*, Oxford 2010.

Phillips-Wren G., Ichalkaranje N., Jain L., *Intelligent Decision Making: An AI-Based Approach*, Studies in Computational Intelligence, Berlin 2008.

Posner R. A., *How Judges Think*, Cambridge 2008.

Posner R.A., *Law, Pragmatism and Democracy*, Cambridge 2003.

Posner R. A. , *The Right of Privacy*, Georgia Law Review 1977, vol. 12, p. 393.

Pound R., *Interests in Personality*, Harvard Law Review 1914, vol. 28, 1915, p. 343.

Pound R., *Law in Books and Law in Action*, American Law Review 1910 , vol. 44, no. 1, pp. 12-36.

Pound R., *Mechanical Jurisprudence*, Columbia Law Review 1908, vol. 8, no. 8, pp. 605–623. Retrieved April 17, 2023 from https://www.jstor.org/stable/1108954 .

Pound R., *Task of Law:The North Law Lectures*, Lancaster 1944.

Pound R., The Spirit of the Common Law. Francestown, New Hampshire, 1921. Retrieved April 17, 2023 from https://core.ac.uk/download/pdf/188047771.pdf .

Pound R., *Social Control Through Law*, New Haven, London 1942.

Pound, R. *Law in Books and Law in Action*. American Law Review 1910, vol. 44, no. 1, pp. 12-36.

Prawa człowieka w Stanach Zjednoczonych, L. Pastusiak (Ed.), Warszawa 1985.

Prawa i wolności obywatelskie w Konstytucji RP, B. Banaszak, A. Preisner (Eds.), Warszawa 2002.

Preston W. C., *Backup & Recovery. Inexpensive Backup Solutions for Open Systems*, Sebastopol 1999.

Privacy and Identity Management. Fairness, accountability, and transparency in the age of big data. *13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers*, E. Kosta, J. Pierson, D. Slamanig, S. [et al.] (Eds.), Cham 2019. Retrieved April 17, 2023 from https://link.springer.com/book/10.1007/978-3-030-16744-8.

Privacy and the criminal law, E. Claes, A. Duff, S. Gutwirth (Eds.), Antwerp 2006.

Privacy: Nomos XIII, J. Roland Pennock, John W. Chapman (Eds.), New York 1971.

Rainey B., McCormick P., Ovey C., *Jacobs, White, and Ovey: the European Convention on Human Rights*, 8th Edition, Oxford 2021.

Ramos J.L.H., Skarmeta A., *Security and Privacy in the Internet of Things: Challenges and Solutions*, Amsterdam 2020.

Research Handbook on Modern Legal Realism, S. Talesh, E. Mertz, H. Klug (Eds.), Northampton, 2021.

Rucker D., Kugler T. , *New European General Data Protection Regulation. A Practitioner's Guide Enduring Compliant Corporate Practice*, Baden-Baden, 2018.

Ruis B. R., *Privacy in Telecommunications: A European and an American Approach*, Hague 1999.

Rule J. B., *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, Oxford 2007.

Saffady W., *Managing Information Risks: Threats, Vulnerabilities, and Responses*, Maryland 2020.

Salesforce Data Transfer Mechanisms Policy. Retrieved December 30, 2022 from https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-transfer-mechanisms-FAQ.pdf.

Satariano A., *'Right to Be Forgotten': Privacy Rule Is Limited by Europe's Top Court: The European Court of Justice said the landmark privacy law cannot be enforced beyond the European Union*. New York Times, Sept. 25, 2019, Sect. B, p. 1. Retrieved June 9, 2021 from https://www.nytimes.com/2019/09/24/technology/europe-google-right-to-be-forgotten.html.

Savin A., *EU Internet Law*, Third Edition, Cheltenham 2020

Sharma S., *Data Privacy and GDPR Handbook*, Hoboken 2020.

Siltala R., *Law, Truth, and Reason: A Treatise on Legal Argumentation*, 11th Edition. Dordrecht, New York, 2011.

