

Personal Data as a Market Commodity in the GDPR Era: A Systematic Review of Social and Economic Aspects

Aleksei Zelianin

D'Annunzio University of Chieti–Pescara, Pescara, Viale Pindaro, 42, 65122 Pescara PE, Italy

Corresponding author: Aleksei Zelianin (alekseizelianin@unich.it)

Abstract

With the development of modern data processing, mining and collection technologies, various companies and institutions will have more opportunities to make these data operations faster and more efficiently. From the economic perspective, processing personal data is evidently lucrative and companies would therefore like to obtain as much data as possible. This paper analyses and summarizes existing and emerging social and economic trends, implications and issues caused by clashes between European legislation on personal data protection (the GDPR) and current data processing practices. Utilizing both quantitative and qualitative data, the article attempts to scrutinize the implications of the conflict between the rising demand for privacy and personal data protection on the one hand and the ever-growing need to process and store personal data, especially by commercial organizations, on the other. Analysing databases, legislation, reports, statistical data and surveys, the paper attempts to provide an estimate of the value of personal data and the consequences of poor handling of personal data.

Keywords

General data protection regulation; Personal data; Digital marketing; Personal data protection; Personal data processing; Data breach.

Citation: Zelianin, A. (2022). Personal Data as a Market Commodity in the GDPR Era: A Systematic Review of Social and Economic Aspects. *Acta Informatica Pragensia*, 11(1), 123–140. <https://doi.org/10.18267/j.aip.168>

Academic Editor: Zdenek Smutny, Prague University of Economics and Business, Czech Republic

Copyright: © 2022 by the author(s). Licensee Prague University of Economics and Business, Czech Republic.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (CC BY 4.0).

1 Introduction

Those whose area of interest is somehow related to the flows of data on the Internet have most likely noticed many times how books, research studies, professors and media recognize data and specifically flow of personal data as the “new oil of the 21st century”, which is further confirmed by the sheer statistical data and facts presented in studies all across the world and in this article. Personal data have become valuable to an extent where they are called “the world’s most valuable resource” ahead of oil, because of how much they now inform the way companies communicate with their customers and how they positively impact on customer experience (The Economist, 2017). Indeed, the world is witnessing the triumphant march of information and communication technology (ICT) along with information technology (IT). With it, the data shift from the physical dimension to the digital. More than 5 billion people on Earth, which constitutes 65.6% of the world’s population, are Internet users (Internet World Stats, 2021). The biggest online storage and service companies, such as Google, Amazon, Microsoft and Facebook, are estimated to store at least 1.2 million terabytes of data among them (Science Focus, 2021). That figure excludes other big providers such as Dropbox, Barracuda and SugarSync, and massive servers in industry and academia (Science Focus, 2021). With this information in mind, the situation on the market leaves little or no choice but to make the most of modern means of processing potential customers’ personal and sometimes even sensitive data. If one company refuses to employ digital means of data analysis, it will inevitably lose to another company that will take advantage of using them. Thus, massive and increasingly larger amounts of IoT (Internet of Things) and user-generated data are now stored and processed. In many aspects of life, the World Wide Web has made communication so fast and simple that in certain cases people think it has erased national borders. People can base their daily life around the Internet. One can relatively easily work and earn money on the Internet, socialize, educate, self-entertain and shop buying goods globally rather than locally (Peukert et al., 2020).

Considering these circumstances from the business or economic perspective, it is not surprising that most companies are aspiring to obtain, analyse and use personal data to their advantage. However, since personal data are gathered and processed in increasingly large amounts employing sophisticated, sometimes questionable ways, data protection non-governmental organizations (NGO) are able to identify cases of illegal data storage and processing and, consequently, criticize entities that process personal data in dubious ways. The most famous NGO dealing with personal data protection is NOYB – European Centre for Digital Rights. The founder of the organization, Maximillian Schrems, won the case called “Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (“Schrems II”) – Case C-311/18” (European Parliament, 2020). The judgment was presented on 16 July 2020. According to the judgment, “European data protection authorities must stop transfers of personal data made under the standard contractual clauses by companies, like Facebook, subject to overbroad surveillance” (European Parliament, 2020). Shortly after the GDPR became effective on 25 May 2018, NOYB filed complaints against Facebook and its subsidiaries WhatsApp and Instagram, as well as Google LLC (targeting Android), for allegedly violating Article 7 of the GDPR. Based on the complaint, the French data protection authority CNIL (Commission nationale de l’informatique et des libertés) issued a fine of €50 million against Google LLC (CNIL, 2019). The cases of unravelling the mechanisms behind unlawful profiling and data processing, especially on the large scale, resonate with society’s sense of privacy and individuals start valuing their personal data privacy more. This, in turn, leads to an important trend – governments and society, in general, are increasingly concerned about privacy and the ways to protect personal data.

Correct and efficient development and implementation of modern technologies are crucial in the competitive sector. Technologies such as blockchain, artificial intelligence (AI) and cloud computing are enabling companies to be competitive and help boosting performance, productivity and efficiency. More than that, security automation solutions – including AI, analytics and orchestration – and incident

response preparedness, including the formation of incident response teams and testing of incident tackling plans, have shown the greatest reduction in data breach costs (IBM, 2020). Companies employ cutting-edge technologies to store and process personal data in the most efficient way possible or simply make mistakes, especially while using technologies such as AI on a large scale. It is necessary to consider that companies pursuing financial benefit at its core objective might be more interested in their revenues than in the individual's right to privacy and might obtain and use personal data in illegal ways deliberately or by mistake. Statistics demonstrate a surge in the number of fines and the overall sum of fines for non-compliance with the GDPR (see Figures 2 and 3). However, with adequate legislation, fines and rising public awareness, illegal ways of obtaining and processing personal data are becoming more visible to society and result in heavy fines and reputational damage as demonstrated in this paper. In Europe, the General Data Protection Regulation (GDPR) is the main law that regulates the personal data processing boundaries for big companies.

Designed to be the cornerstone of the European online privacy regime, the GDPR was adopted on 14 April 2016, becoming effective on 25 May 2018, and is often considered the most comprehensive, state-of-the-art, globally leading privacy legislation. The GDPR has an extraterritorial reach meaning that according to Article 3 and Recitals 22 to 25 of the GDPR, as a non-EU organization you can fall in the scope of the GDPR when you are offering goods or services to individuals in the EU (Regulation (EU) 2016/679). Indeed, due to its extraterritoriality, it has had a very strong influence not just on Europe's online privacy regime, but on the rest of the world as well. Considering that the Internet is practically a space without conventional borders, data are sold, purchased, stored and processed globally rather than locally. The GDPR has replaced the 1995 Data Protection Directive, which was adopted at a time when the Internet was in the early stages of its existence, and, unlike the GDPR, it was a directive, meaning it did not have a binding legal force. It only provided specific rules and results that must be achieved, but each Member State is free to decide how to transpose directives into national laws. After the GDPR became effective in 2018, there has been a rising trend of increasing concern for data privacy in Western societies, which will be further analysed in the article. Naturally, as a logical response, companies, small or large, are seizing the rising demand for privacy and emphasizing their aspiration for user privacy more often in their policies and marketing campaigns. The issue of preserving privacy on the Internet is becoming more and more prominent: people are more concerned about the security of personal data, and platforms, in response, are introducing new technologies for protecting personal information. In recent years, a number of technologies have emerged that have influenced the usual mechanics of the advertising market. One of the brightest examples is Apple (one of the world's largest technology companies by revenue and, since January 2021, the world's highest market capitalization company), which launched a series of advertisements in May 2021 with the slogan "Privacy. That's iPhone". Additionally, Apple announced the launch of the Intelligent Tracking Prevention (ITP) system built into Safari – from version 2.1, it blocks all third-party cookies in the browser by default. Essentially, the ITP has deprived advertisers of the ability to use third-party cookies to track the interests of Safari users and target ads to the right audiences.

