RIGA GRADUATE SCHOOL OF LAW

From Directive 95/46/EC to the General Data Protection Regulation: Addressing the potential harm to data subjects' rights arising from personal data collection and data analytics

BACHELOR THESIS

Author: Elvīra Krēķe

LL.B. 2017/2018 year student

student number B015049

SUPERVISOR: *ĒRIKS KRISTIĀNS SELGA*

LL.M.

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) …….

RIGA, 2018

Abstract

This work highlights the issues of personal data collection and its use in data analytics by analyzing the potential harms to idndividuals rights' arising prom personal data collection and data analytics and comparing the findings with the newly developed General Data Protection Regulation, and whether the new Regulation effectively addresses the existing issues.

The topic for the Bachelor thesis has been chosen due to its relevance, namely the introduction of the new General Data Protection Regulation, which fully is to be enforced in the 25th of May, 2018. The reason behind the development of the new regulation is the Directive's 95/46 inability to address current issues which are to be faced in regards to personal data protection. The Directive is not designed to address current issues. Currently, data collecting and processing occurs through highly advanced technologies which were not existant at the time when the Directive was shaped. In the period when the old Directive emerged, data processing was carried out by different means, and consequently was exposed to different risks than currently. Currently, data controllers in the online realm are collecting huge amounts of unnecessary peronal data, in order to improve their provided online services and to design them to be more personalised and appealing to individuals, through data analytics and using algorithms. The personalised data is being collected not only by the information which is provided by the subject willingly, but also from the data trail which the subject leaves behind – it may be the search or particular topics or most frequently visited websites, or video's which are being watched on the Internet.

The work concludes with findings that the Regulation efficiently addresses the opposed issues, leaving room for interpretation in certain areas, by safeguarding the rights of data controllers. By analysing the opinion of Bryce Goodman and Seth Flaxman, statements about the Article 22 are to be proven as faulty, as well as concluding with an in-depth analysis on Article 22 "the right not to be subjectd to automated decision making, including profiling", and finding that profiling as a form of data analytics in its nature is not protected fully by Article 22, but by two different articles of the Regulation.

Table of contents

Introduction **4**

1. Data protection in the European Union prior General Data Protection Regulation **5**

1.1. The concept of personal data 6

1.2. Reasons behind collecting personal data 9

1.2.1. Data trails……10

1.2.1.1. Profiling, targeted marketing and filter bubbles……11

1.3. Data analytics and consequences of data analytics……..13

1.4. EU regulation regarding data protection prior GRPD……..14

1.4.1. Potential harm to Data subjects' rights according to Directive 95/46/EC……..15

1.4.1.1. Google Spain C-131/12 and Weltimmo C-230/14 ……17

2. The Development of General Data Protection Regulation ……....18

2.1. Rights of the data subject according to General Data Protection Regulation …….20

2.1.1. Data subject's right not to be subjected to automated decision-making……21

2.1.2. The non-existing right to explanation……..…22

2.2. Potential harm to Data subjects' rights according to GDPR……....24

3. Comparison and the effectiveness of General Data Protection Regulation …….27

Conclusion **30**

Introduction

Due to the new General Data Protection Regulation, which is to be enforced on 25th of May, 2018, data protection has evolved to be a topical subject, as it is directly applicable and poses a more strict regulation than the current Directive 95/46/EC. The new Regulation has been developed to address current data protection issues, and to replace the out-dated Directive 95/46/EC. Particularly, the issue of data analytics, profiling and the collection of personal data in the online realm is concerning amongst many, as the Directive excludes provisions for specific instances in regards to the Internet and the online realm. Consequently, such actions may potentially harm individuals' and their rights to excercise protection according to data protection laws.

Research question - Does the General Data Protection Regulation better address the potential harm to data subjects rights arising from the collection of their personal data from the data trail left behind, and of its use in targeted algorithms than the Directive 95/46?

Hypothesis - The GDPR effectively addresses the issue of data analytics by granting individuals additional rights, although not absolute, shifting the ability to control personal data between controllers and subjects, and by posing additional obligations on controllers.