Software As A Service (SaaS) Market Size [2023 Report]. Retrieved December 30, 2022 from https://www.grandviewresearch.com/industry-analysis/saas-market-report.

Somin I, *Thoughts on Judge Richard Posner's legal pragmatism*, The Washington Post 2017, September 2, Retrieved April 17, 2023 from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/09/02/thoughts-on-judge-richard-posners-legal-pragmatism/.

Stahl B.C., *Artificial intelligence for a better future: an ecosystem perspective on the ethics of AI and emerging digital technologies*, Cham.2021. Retrieved April 30, 2023 from https://doi.org/ 10.1007/978-3-030-69978-9.

The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (Eds.). Retrieved June 22, 2021 from https://plato.stanford.edu/archives/spr2018/entries/privacy/.

Szente Z. , Lachmayer K., *The Principle of Effective Legal Protection in Administrative Law: A European Perspective*, Routledge, New York 2009.

Thomson J. J., The right to Privacy, Philosophy & Public Affairs 1975, vol. 4, no. 4, pp. 295-314.

Thomson J. J., *The Right to Privacy*, Philosophy and Public Affairs 1975, vol. 4, no. 4., pp. 295-314. Retrieved April 18, 2020 from https://www.jstor.org/stable/2265075.

Timmons M. , *Oxford Studies in Normative Ethics*, vol. 9, Oxford 2019.

Ticher P. , *Data Protection and the Cloud: Are the risks too great?*, Cambridgeshire 2015.

Twinning W., *Karl Llewellyn and the Realist Movement*, Second Edition, Cambridge 2012.

Ulrich G., Ziemele I., *How International Law Works in Times of Crisis*, Oxford 2019.

The UN Convention on the Rights of Persons with Disabilities: A Commentary, I. Bantekas, M. A. Stein, [et al.] (Eds.), Oxford,New York 2018.

Verdun-Jones S.N., *The Jurisprudence of Karl Llewellyn*, Dalhousie Law Journal 1973, vol. 1, no 3, pp 441-481. Retrieved November 11, 2021 from https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1019&context=dlj.

Werro F., *The Right To Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia*, Washington 2020.

Wierczyński G., *Pound*, Sopot 2018.

Williams R., *Keywords: A Vocabulary of Culture and Society*, London 1988.

Zanfir-Fortuna G., *Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right* [In:] *Reforming European data protection law*, S. Gutwirth, R. Leenes, P. De Hert (Eds.), Dordrecht 2015, p. 6, Retrieved June 13, 2021 from https://ssrn.com/abstract=2501312.

Zych T., *W poszukiwaniu pewności prawa. Precedens a przewidywalność orzeczeń sądowych w tradycji prawa anglosaskiego*, Toruń 2017.

Legislative acts and case-law

Adequacy decisions. Retrieved March 24, 2023 from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents.

Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, 16/EN/WP242. Adopted on 13 December 2016. Retrieved April 31 July, 2022 from https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

BVerfG, Decision of Bundesverfassungsgericht on the constitutionality of the 1983 Census Act, 1BvR 209/83, May 1985. Retrieved April 19, 2020 from https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.

Charter of the United Nations, San Francisco 1945.

CJEU (Grand Chamber), Judgment, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* , Case C-311/18, July 2020, ECLI:EU:C:2020:791.

CJEU, Judgment (Grand Chamber), *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, Case C-311/18, July 2020. ECLI:EU:C:2020:559.

CJEU, Judgment (Second Chamber), *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, Case C-40/17, July 2019. ECLI:EU:C:2019:629.

CJEU, Judgement, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, September 2019. ECLI:EU:C:2019:773.

CJEU, Judgement, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, September 2019. ECLI:EU:C:2019:772.

CJEU, Judgment (Grand Chamber), *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*, Case C-210/16, June 2018. ECLI:EU:C:2018:388.