Considering the aforesaid, the main focus of the paper is to analyse and summarize existing and emerging social and economic trends, implications and issues caused by clashes between European legislation on personal data protection (the GDPR) and current data processing practices. The following questions are addressed: "How does the GDPR tackle the issues caused by the demand for data storage and processing?" "What are the social trends in the context of conflict between personal data protection and the ever-growing demand for personal data processing?" and "How valuable are personal data to companies and what are the consequences of poor data handling?" The paper attempts to answer these questions and provides qualitative research results by analysing both quantitative and qualitative secondary data.

2 Research Methods

2.1 Data collection

The data for this study include surveys, reports, relevant statistical data, international publications and legislative acts of the EU relevant to the topic of social and economic aspects of personal data processing in the EU. However, since this topic cannot be studied comprehensively without the context of modern personal data processing technologies, such technologies are also scrutinized in the present study. All databases, registers, websites, organizations and publications as well as the date when each source was last searched or consulted are specified in the reference list. The search strategy included screening sources indexed by academic databases (Web of Science, Scopus, etc.) using the bibliometric analysis method and reports of leading consulting and cybersecurity companies. The keywords were used as search words in order to reach the most relevant and distinguished articles. Since the implementation of the GDPR (which became effective on 25 May 2018) is crucial to the study, articles between 2018 and 2021 were given a high priority. However, to study the changes between pre- and post-GDPR legislation, a small quantity of sources dated earlier than 2018 were used as well.

2.2 Data analysis

The secondary data are analysed using the following methods: a content analysis of surveys and reports provided by studies and reports of management and security consulting companies.

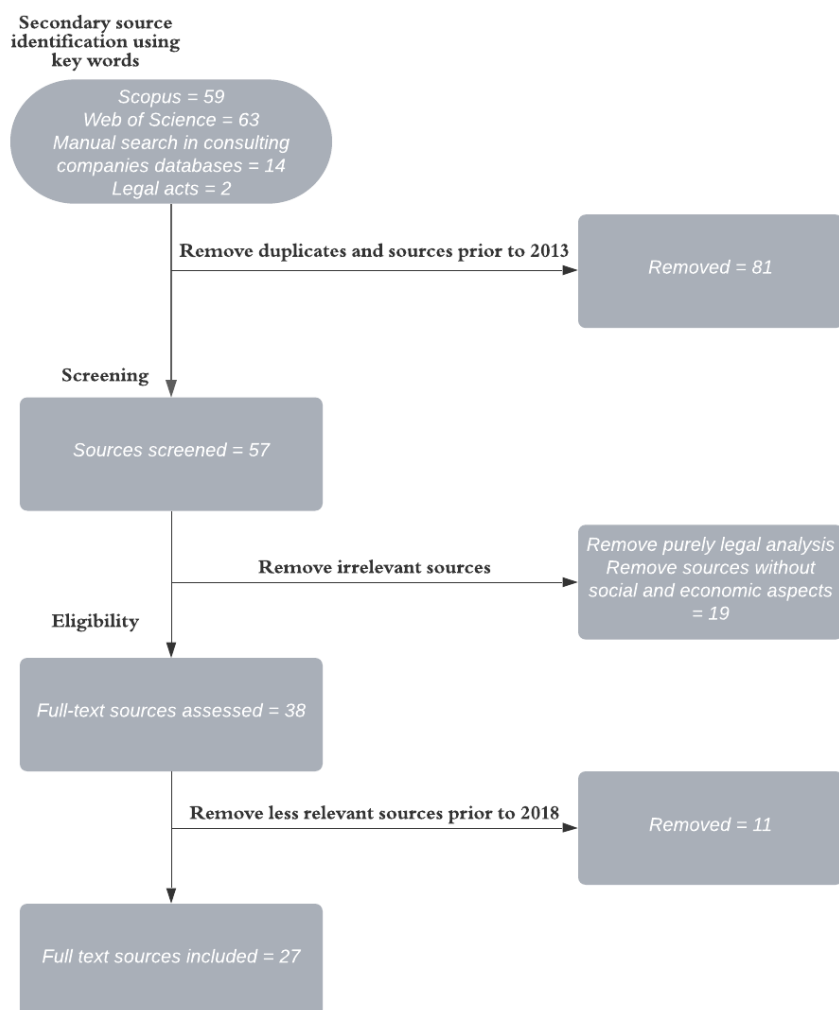


Figure 1. Flow diagram: Identification, inclusion and exclusion of sources.

Predominantly, secondary data are analysed based on an assessment of statistical data, expert assessment and forecasting. To interpret and analyse a complex interrelation between different aspects of modern personal data processing and collection, a systematic approach and descriptive statistics are used in the paper. Document analysis is used when addressing data from the database of the European Commission and other legal documents of the European Union. The keywords used for source identification are following: GDPR, personal data protection, digital marketing, data misuse, big data, user trust, personal data market, data breach.

The text sources include information presented by think tanks, relevant journals, groups of academic researchers, documents and studies by EU institutions, reports and surveys conducted by private organizations and large companies dealing with personal data. The risk of bias exists since individually some of these sources present data predominantly from one perspective. However, including sources with competing interests allows building a comprehensive picture and thus comparing and identifying biased information (see Figure 1).

3 Research Results

3.1 Internet economy and GDPR

Topics, data and results of the chosen and analysed sources are briefly summarised in the following table. It is followed by an interpretation and analysis of the interrelation of different data sources.

Table 1. Summarized social and economic trends of sources included in paper.

Row	Title	Brief summary of social/economic trends
1	The impact of the General Data Protection Regulation on Internet interconnection. (Zhuo et al., 2021)	<ul style="list-style-type: none"> - Available empirical evidence confirms a reduction in personal data usage in the European Economic Area relative to other markets. - Economic dominance on the market is exercised through control over personally identifiable information that can be further monetized.
2	Consumer Privacy Survey. The growing imperative of getting data privacy right (CISCO, 2019)	<ul style="list-style-type: none"> - 61% of the individuals engaged in data protection issues are under the age of 45 - 83% of respondents care about their privacy - 80% are willing to act to protect personal data - Majority of the respondents believe government should be held accountable for protection of data privacy
3	GDPR Enforcement Tracker Report 2021 (CMS, 2021)	<ul style="list-style-type: none"> - The biggest fine under the GDPR up to this date is €746,000,000 - Overall sum of GDPR fines has surged rapidly since May 2021 - Overall cumulative number of GDPR fines is on the rise
4	Privacy, Data Breach, and Reputation Management (Data Privacy Manager, 2020)	<ul style="list-style-type: none"> - Data breaches cause companies to suffer reputational damage - Large quantities of resources must be allocated to tackle the consequences of a data breach
5	The Value of Personal Online Data (ENISA, 2018)	<ul style="list-style-type: none"> - Personal data analysis has become widely used by various businesses - Estimated average revenue per user reached \$59 in 2017 - Personal data analysis is important not only to businesses but also to societies in general
6	Blockchain and the General Data Protection Regulation (European Parliamentary Research Service, 2019)	<ul style="list-style-type: none"> - Tensions between the GDPR and emerging technologies exist (specifically blockchain) - Case-to-case analysis is required when using a blockchain to store and/or process personal data