Structure and Scope

The following work is designed to put an emphasis on the online realm of data protection law by carrying out a comparative research on both legislative acts and how the General Data Protection Regulation copes with the aforementioned concerns posed to the Directive 95/46/EC. The first part of the work highlights the main concepts of data protection, additionally carrying out analysis on the potential harm to individuals' rights, as well as consequences of unprotected data collection in accordance with Directive 95/46/EC, and how such issues may be tackled according to the provisions laid down by the Directive 95/46/EC. The second part of the work gives an explanation on the significance and the development of the General Data Protection Regulation, followed by an in-depth analysis on the innovations introduced, the widely discussed perception on the existence of the "right to explanation" included in the new Regulation, as posed by Bryce Goodman and Seth Flaxman, and, finally, by examining the potential risks which may arise due to the new Regulation, if any found. The Thesis is to be concluded with a comparison between both legislative acts, the effectiveness of the General Data Protection Regulation and on whether it successfully tackles the risks in comparison with the Directive 95/46/EC, as well as an analysis of the power-relationship shift between data controllers and data subjects and the potential predictions of the further development of the relationship.

Methodology

In regards to the research methods applied in the work, the research will mostly encompass the use of doctrinal method, as primary sources serve as the basis of the research that is to be carried out – specifically Directive 95/46/EC and General Data Protection Regulation with the relevant legislative acts issued thereof. The interpretations explained in the continuing

work are to be solely based on the interpretations given by the European Commission and the Article 29 Working Party guidelines and opinions issued on the following research topics. In this study, the interdisciplinary method is present and to be used in theoretical parts of the work, namely, in part one, by using secondary sources in order to gain a theoretical understanding and an overview in the field of data protection law. Each part of the work will encompass analysis of the author, as continuing examination is to be carried out throughout the work along with theoretical explanations, nonetheless, part three finalizes the research with an in-depth analysis of the issues discussed above which is supplemented by a conclusion on the comparative research by summing up the analysis made throughout the work.

Legal Study

To successfully carry out a comparative research between both legislative acts in regards to the protection of individuals' rights concerning personal data used in data analytics, it is crucial to highlight the main concepts of data protection, the process of data analytics, as well as to examine what type of risks and consequences individuals' are exposed to during data processing which is carried out by the collected personal data from the data trail left behind. Thus, the following part of the work will consist of the following – a theoretical explanation of concepts and processes, alongside with the analysis of the Directive 95/46/EC/ in order to determine on the effectiveness of the Regulation in regards to the aforementioned issue. The protection in the field of data analytics will be analysed from the perspective of the Regulation and the Directive, thus concluding on whether all of the potential harms to individuals have been addressed in the new regulation, and on whether no potential harms are to be found according to the upcoming new Regulation.

1. Data protection in the European Union prior General Data Protection Regulation

In a century, where innovative technologies undertake an excessive part of an individuals' every day life, where data is being transmitted and manipulated through means which an individual cannot visibly follow, the concern about data protection grows among people, who strive to possess a greater control over their personal data.

Therefore, in order to protect the rights of individuals, data protection laws have been established. Data protection law ensures individuals with rights to control their personal information to a certain extent, in order to prevent unneccessary use of information to benefit establishments, which receive or request such personal information, as well as to avoid an extensive intervention with individual's personal rights and privacy.

In 1970's the need for data protection legislation arose from the increased use of computers, as various countries begun to establish laws regarding data protection, as, for instance, in 1983, the United Kingdom introduced the Data Protection Act 1984.[1] The European Union, on the other hand, did hesitate to introduce any legislative acts up until 1995, when the

[1] Peter Carey, Data Protection: Fourth Edition – A Practical Guide to UK and EU Law, Oxford University press, 2015, p.1.

European Directive 95/46/EC (hereinafter – the Directive) was finally introduced.[2] As the European Union had established the Directive, it was the duty of all member states to incorporate the Directive into their national legislation, in order for the Directive to take effect. [3] It was not long after, in 2000, when data protection was mentioned repeatedly - when the Charter of Fundamental Rights of the European Union was introduced ('Charter'), which underlined the rights of individuals which are independent from the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR'). Article 8 of the Charter was devoted to "Protection of Personal Data", and provided the basic fundamental rights regarding data protection, such as the right to protection of personal data concerning a particular individual, the provision that data must be processed on the basis of the consent of the individual who is a subject to personal data processing, as well as the data must be processed fairly and for the purposes for which it was needed and, lastly, the rules set out in the Article and compliance is subjected to an independent authority. [4]

The European Union clearly had marked the beginning of a new era in the field of law – a field where law and technology collides, nonetheless, many issues were yet to be tackled, as the technologies, practice and case law continuously changed, leading to new legislation and issues, including targeted algorithms, which will be touched upon in the continuing work.