CJEU, Judgment (Grand Chamber), *Proceedings brought by Tietosuojavaltuutettu*, Case C-25/17, July 2018. ECLI:EU:C:2018:551.

CJEU, Judgment (Second Chamber), *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, Case C-398/15, March 2017. ECLI:EU:C:2017:197.

CJEU, Judgement, *Peter Nowak v Data Protection Commissioner*, Case C-434/16, December 2017. ECLI:EU:C:2017:994.

CJEU, Judgment (Third Chamber), *Verein für Konsumenteninformation v Amazon EU Sàrl*, Case C-191/15, July 2016. ECLI:EU:C:2016:612.

CJEU, Judgment (Second Chamber), *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, October 2016. ECLI:EU:C:2016:779.

CJEU, (Request for a preliminary ruling from the Audiencia Nacional — Spain), *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* C-131/12, May 2014, ECLI:EU:C:2014:317.

CJEU, Judgment (Third Chamber), *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, May 2014. ECLI:EU:C:2014:317.

CJEU, Judgement (Third Chambre), *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, Case C-141/12, July 2014. ECLI:EU:C:2014:2081.

CJEU, Judgement, *GFrantišek Ryneš v. Úřad pro ochranu osobních údajů*, Case C-212/13, December 2014. ECLI:EU:C:2014:2428.

CJEU, Application (OJ), *M and S*, Case C-141/12, September 2012.

CJEU, Judgment (Grand Chamber), *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, joined cases C-92/09 and C-93/09, November 2010. ECLI:EU:C:2010:662.

CJEU, Judgment (Third Chamber*), College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, Case C-553/07, May 2009, ECLI:EU:C:2009:293.

CJEU, Opinion of Advocate General, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, September 2015, ECLI:EU:C:2015:627.

CJEU, Opinion of Advocate General, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, September 2015, ECLI:EU:C:2015:627.

CJEU, Judgment, *J. R. Geigy AG v Commission of the European Communities*, Case C-52/69, July 1972. ECLI:EU:C:1972:73.

European Parliament and Council of the European Union, *Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council*. Official Journal of the European Union 2011, L 304/64.

Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg 1981.

Council of Europe, *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, Strasbourg 2015.

Council of the European Union, *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*. Official Journal of the European Union 1995, L 281/31.

Data Protection and Cloud Computing Framework. Retrieved March 24, 2023 from http://architectureportal.org/data-protection-and-cloud-computing-framework.

Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Adopted on 9 April 2014, 844/14/EN WP 217*. Retrieved March 24, 2023 from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm.

Data Protection Working Party, *Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, 00569/13/EN WP 203*. Retrieved April 31 July, 2022 from https://ec.europa.eu/ justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Data Protection Working Party, *Opinion 05/2012 on Cloud Computing, Adopted July 1st 2012, 01037/12/EN WP 196*. Retrieved June 20, 2022 from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

Directive (EU) 2016/680 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 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. Dz.U. L 119 z 4.5.2016. Retrieved April 17, 2023 from https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

European Parliament and Council of the European Union, *Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC*. Official Journal of the European Union 2003, L 41/26.

ECtHR, Judgment, *Węgrzynowski and Smolczewski v. Poland,* no. 33846/07, July 2013.

ECtHR, Application, *Ciubotaru v. Moldova*, no. 27138/04, April 2010.

ECtHR, Application, *Roche v. the United Kingdom*, no. 32555/96, October 2005.

ECtHR, Judgment, *Leander v. Sweden,* No. 9248/81, March 1987.

ECtHR, Application, *Rees v. the United Kingdom*, no. 9532/81, October 1986.

ECtHR, Decision, *Lundvall v. Sweden*, no. 10473/83, December 1985.

ECtHR, Application, *Klass and Others v. Germany*, nos. 5029/71, 5485/72, and 6234/73, September 1978.

Engraving Copyright Acts, London 1735.

Engraving Copyright Acts, London 1766.