Row	Title	Brief summary of social/economic trends
7	The New Deal on Data: A Framework for Institutional Controls (Greenwood et al., 2014)	<ul style="list-style-type: none"> - Digital footprints left by Internet users are valuable since combined they contain a variety of information about users - Personal data processing can be used for the public good and for financial benefits
8	The European Union general data protection regulation: what it is and what it means (Hoofnagle et al., 2019)	<ul style="list-style-type: none"> - The GDPR is the most consequential regulatory development in information policy in a generation - The GDPR encourages firms to develop information governance frameworks - The GDPR will complicate and restrain some information-intensive business models
9	Annual Governance Report 2019 (IAPP, 2019)	<ul style="list-style-type: none"> - Majority (90%) of companies prefer to delegate data processing to third parties - The most difficult GDPR obligation to fulfil by the companies is the right to erasure (right to be forgotten)
10	How much does a data breach cost? (IBM, 2020)	<ul style="list-style-type: none"> - Adequate data breach response preparedness reduces significantly the damage caused by a data breach - \$3.86 million is the average total cost of a data breach
11	The future of online privacy and the security of personal data (IFLA, 2019)	<ul style="list-style-type: none"> - In a globalized world it becomes ever more challenging to ensure uniform standards of privacy - Current levels of trust in the online world may eventually plateau or even decrease significantly
12	Google: annual advertising revenue 2001-2019 (Statista, 2020)	<ul style="list-style-type: none"> - Digital advertising profits are constantly on the rise - Majority (70.9%) of the revenue of Google comes from digital advertising
13	European privacy law and global markets for data (Peukert et al., 2020)	<ul style="list-style-type: none"> - An increase in market concentration in web technology services after the introduction of GDPR - While most firms lose market share, the leading firm, Google, increases market share significantly
14	Regulatory export and spillovers: How GDPR affects global markets for data (Peukert et al., 2020)	<ul style="list-style-type: none"> - The market for web tracking technologies became more concentrated - Websites reduce their use of third-party web technology providers after the GDPR - The GDPR has expanded the de facto territorial reach of European privacy laws beyond the geographical boundaries of the EU
15	The Impact of data breaches on reputation & share value (Ponemon, 2017)	<ul style="list-style-type: none"> - Data breach is a top threat to companies' reputation and brand value according to IT specialists - Data breaches and weak data protection measures lead to stock value losses - Companies with adequate security measures are much more resilient to reputational damages
16	Building a Blockchain Application that Complies with the EU General Data Protection Regulation (Rieger et al., 2019)	<ul style="list-style-type: none"> - There is no unanimous solution to using blockchain to store and process personal data - Complying with the GDPR poses significant challenges for blockchain projects - There are several possible solutions to using blockchain to store and process personal data
17	Q3 2019 Data Breach QuickView Report (Risk based security, 2019)	<ul style="list-style-type: none"> - After the GDPR became effective there has been a surge in reported data breaches in the EU
18	How much data is on the Internet? (Science Focus, 2021)	<ul style="list-style-type: none"> - The amount of personal data on the Internet is constantly on the rise

Row	Title	Brief summary of social/economic trends
		- According to the estimations, the trend of accumulation of personal data online will continue
19	GDPR survey. Benefits beyond compliance (Backer McKenzie, 2020)	- GDPR compliance requires a budget and strong sponsorship - To achieve GDPR compliance, it is important to nurture a data culture, clarify data governance and improve its management, security standards and process effectiveness
20	Be transparent on social media or risk the consequences (The Chartered Institute of Marketing, 2016)	- Majority of consumers (58%) do not trust brands to handle their data responsibly - Businesses are increasingly employing questionable digital marketing methods
21	The world's most valuable resource is no longer oil, but data (The Economist, 2017)	- Modern economy has become data-driven - Large companies are able to seize profits from digital advertising comparable to profits of oil companies
22	Global Privacy Benchmarks Report 2021 (TrustArc, 2021)	- 83% of enterprises have employed formal data protection measures and privacy offices - Privacy is becoming one of the top priorities for companies - With growing threats, companies are enhancing their data protection strategies
23	Bridging the Trust Gap in Personal Data (Boston Consulting Group, 2018)	- Users tend not to trust companies that were previously accused of mistreating personal data - Companies without appropriate personal data protection policy risk jeopardizing their revenues while companies having such policy are reaping benefits
24	Big Data and Analytics in the Age of the GDPR (Bonatti and Kirrane, 2019)	- Apart from free exploratory data analysis, explicit consent is the most flexible and safest legal basis - Personal data processing allows companies to use the data in a great variety of ways, from predicting consumer demand to regulating and adjusting prices
25	Personal data markets (Spiekermann et al., 2015)	- Internet economics is data-driven - Data value to companies is on the rise
26	Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR (Golla, 2017)	- Coordination of data protection authorities in all EU member states is the key to an effective data protection regime - The GDPR has the potential to become a very important step towards an effective data protection regime
27	Benefits of Targeted Advertisements: A Spotify Fail (Keating, 2016)	- More information allows advertisers to be more efficient - While consumers benefit from appropriate targeted advertising, advertisers benefit more

Companies can now face severe fines for non-compliance with the GDPR. The GDPR's predecessor, Data Protection Directive 95/46/EC does not specifically mention or require administrative fines for data protection violations. However, most EU member states have implemented such sanctions in their Data Protection Acts (Golla, 2017). The maximum fine amount differed greatly from one country to another. While Romanian law (maximum €11,000) and Slovenian law (€12,510) allow for relatively low fines, Spanish (€600,000) and UK laws (£500,000) had much higher thresholds (Golla, 2017). However, even the highest fine thresholds under Data Protection Directive 95/46/EC are sometimes 1000 times lower compared to fines under the GDPR. Under the GDPR, the EU's data protection authorities can impose fines of up to up to €20 million, or 4 percent of worldwide turnover for the preceding financial year (Regulation (EU) 2016/679). The biggest fine under the GDPR up to date is €746,000,000, imposed on Amazon (GDPR Enforcement Tracker, 2021). The overall sum of fines surged rapidly recently, after May

2021. Both sum and number of fines have been increasing since February 2019. The following figures demonstrate the dynamics, sum and number of fines under the GDPR.