1. The concept of personal data

By the introduction of data protection law in the European Union, specifically the Directive 95/46/EC, the term "personal data" obtained a more contemporary and advanced definition as posed by the Directive 95/46/EC itself, due to the necessity to precisely define the meaning of "personal data" in order to exercise data protection laws. The term "personal data" is more complex in the field of data protection law, as it may be perceived at first glance. In data protection law, personal data is to be understood as a broad concept which includes four main fundamental elements. Article 2 of the Directive defines personal data as follows:

> "personal data shall mean any information relating to an identified or identifiable natural person ("data subject")"[5]

from which the main four key elements are: 1) any information; 2) relating to; 3) identified or identifiable; 4) natural person[6]. All of the aforementioned elements are inter-connected and must be met in order to conclude on whether the data which is being processed is, in fact, personal data and whether it is in the scope of data protection laws to protect the particular data. Due to misinterpretation and erroneous applications of the concept in different Member States, the

---

[2] Ibid., p. 6.
[3] European Commission, Applying EU law, https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en, Accessed on 3rd of April, 2018
[4] Peter Carey, Data Protection: Fourth Edition – A Practical Guide to UK and EU Law, Oxford University press, 2015, p. 13.
[5] Data Protection Commissioner, EU Directive 95/46/EC - The Data Protection Directive, Article 2, https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm, Accessed on 3rd of April, 2018
[6] Data State Inspectorate, DSI Recommendation "Personal data definition", Riga, 2008, p. 4, http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/Personas_datu_definicija_rekomendacija.pdf, Accessed on 3rd of April, 2018

concept needed to be analysed in depth for the data protection framework to function properly. Therefore, Article 29 Data Protection Working Party (hereinafter – Working party) in it's published Opinion 4/2007 on the concept of personal data lays down a more descriptive analysis on each of the four key elements included in the definition. It is impotant to note the nature of the Working Party issued opinions. While it is to be considered more of an advisory nature, the legal force is stated to be as follows:

> "While not strictly legally binding, non-compliance with an opinion of the Working Party is highly indicative of violation of European data protection regulations. The opinions are authoritative, but not binding."[7]

The first of all of the four key elements is "any information". The wording "any information" may be understood as a widely interpreted element – but, the nature of the element is that in this context "any information" is meant to be any type of information about an individual. The information futher may be divided into two sub-groups "objective" and "subjective" information. Objective information is information about an individual which is more fact-based, for instance, a great example would be an individuals' hair color, health records or the current workplace. A subjective information, on the other hand, is formed by other people subjective opinions or assessments, such as, a statement of *"My co-worker is bad at his job"*. While it is an information which affects the recently discussed co-worker, and is directly linked to him, it is a subjective statement, which derives from the individual's point of view and opinion. For the information to be considered personal data, it is crucial to understand the fact that the data is not necessary to be true or even proven, thus the Directive provides remedies for data subjects to request for changing the erroneous information, in accordance with the law.[8] To conclude – the element encompasses any information, subjective or objective, even if it has not been proven or true, and contains any sort of information, including "sensitive data" which is information about an individual's health, religion, sexual orientation, racial or ethnic origin, political opinions, genetic data, and other. [9]

The second element "relating to" is crucial in terms of finding the links between the data subject and the information. The data must be related to the particular individual for it to be considered as personal data, this means – from the data given, it must be possible to link the information and about who the information has been provided. In most of the instances, where information is given, it is easy to conclude that the information is indeed *about* the particular individual, for instance, the aforementioned health records, a video filmed on a job interview, information about an employee in the workplace's system. All of the mentioned are clearly linked to a particular individual. Nonetheless, while in some instances it it may be difficult to find the "link", under certain cicrumstances it can be found. Such data is indirectly related data. Mostly, related data is obvious and the relationship is to be established without any complications, it is the indirectly related data which causes misunderstandings. Data, in instances where it is difficult

---

[7] European Union Agency for Network and Information Security, Article 29 Working Party, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/article-29-working-party, Accessed on 2nd of May, 2018

[8] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June, p.6.