European Commission, Commission Staff Working Paper, Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final, Annex 2, pp. 27. Retrieved April 31 July, 2022 from https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf.

European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Brussels*, Brussels 2020. Retrieved March 24, 2023 from https://edpb.euro U.S., Supreme Court, North Carolina, *Cora E. Wyatt And L. R. Wyatt v. W. S. Wilson And A. H. Martin (Wyatt v. Wilson)*, 67 S.E. 501 (N.C. 1910) 152 N.C. 276, March 1910.pa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*. Brussels 2018.

EWHC KB, *Decisions, John Entick, (Clerk) v Nathan Carrington and Three Others Messengers in ordinary to the King*, [1765] EWHC KB J98; 95 ER 807, November 1765. Retrieved December 13, 2021 from https://www.bailii.org/ew/cases/ EWHC/KB/1765/ J98.html.

SCC, Judgments, *Google Inc. v. Equustek Solutions Inc*., SCC 34, [2017] 1 S.C.R. 824, June 2017.

The Universal Declaration of Human Rights (UDHR), Paris 1948.

U.S. Constitution, Amendment I, December 15, 1791.

U.S., Supreme Court, The Ninth Circuit, *Olmstead v. United States*, 277 U.S. 438, February 1928. Retrieved December 19, 2021 from https://supreme.justia.com/cases/federal/us/277/438/.

U.S., Supreme Court, North Carolina, *Cora E. Wyatt And L. R. Wyatt v. W. S. Wilson And A. H. Martin (Wyatt v. Wilson)*, 67 S.E. 501 (N.C. 1910) 152 N.C. 276, March 1910.

U.S., Court of Appeals, New York, People v. Lochner, 177 N.Y. 145,69 N.E. 373, January 1904.

U.S. Supreme Court, Minnesota, *Northern Securities Co. v. United States*, 193 U.S. 197, no. 277, March 1904.

U.S., Court of Appeals, New York, The People Of The State Of New York Ex Rel. William J. Rodgers v. Coler, 59 N.E. 716,166 N.Y. 1, February 1901.

U.S., Supreme Court, New York, *Boyd v. United States*, 116 U.S. 616, December 1886. Retrieved December 13, 2021 from https://supreme.justia.com/cases/federal/us/116/616/.

U.S., Supreme Court, New York, *Pollock v. Farmers' Loan & Trust Co.*, 157 U.S. 429, no. 898, April 1895.

UK, Court of Appeal, *A Local Authority v A Mother and Others*, B4/2019/0291 [2019] EWCA Civ 799, May 2019.

UK, Court of Appeal, *NT1 and NT2 v. Google LLC*, HQ15X04128, HQ15X04127 [2018] EWHC 799 (QB). April 2018.

UK, Judgment, *Marion Manola v Stevens & Mayers*, [1901] 2 KB 102. July 1901.

UK, Judgment, *Pollard v Photographic Co*, 1888, 40 Ch Div 345, June 1888.

UK, Judgment, *Prince Albert v Strange*, [1849] EWHC Ch J20, January 1849.

UK, Judgment, *Abernethy v Hutchinson*, 1 HandTw 28, [1825] EngR 653, (1824-1825) 1 H and Tw 28, (1825) 47 ER 1313, June 1825.

UK, Judgement, *Gee v Pritchard*, [1818] EngR 605, (1818) 2 Swans 402, (1818) 36 ER 670, July 1818. Retrieved December 27, 2021 from http://www.commonlii.org/uk/cases/EngR/1818/605.pdf.

UK, Judgement, *Southey v Sherwood And Others*, [1817] EngR 351, (1817) 2 Mer 435, (1817), 35 ER 1006, March 1817. Retrieved December 13, 2021 from https://vlex.co.uk/vid/southey-v-sherwood-and-805313089.

United Nations General Assembly, *Universal Declaration of Human Rights*, 1948. Retrieved April 17, 2023 from www.un.org/en/about-us/universal-declaration-of-human-rights.