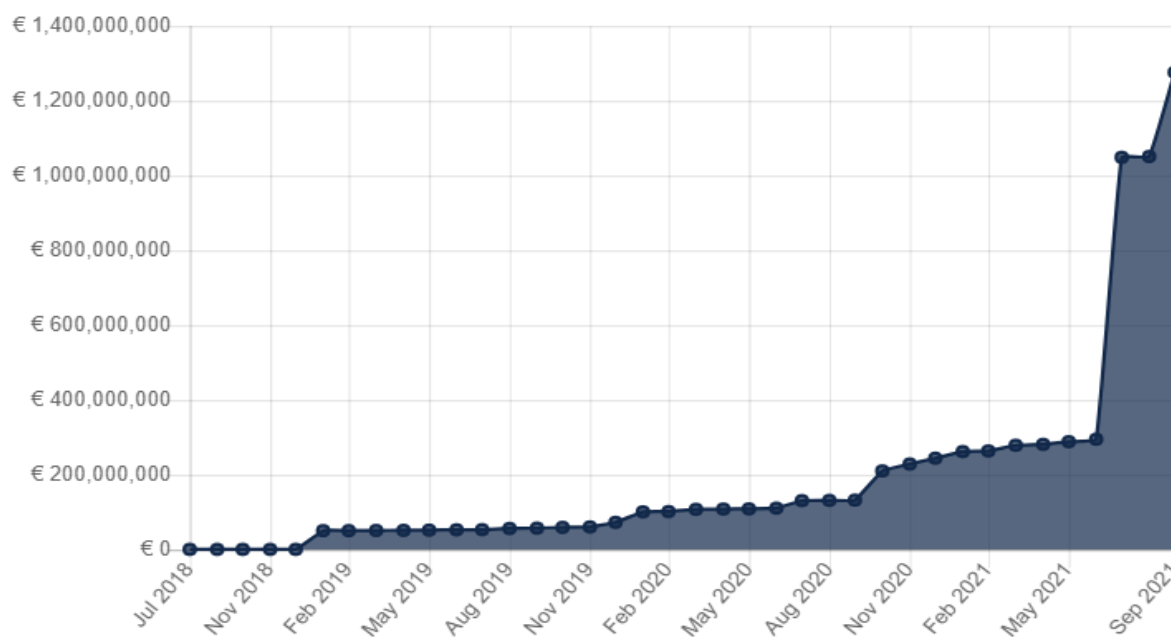


Figure 2. Overall sum of GDPR fines (cumulative). Source: (GDPR Enforcement Tracker, 2021).

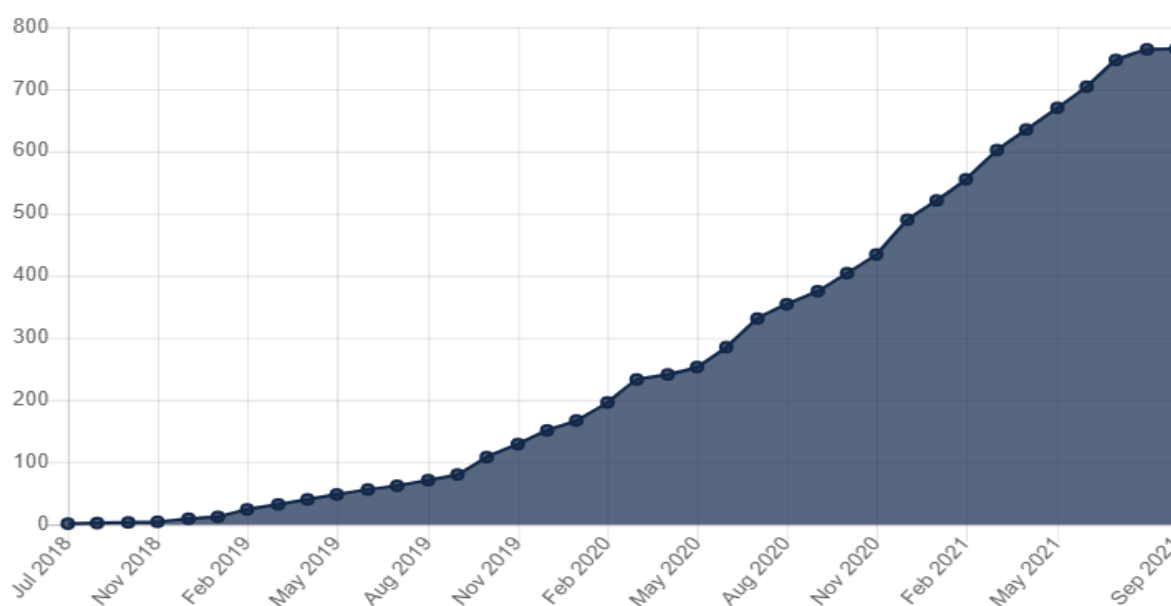


Figure 3. Overall number of GDPR fines (cumulative). Source: (GDPR Enforcement Tracker, 2021).

The era of digitization and emerging technologies (blockchain, big data, cloud computing, etc.) provides new, sometimes controversial possibilities to utilize these technologies in order to benefit from them. From the economic perspective, processing personal data is evidently lucrative and companies therefore want to obtain as many data as possible. In Europe, the GDPR acts as the main constraint to the ever-growing demands of companies to store and process personal data. However, the GDPR is a relatively new regulation and a number of researchers state that some articles of the Regulation (especially regarding the use of new data processing technologies) are ambiguous and require very profound consideration. For instance, the European Parliamentary Research Service published a study in 2019

regarding using blockchain technology to process and store data, called “Blockchain and the General Data Protection Regulation”. The study concludes that the compatibility of blockchain instruments with the Regulation can only ever be assessed on a case-by-case basis (EPRS, 2019). Moreover, technologies that allow more efficient processing of personal data (including blockchain) are constantly developing and therefore changing.

As summarized by Greenwood, the “digital breadcrumbs” that we leave behind are clues to who we are, what we do and what we want (Greenwood et al., 2014). This makes personal data extremely valuable, both for the public good and for private companies (Greenwood et al., 2014). However, due to the high value of personal data and digital footprints, they are vulnerable to theft, misuse and many other ways of abuse involving modern technologies. It leads to consumers’ demand to be informed on how their personal data are stored and processed by companies. With the rising media attention to privacy issues and an ever-growing number of cases of data breaches, people are rapidly losing faith in the measures that companies employ to protect their personal data. According to one of the studies conducted by TRUSTe/NCSA, 92% of online customers consider data security and privacy as a concern (TrustArc, 2021). Another report by the Chartered Institute of Marketing found out that 58% of consumers do not trust brands to use their data responsibly (Chartered Institute of Marketing, 2016). However, not only consumers demonstrate concerns about compliance with data protection measures, especially before the implementation of the GDPR. Several pieces of research have been made to investigate whether businesses are well prepared to take measures and protect their customers’ personal data. Statistical data on European privacy show that 65% of respondents struggled to implement the GDPR due to lack of resources, and 60% of respondents had difficulty establishing their level of risk (Backer McKenzie, 2020). Only 54% of respondents stated that internal procedures had been implemented and the status of the GDPR compliance project was considered finalized and was being maintained (Backer McKenzie, 2020).

The GDPR sets out some key principles regarding data processing: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; accountability (Regulation (EU) 2016/679). These principles are the sets of obligations to be achieved by companies involved in data processing. However, in some cases, the GDPR does not provide clear instructions on which actions and technologies are permissible and which are not, especially in cases related to utilization of modern IT technologies. Besides the imperfection of the GDPR itself, there are other reasons for that. The main one is that the IT industry develops rapidly and new technologies emerge. Some of these technologies are perfectly compliant with the GDPR, some are not, but most of them can be used in both a compliant and a non-compliant manner. The legislators who were designing the GDPR most likely realized that the world has entered an era when data mean power and industries and data-driven. The economic importance of data allows some researchers to say that economic dominance on the market “does not manifest through firms’ ability to dictate prices and/or raise entry barriers, but rather through control of vast amounts of personally identifiable information (or privacy-relevant data) that may either be monetized through fine-grained targeting of consumers or reselling the data to third parties for their own targeting and personalization efforts” (Zhuo et al., 2020).

In this regard, it is important to mention some of the terminology and key concepts. Some of the personal data are considered sensitive and require specific processing conditions. According to Articles 4 and 9, as well as Recitals 51 to 56 of the GDPR, the following personal data are sensitive: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person’s sex life or sexual orientation (Regulation (EU) 2016/679). Processing sensitive data always requires appropriate safeguards. Exceptions that allow processing of sensitive data are stated in Article 9 of the GDPR and can be divided into the following categories: explicit consent; employment, social security and social protection; vital interests; not-for-profit bodies; information made public by the

data subject; legal claims or judicial acts; public interest; health or social care; public health; archiving, research and statistics.