[9] European Commission, What personal data is considered sensitive?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en, Accessed on 5th of April, 2018

to find the link, may be linked to an object which is under the possession of the data subject. For instance, if a car is under mainteinance and repair works in a service, while at first, the car itself is not linked to the owner, from the licence plate it would be easy for the mechanic to clarify to whom the vehicle belongs to – and in purposes of billing the owner for the services, as well as the connection established, it is to be considered as personal data which "relates to" the owner.[10] The Working party, answering to many questions which had arisen due to this element, has noted its final words on such a situation:

> "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated"[11]

Thus, under the concept of "relating to" it is also important to find the elements of *content, purpose* and *result*. The element *content* is the basic understanding on whether the information is related to a person – indirectly or directly, *purpose* is established if the data acknowledged is used in any way to evaluate, treat in a certain way or influence the behaviour of the individual, and lastly, *result* is fulfilled if an impact has been made on an individual's rights and interests. The elements must not all be met at once, and are only to be considered as alternative conditions, where the presence of one element is established, it is to be considered enough to conclude that the information relates to the data subject.[12]

The Directive provides that data only may relate to a "Identified or identifiable" natural person.[13] Usually, an identifiable person is a person which clearly differs in a group of people from the others, and is identifiable, nonetheless, in situations where one person is in a crowd and is not identifiable right away, may become identifiable under certain circumstances and conditions. Therefore, data subjects may be classified in "directly" and "indirectly" identifiable individuals. Identification occurs through various types of *identifiers* – whether it is the elements of individual's appearance, his name, profession or identification number. A directly identifiable person may be identified by a phone number, name and surname, or identification number – a standard procedure in terms of recognizing a person. But, in instances where a common name or surname is a subject to identification, it may not be sufficient to use the name alone for identification, as there may be many individuals with such a name, as for instance taking the most popular name from a country in which the subject is located in. Concerning "indirectly" identifiable persons, it is the combination of various *identifiers* which leads to the identification of an individual.[14] Although the identifiers may not be directly linked to one person, it may lead to identification, for instance, if a meeting were held between 7 strangers from which one would be significantly taller, and the chairman of the meeting stated that the tallest man in the room has

---

[10] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June, p.9.

[11] Working Party document No WP 105: "Working document on data protection issues related to RFID technology", adopted on 19.1.2005, p. 8.

[12] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June, p.10.

[13] 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, of 24 October 1995, Article 2

[14] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June, p.12

not fulfill his duties, it would be clear for all of the 7 people in the room about whom this particular statement has been targeted to - although the name has not been used, nor it was pointed directly to the person.[15] Many enterprises use data pseudonymisation, codification or anonymisation. It is important to remember, that pseudonymisation and codification are data which are possible to trace back to the individual, whereas anonymous data is the only thata which trully cannot be traced back. Therefore – the traceability factor plays a great role in terms of concluding on whether the person is identifiable under certain circumstances.[16]

The final element is "natural person". This element encompasses any individual, a natural person who may be considered as a data subject. Article 6 of the Universal Declaration of Human Rights states as follows:

> "Everyone has the right to recognition everywhere as a person before the law."[17]

The more precise definition of a natural could be found in every Member State's national laws, but mainly in the field of data protection – a natural person is considered a living person, starting from the period of birth up until the person has deceased. Unborn children and deceased persons are not *prima facie* subject of the Directive and data protection, but exceptions exist where deceased person data might be protected. Such exceptions may be seen in circumstances for where the data of the deceased may affect the persons who are still alive. For example – if a deceased person X had suffered from a certain genetically inherited disease which may indicate that his/her living children may also be affected with this disease, such sensitive data receive protection, as they are considered as sensitive data which relate to the children. Overall, deceased persons and unborn children are not subjected to data protection, until the data is related to and affects a living individual. In terms of Legal persons – although the Directive does not protect Legal persons, every legal person is controlled by a natural person and any information about the legal person is indirectly related to a natural person, therefore making Legal persons indirectly a subject to data protection.[18]

As stated beforehand, all of the components must be met in order to recognise whether the data being processed is personal data.