Inappropriate handling of personal data by businesses was one of the main reasons to develop and implement the GDPR. With the GDPR enforced and its concepts of data protection by design and data protection by default, companies are now required to design their websites and products with built-in privacy protection and have data privacy protection settings switched on by default. At the same time, with the GDPR the EU has set very high standards for digital privacy. With stricter regulations on data handling and processing, it has become more difficult for organizations to benefit from the massive amount of data processed with the means of modern data processing technologies and remain GDPR-compliant at the same time. One of the tasks of the GDPR is to set legal boundaries for these companies and ensure that the personal data protection regimes are unified to a great extent across the EU.

According to the GDPR, 'personal data' means "any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Regulation (EU) 2016/679). 'Processing' means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Regulation (EU) 2016/679). The GDPR introduces several boundaries and principles to limit companies' ability to process personal data and give control to the consumers. First is the notion of consent, which is very important in this context. Consent must be freely given, specific, informed, unambiguous and revocable in order to prevent firms from using long and inaccessible consent processes to obtain personal data (Hoofnagle et al., 2019). The purpose limitation principle states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Regulation (EU) 2016/679). This principle is there to make sure that the reasons for obtaining personal data are clear and open, and will not exceed the boundaries of the user's expectation of why his/her data are being processed. It also helps individuals understand how companies use their data and would limit companies' ability to further process data in unanticipated ways for purposes different from the original ones (Zhuo et al., 2020). Another important fact is that companies that do not comply can face fines of up to €20 million or 4% of their global turnover (Regulation (EU) 2016/679). The GDPR provides six legal bases for processing data: consent, contract, legal obligation, vital interests, tasks in the public interest, legitimate interests. Companies primarily chose consent or legitimate interests to process personal data (Deloitte, 2019). Given that digital marketing is always optional, all companies are aspiring to receive permission to collect and process data.

With these changes, most companies that operate online have changed their marketing strategies. The trend of individual privacy awareness is on the rise, especially in the case of younger people, and businesses are now therefore more likely to demonstrate that they prioritize and care more about their clients' personal data and have to design their products and websites accordingly. According to CISCO data, the majority (61%) of individuals who are engaged in their data protection issues are under the age of 45 (Consumer Privacy Survey, 2019). This constitutes one of the principal reasons why in the future privacy awareness will have even more significance to governments and companies. The same survey by CISCO reveals that an even bigger percentage (83%) of respondents care about privacy and their data safety and want to have more control over the ways in which their data are used (Consumer Privacy Survey, 2019). Eighty percent of the respondents also stated that they are willing to act to protect their data privacy (Consumer Privacy Survey, 2019). On the other hand, the majority of the respondents distrust

handling of their personal data by the companies (Consumer Privacy Survey, 2019). They stated that they are not aware of the ways in which they can protect their personal data (Consumer Privacy Survey, 2019). The figure below demonstrates that the majority of the respondents claims that it is the responsibility of a government to protect privacy and personal data. Less frequent is the opinion that individuals and companies should be held responsible.

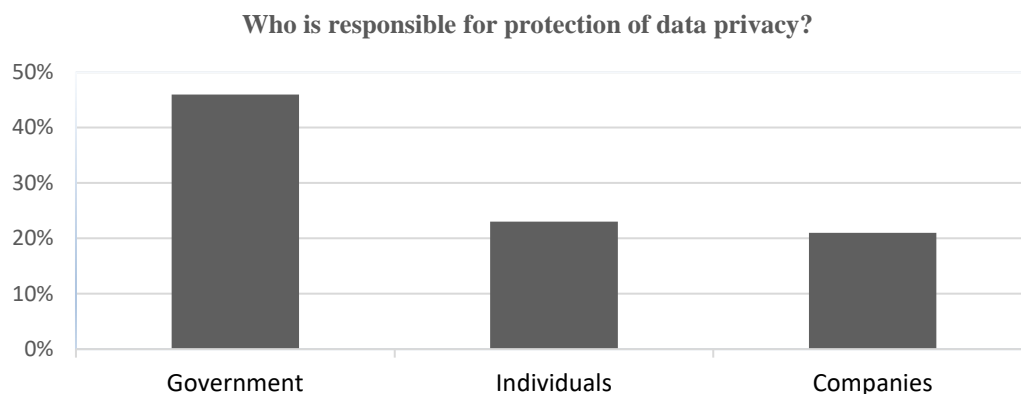


Figure 4. Protection of data privacy survey. Source: (CISCO, 2019).

Data from another report (see Figure 5) demonstrate that companies claim the right to be forgotten (also known as the right to erasure) to be the most difficult GDPR obligation to fulfil. The right to erasure is specifically mentioned in the GDPR. The conditions upon which the right to erasure can be fulfilled are specified in Article 17 of the GDPR. These conditions include: the personal data are no longer necessary for the original purpose of data collection; an organization is processing personal data for direct marketing purposes and the individual objects to this processing; an organization is relying on an individual's consent as the lawful basis for processing the data and that individual withdraws their consent, etc. (Regulation (EU) 2016/679). Indeed, besides the fact that the right to be forgotten is technically difficult to fulfil by most of the companies, critics also argue that it could lead to numerous cases of erasure of content that already exists online. This, in turn, can be seen as an assault on the freedom of expression and other human rights. The advancement of new technologies used to store data, such as blockchain, pose even more challenges to that: blockchain is designed precisely to record everything permanently; therefore, it renders it technically impossible (or extremely hard at the very least) to eliminate a record of a transaction or other data stored in the blockchain.

The topic of blockchain technology usage has been vague yet important. The 2019 study "Blockchain and the General Data Protection Regulation" by the European Parliamentary Research Service states that indeed many tensions between GDPR and blockchain exist, yet there are ways to reduce these tensions. It includes several recommendations for how to apply blockchain and ensure it is GDPR compliant. Firstly, new and improving techniques might help ease the tensions since these new techniques allow for data to be removed from blockchains when they are no longer needed. The study suggests that the best practice is to store all personal data "off-chain" which can then be linked back to the ledger by a hash (EPRS, 2019). Whether this hash (which cannot be deleted from the ledger) constitutes personal data is still unclear (EPRS, 2019). Secondly, a blockchain solution that needs to process personal data should use a private and permissioned pseudonymization approach (Rieger et al., 2019). This solution would store information with a high degree of security. Moreover, such an approach would make it easier to identify controllers since all those who possess additional information required for attribution qualify as controllers. Thirdly, a blockchain solution that needs to coordinate cross-organizational workflows should use a private and permissioned pseudonymization approach with identifier mapping (Rieger et al., 2019). Essentially, this approach provides the best balance between security and compliance.

In order to make data serve one's interest, they need to be processed. Usually, companies (data controllers) delegate the work related to data processing to third parties. The percentage of companies delegating data processing to third parties constitutes 90% (IAPP, 2020). To ensure that the necessary data protection measures are in place, they rely on the assurances in contracts made with these third parties (IAPP, 2020). Apparently, the GDPR architects took this phenomenon into consideration. Under the previous Data Protection Directive 95/46/EC only controllers were accountable for data protection noncompliance. With the GDPR, both processors and controllers can be held accountable for the noncompliance. According to Article 83 of the GDPR, in the case of non-compliance, fines can be applied to both controllers and processors (Regulation (EU) 2016/679). These fines shall be imposed regarding “the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them (Regulation (EU) 2016/679).”

What are the most difficult GDPR obligations in 2019

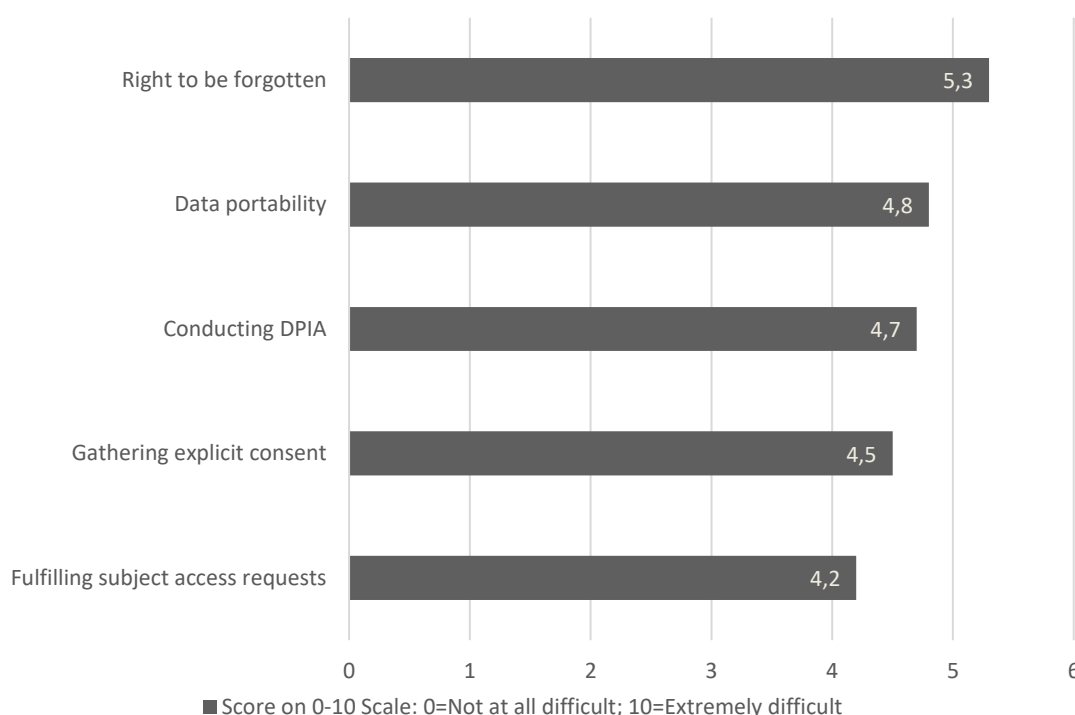


Figure 5. Most difficult GDPR obligations in 2019. Source: (IAPP, 2019).

However, one cannot build a marketing strategy efficiently without data since data collection lies at the core of marketing activities. Marketing specialists tend to use increasingly personalized data to increase sales, gather leads, improve customer experience and be more efficient overall. One of the most efficient types of advertising is targeted and location-targeted advertising since it allows using data in order to deliver advertisements in a very precise manner, specifically tailoring advertisements to customers' preferences or predicted online behaviour. The most common way to obtain personal data for these purposes is through free online services. The brightest examples are Facebook and Alphabet Inc. (previously known as Google). Both companies, in one way or another, use personal data acquired from their users for their benefit. Mostly, they analyse and process personal data in order to advertise more efficiently. In 2019, advertising accounted for the majority of Google's total revenue, which amounted to a total of 160.74 billion US dollars. In the most recent fiscal period, advertising revenue through Google Sites made up 70.9 percent of the company's revenues (Statista, 2020).

Originally, the scope of targeted ads was to advertise products suitable to the preferences of a specific individual. In other words, advertisers want to put their commercials in front of people who may be interested in these commercials and thus aligning the interests of both sides. That way, both the consumer and the company that sells the product are satisfied. From an economic perspective, targeted advertising is very efficient and beneficial to the advertiser due to the reduced resource costs and ability to create a strong appeal to the product. The reduced costs come from minimizing inefficient or useless advertisements shown to the potential customer. Due to their properties, such advertising is able to captivate a customer's attention and thus result in a higher return on investments in the marketing campaign. Behavioural advertising is used to accurately determine potential customers' purchasing habits and preferences, making the advertisements more suitable to consumers. The more information, including personal data, the advertiser has, the more efficient the advertising can be and the advertising campaign development can improve: by having information about the consumer, the advertiser is able to make more concise decisions on how to best communicate with them (Keating, 2013).

Constantly developing technologies allow advertisers on the Internet to pierce and target consumers on a larger scale and more efficiently compared to traditional media (Bergemann and Bonatti, 2011). In most cases, individuals are not fully aware of the ways in which their data are being processed since they are not able to invest enough time in understanding the intricate background and data processing legislation and are not given oversight over how their personal data are used to draw inferences about them. In this regard, great examples illustrating the influence of modern technologies on data processing are big data analytics (BDA) and AI.

For companies, researchers and legislators, it is crucial to understand which technologies and methods can be used to process and store personal data and comply with the GDPR at the same time. However, due to the complexity of such technologies and the changing state of the art, clarifications and case-to-case analysis (as suggested by the European Parliamentary Research Service) are required in the majority of the cases where data are stored and processed using modern IT technologies.

3.2 Personal data value and privacy trend

Data are immensely valuable from a commercial perspective since they allow gaining a significant advantage on the market and winning the competition, which ultimately means success for the entrepreneurs. A good example to demonstrate the application of data processing technologies in this context is the retail sector. This sector has been using data processing technologies and data acquired with BDA as a tool that enables predictions about what, where, how, when and in what quantities consumers want to buy (Bonatti and Kirrane, 2019). For instance, BDA is also used by retailers to regulate the prices of their goods according to current demand and inventory. In the retail industry, as in many others, data processing technologies assist companies to adjust their online advertising to the preferences and demands of potential customers (Bonatti and Kirrane, 2019). The US retail chain Stage Stores uses big personal data for what is known as "markdown optimization, which tells merchants the best time to cut the price of a particular item in a particular store" (Bonatti and Kirrane, 2019).

Personal data analysis and collection are important for businesses but not less important for society in general: "policy decisions are taken based on personal data analysis and medical research using patients' and caregivers' data to improve healthcare are just a few examples" (ENISA, 2018).

Given that personal data are an extremely valuable asset to any company that wants to sell its product and therefore efficiently advertise it, successful companies rarely have an option to refuse to employ modern data processing technologies to mine and process personal data. Personal data markets thrive, driving online companies' valuation and fuelling Internet economics (Spikerman et al., 2015). According to the Boston Consulting Group, use of personal data can deliver up to EUR 330 billion in annual economic benefit to organizations in Europe alone by 2020 (Boston Consulting Group, 2018). Another estimation

made by ENISA states that data collection has become widely used in a large variety of businesses. The estimated average revenue per user in digital advertisement, mainly controlled by Google and Facebook, reached \$59 per person in 2017 (ENISA, 2018). If we multiply this number by an average of 3.8 billion active Internet users (the number is constantly growing), we can roughly estimate the size and value of digital advertisement-related businesses (ENISA, 2018). However, the majority of users are rarely aware of the monetary value of their personal data and sometimes not even aware of the fact their data are being collected very carefully. Ordinary individuals tend to underestimate their economic influence and, therefore, power over the companies. The situation where a person is not aware of their personal data value and passively accedes to the collection and further commodification of their data is very typical.

However, while there is competition on the market, consumers have various options to choose from. They can choose similar products provided by different companies and companies will have to compete to win the trust of the customers. In the context of data protection, the customer, *ceteris paribus*, will choose a company that cares more about the safety of personal data and processes the data in a legal, transparent way. Therefore, a company that methodically invest thoughts and efforts into building safeguards for the personal data it holds and can potentially acquire is doing it both for its own good and that of the customer, given that the customer preferentially chooses to buy products and services from this company and is willing to share relevant data with it. Relative examples proving this point of view and worth mentioning are the number of companies that have suffered reputational damage and have been appearing in newspaper headlines due to inappropriate treatment of personal data. Thus, these companies have suffered reputational losses for collecting and processing data in a way that distresses customers, without their awareness and permission. Subsequently, reputational losses lead to the distress of existing and potential customers, which in turn leads to financial losses and disapproval of stakeholders.

As a result, we can witness a trend towards privacy on the Internet. It indicates an increase in the level of users' awareness and responsibility. More people tend to use features or special browsers for anonymous Internet browsing that do not record user actions. Classic search engines such as Firefox or Chrome track requests and, when the user browses the site, they record the IP and MAC address. It is a unique combination of numbers and letters with a length of 48 characters: this is the hardware number of the equipment that goes online. The MAC address is assigned to the device's network card during manufacture at the factory. As soon as the provider connects the device to the network, it fixes its MAC address in the system and delivers traffic to it according to the installed package. It has been decades since users started using trackers and ad blockers. Trackers are a class of technologies that collect and store information about a user's online activities. Today these programs take many forms, use sophisticated tracking techniques and also significantly slow down page loading. They can be bypassed with user-friendly tracker blockers. Additionally, they hide some of the banner ads. This is because most of them are downloaded from third-party servers that track user transitions between sites.

However, the current level of users' trust in the online world could decline significantly. Many people still share significant amounts of personal information online (through social media or online activity tracking systems) voluntarily and sometimes carelessly, but it might change due to the privacy awareness trend. With the development of the Internet, people, especially younger generations, are becoming aware of the potential consequences of their online behaviour. This could result in the creation of a larger, more active and innovative market for online privacy tools (IFLA, 2019).

3.3 Trust, reputation and data breach impact

Companies that want to win the trust of their customers and be successful on the market now have to take stricter measures to protect their clients' data and maintain a good reputation. A data breach, especially if managed poorly, can cause very serious, sometimes irreversible harm to a company's reputation. After

the enforcement of the GDPR, the number of reported data breaches has surged. In 2019 the total number of records exposed increased by 284% compared to 2018, according to Risk Based Security (RBS, 2019). Therefore, although the priority should be to prevent data breaches and none of the companies want to have a data breach, in some cases it is impossible to avoid mistakes that lead to a data breach. In this case, the client's trust will be compromised and the company will have to allocate significant resources to deal with the consequences and restore the trust (Data Privacy Manager, 2020). According to the GDPR, in the case of a personal data breach, the controller shall notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (Regulation (EU) 2016/679).

In case a data breach occurs, a company can expect all sorts of scenarios damaging its image: media attention, customers and potential customers turning against the company and expressing their discontent via social media and ultimately loss of clients. In turn, this may result in loss of trust and brand value as well as financial losses. According to a study conducted in the UK, 61% of chief marketing officers believe that loss of brand value is the biggest cost of a security incident (Ponemon, 2017). IT specialists as well as marketing specialists consider a data breach a top threat to their companies' reputation and brand value (Ponemon, 2017). IBM in cooperation with Ponemon Institute provides specific figures in their data breach report. According to the report, the average total cost of a data breach is \$3.86 million (IBM, 2020). Data breaches are quite expensive for several reasons. Firstly, the company has to tackle the costs incurred by containing the breach. Secondly, in certain circumstances, it is necessary to compensate affected customers. Thirdly, it results in a decreased share value. When a data breach occurs and personal data are disclosed, stock prices fall by approximately 5% (Ponemon, 2017). Fourthly, there is a need to increase short-term and long-term security costs.

According to research conducted by the Boston Consulting Group, data misuse in most cases is perceived by consumers not as a legal issue since consumers rarely read agreements of use when they sign up for a credit card, social media services or other services (Boston Consulting Group, 2018). On the one hand, consumers can be careless about posting their personal data publicly. On the other hand, according to the research, consumers do not trust companies that misuse their personal data. When consumers learn that their data have been leaked or collected and used in dubious ways (different from the original purpose for which they were used and collected), they tend not to trust such companies since they feel that harm has been done to them and their privacy has been compromised (Boston Consulting Group, 2018). Consequently, research suggests that consumers' reactions to data misuse can cause them to reduce their spending with a company by about one-third (Boston Consulting Group, 2018). This might serve as a viable stimulus for the companies to genuinely care, if not about personal data safety, then about their own reputation, which is extremely important when it comes to customer trust. The steps made by companies to implement data protection impact assessment and provide reasonable safeguards for customer personal data will ultimately lead to a long-term and sustainable competitive advantage on the market.

The proliferation of the data protection topic in the news and academic circles combined with a healthy market competition are rendering issues of trust and privacy increasingly important for both academicians and entrepreneurs. Companies that misuse personal data are facing serious consequences. They are losing access to five to ten times the data they could have used had they made appropriate measures to create trust between the company and clients (Boston Consulting Group, 2018). Therefore, even without awareness about personal data value, consumers would choose good data protection.

However, companies must and are able to employ means of preventing and tackling potential data breaches and personal data misuse. Researchers suggest that companies with adequate security measures are much more resilient and are less likely to suffer the detrimental impact on stock prices posed by data

security issues (Ponemon, 2017). Adequately strong security indicators are: –(i) a dedicated chief information security officer; (ii) adequate investment in security technologies and especially communication encryption; (iii) measures designed to increase awareness and reduce employees' negligence regarding personal data and online security; (iv) regular assessment of data security measures and vulnerabilities; –(v) a comprehensive course of action in case a data breach occurs and a program with policies and assessment to manage third-party risks; (vi) sharing experience and advancements in data security measures with other institutions.

Another important feature of adequate security measures is that companies that employ them are much more likely to recover faster after a data breach. Companies employing high standards of security demonstrate a strong resilience and a quick reaction to data breaches. This results in their stock value recovering after approximately seven days. In contrast, stock prices of companies with insufficient security measures do not recover fully after a breach. Such companies experience a stock price decline after the data breach disclosure, and this decline appears to be long-lasting (more than 90 days). According to the comparative research by Ponemon, the data breach consequences are more detrimental for companies with poor data protection measures (Ponemon, 2017). The average difference in index values between companies employing adequate security measures and companies with poor security measures is 4 percentage points (Ponemon, 2017).

4 Discussion

Technologies will undoubtedly continue to evolve, interactions between users, advertisers and platforms will become even more transparent, and privacy protection mechanisms will continue to improve. Users' computers and mobile devices are becoming more powerful, the Internet is ever faster, and as a result, more data, including personal data, appear on the Internet. With the digitization of personal data and IT technologies that march victoriously around the globe, the topic of personal data protection will inevitably proliferate even faster. With the development of modern data processing, mining and collection technologies, various companies and institutions will have more opportunities to make these data operations faster and more efficiently.

Most of the research studies and statistical data available (including data presented in this article) come to a reasonable conclusion that personal data are valuable or even extremely valuable when it comes to particular spheres such as online sales and marketing. Even more importantly, it is evident that the value of personal data has been increasing recently and will apparently continue to increase. This brings many consequences to consider. The trend of online privacy is on the rise. More users are becoming aware of their data being collected and processed and as a result, they tend to choose options that will allow them to prevent their data from being collected. It is only logical that the market responds to such demand by providing ways of protecting or minimizing the collection of personal data and making it possible for users to maintain their privacy online.

Protecting clients' personal data has not only become a legal obligation, but according to various research papers, it has become profitable. Conversely, poor protection and abuse of users' personal data results in financial losses for companies. Research and statistical data confirm that nowadays people tend to distrust companies that handle their data in dubious ways. Data breaches result in serious reputational damage. Consequently, losing a clients' trust results in losing clients' money. Considering raising personal data protection awareness, the example of the leading IT companies starting to put an emphasis on privacy (Apple) and the enforcement of the GDPR, the trend of privacy will find its manifestation in strategies and products of an increasing number of companies.

Companies that misuse personal data are facing serious consequences. They are losing access to five to ten times the data they could have used had they made appropriate measures to create trust between the

company and clients (Ponemon, 2017). Therefore, even without awareness about personal data value, consumers would choose good data protection. However, if individuals are shown the true value of their personal data and are aware of the personal data value and their power on the digital market, they can effectively regulate the market in favour of personal data protection and thus effectively create an environment for protection of their information privacy.

The commodification of personal data is a reality that has already emerged due to the value of such data. Healthy market competition is an effective way to genuinely incentivize data protection of individuals. In most cases, however, individuals are not fully aware of the true value of their personal data. Accordingly, one of the best ways to encourage data protection is to empower data subjects and increase awareness of their personal data value. Articles 13, 14 and 15 of the GDPR are already providing several provisions about the obligation to inform data subjects. However, the GDPR is relatively new legislation and the majority of Internet users are still rarely aware of their rights in this regard. Nevertheless, the introduction of the GDPR is a very important step on the road towards comprehensive data protection and this topic will inevitably circulate both among scholars and in the social and economic life of different societies across the globe.

Additional Information and Declarations


Conflict of Interests: The author declares no conflict of interest.

Author Contributions: The author confirms being the sole contributor of this work.

References

- Backer McKenzie.** (2020). *GDPR survey. Benefits beyond compliance.* https://www.bakermckenzie.com/-/media/files/insight/publications/2020/04/gdpr_survey.pdf?la=en
- Bonatti P. A., & Kirrane, S.** (2019). Big Data and Analytics in the Age of the GDPR. In *2019 IEEE International Congress on Big Data (BigDataCongress)*, (pp. 7–16). IEEE. <https://doi.org/10.1109/BigDataCongress.2019.00015>
- Bergemann, D., & Bonatti, A.** (2011). Targeting in advertising markets: implications for offline versus online media. *The RAND Journal of Economics*, 42(3), 417–443. <https://doi.org/10.1111/j.1756-2171.2011.00143.x>
- Boston Consulting Group.** (2018). *Bridging the Trust Gap in Personal Data.* <https://www.bcg.com/publications/2018/bridging-trust-gap-personal-data>
- CISCO.** (2019). *Consumer Privacy Survey. The growing imperative of getting data privacy right.* https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf
- CMS.** (2021). *GDPR Enforcement Tracker Report 2021.* <https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report>
- CNIL.** (2019). *Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.* <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>
- Data privacy manager.** (2020). *Privacy, Data Breach and Reputation Management.* <https://dataprivacymanager.net/data-breach-and-reputation-management/>
- Deloitte.** (2019). *The GDPR: Six Months After Implementation Practitioner Perspectives.* <https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/legal/ce-deloitte-the-gdpr-six-months-after-implementation-report-1.pdf?nc=1>
- ENISA.** (2018). *The Value of Personal Online Data.* <https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data>
- EUR-Lex.** (1995). *Directive 95/46/EC.* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>
- EUR-Lex.** (2016). *Regulation (EU) 2016/679.* <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Parliament.** (2020). *The CJEU judgment in the Schrems II case.* [https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA\(2020\)652073_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)
- European Parliamentary Research Service.** (2019). *Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law? Scientific Foresight Unit (STOA) PE 634.445 – July 2019.* [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445\(ANN1\)_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445(ANN1)_EN.pdf)
- Golla, S.** (2017). Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(1), 70–78.

- Greenwood, D., Stopczynski, A., Sweatt, B., Hardjono, T., & Pentland, A.** (2014). The New Deal on Data: A Framework for Institutional Controls. In J. Lane, V. Stodden, S. Bender, H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 192–210). Cambridge University Press.
- Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z.** (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65–98. <https://doi.org/10.1080/13600834.2019.1573501>
- IAPP.** (2019). *Annual Governance Report 2019*. <https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/>
- IBM.** (2020). *How much does a data breach cost?* <https://www.ibm.com/security/data-breach>
- IFLA.** (2019). *The future of online privacy and the security of personal data*. <https://trends.ifla.org/expert-meeting-summary/the-future-of-online-privacy-and-the-security-of-personal-data>
- Internet World Stats.** (2021). *Internet usage statistics*. <https://www.internetworldstats.com/stats.htm>
- Keating, M. G.** (2013). *Benefits of Targeted Advertisements: A Spotify Fail*. <https://www.ereach.net/benefits-of-targeting-advertisements/>
- Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T.** (2020). European privacy law and global markets for data. In *CEPR Discussion Paper No. DP14475*. <https://doi.org/10.3929/ethz-b-000406601>
- Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T.** (2020). *Regulatory export and spillovers: How GDPR affects global markets for data*. <https://european.economicblogs.org/voxeu/2020/bechtold-batikas-kretschmer-gdpr-affects-global-markets-data>
- Ponemon.** (2017). *The Impact of data breaches on reputation & share value*. https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf
- Rieger, A., Guggenmos, F., Lockl, J., & Urbach, N.** (2019). Building a Blockchain Application that Complies with the EU General Data Protection Regulation. *MIS Quarterly Executive*, 18(4), Article no. 7. <https://aisel.aisnet.org/misqe/vol18/iss4/7>
- Risk based security.** (2019). *Q3 2019 Data Breach QuickView Report*. <https://www.internetworldstats.com/stats.htm>
- Science Focus.** (2021). *How much data is on the internet?* <https://www.sciencefocus.com/future-technology/how-much-data-is-on-the-internet/>
- Spiekermann, S., Böhme, R., Acquisti, A., & Hui, K.-L.** (2015). Personal data markets. *Electronic Markets*, 25(2), 91–93. <https://doi.org/10.1007/s12525-015-0190-1>
- Statista.** (2020). *Google: annual advertising revenue 2001-2019*. <https://www.internetworldstats.com/stats.htm>
- The Chartered Institute of Marketing.** (2016). *Be transparent on social media or risk the consequences*. <https://www.cim.co.uk/newsroom/opinion-be-transparent-on-social-media-or-risk-the-consequences/>
- The Economist.** (2017). *The world's most valuable resource is no longer oil, but data*. May 6th, 2017 edition. <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>
- TrustArc.** (2021). *Global Privacy Benchmarks Report 2021*. https://info.trustarc.com/Web-Resource-2021-05-26-Global-Benchmarking-Report_LP.html
- Zhuo, R., Huffaker, B., Claffy, & Greenstein, S.** (2021). The impact of the General Data Protection Regulation on internet interconnection. *Telecommunications Policy*, 45(2), 102083. <https://doi.org/10.1016/j.telpol.2020.102083>

Editorial record: The article has been peer-reviewed. First submission received on 31 July 2021. Revisions received on 6 September 2021, 14 November 2021, and 9 December 2021. Accepted for publication on 10 December 2021. The editor in charge of coordinating the peer-review of this manuscript and approving it for publication was Zdenek Smutny .

Acta Informatica Pragensia is published by Prague University of Economics and Business, Czech Republic.

ISSN: 1805-4951