1.2. Reasons behind collecting personal data

Furthermore, if the data are found to be personal data according to the criteria given by the Directive 95/45/EC and according to the detailed explanation given by the Working Party Opinion, it must be assessed on whether the data collected are being processed. In regards to data processing, the Directive 95/46/EC gives a precise definition. The given definition of "processing personal data" by the Directive 95/46/EC states as follows:

> " 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as

[15] Agnese Buboviča, Arnis Puksts, Fizisko personu datu aizsardzības speciālista apmācība prezentācija 1. – personas datu tiesību attīstības jēdziens, termini un definīcijas, kas saistītas ar personas datu aizsardzību, 2018, p. 18.
[16] Ibid., p. 20.
[17] The Universal Declaration of Human Rights, Adopted on 10 of December, 1948, Article 6,
[18] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June, p. 22.

> collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"[19]

The Directive's definifion classifies collecting data as a form of data processing. Currently, in the 21st century, data collection has evolved in its importance due to technologies. During the formation of the Directive, it was designed to address data collection in forms of physical collection, as storing Cirruculum Vitae's, case files, health records, or in other words - data which may be physically stored. Presently, in the need and rise of the new Regulation – the General Data Protection Regulation (GDPR), this particular form of processing has become more topical. As technologies have developed, alongside, new foms of data collection have emerged, such as, collecting data from the Internet, GPS locations, storing files on personal computers, and many other ways from which data may be obtained. As the Thesis puts an emphasis on the online realm, especially on the data collection from the Internet, the continuing work will only touch upon one particular type of data collection.

On daily basis, through the Internet, data is being collected from vast amounts of its users without them being aware. The reasons for each of the data collectors differ, nonetheless, the most common and overriding reason for collecting personal data is of commercial nature. Data provides with information and knowledge, which leads to a certain power, eventually leading to a certain amount of income.[20] But, it is not only beneficial for one party, as the users benefit from receiving improved services, as information provides with the opportunity to develop more intelligent, adjusted and personalised programmes – whether it is by delivering more relevant advertisements to each individual, posts or search results adjusted for each individual's profile and interests.[21] Thus, smart search engnines and applications have been created, such as the well known Facebook or Google, which use intelligently designed algorithms in order to improve their provided services to its users. While it eases the use of the Internet for users, nonetheless, it raises the questions on how the data is being obtained, how and for what reasons?

1.2.1. Data trails

After visiting an Internet website or after the use of an application, each individual leaves a digital footprint, also called the data trail. It is impossible to be always aware of what digital footprint is left behind or collected, as the smallest "like" button or watch of a video leaves a mark.

The information is obtained from cookies which are placed on the websites. Internet cookies provide information for the web browser about the user, for the purposes for which the cookie was placed. When the site is visited for the first time, cookies are saved on to the

---

[19] 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, of 24 October 1995, Article 2 (b),

[20] Le VPN, Big Data: Why Do Companies Collect And Store Personal Data, https://www.le-vpn.com/why-companies-collect-big-data/, Accessed on 7th of April, 2018

[21] Jason Morris and Ed Lavandera, Why big companies buy, sell your data, CNN, https://edition.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html, Accessed on 7th of April, 2018

computer, and if an individual repeatedly visits the site, the cookie recognizes this particular individual and is aware that it is his second visit.[22]

> "There are numerous third parties which deliver content to websites and place cookies. Usually, the function of these third parties is to provide website providers with information on the number of visitors and which items on a website attracted the most attention. The third parties, thus, also provide a service to the website provider."[23]

The cookies may track the length of the visit on the website, what is done on the website, what links are clicked on, what type of videos are being watched – as it is the purpose of cookies through which companies obtain personal data.[24] After monitoring and obtaining data, data controllers decide upon how the data will be used to advantage the business itself – whether in marketing or in developing technologies. According to a research carried out in Massachusetts Institute of Technology, it has been sought that enterprises which use Data-Driven Decision making, show a 5%-6% increase in output and productivity.[25] Therefore, It is reasonable to state that in order to compete, the collection of big data and data-driven decision making is one of the best options. Additionally, not only big data are of help to legal persons, it also grants goverments with the chance to improve public sector administration, as well as helps different non-governmental or public organisations in regards to strategic planning.[26]

1.2.1.1. Profiling, targeted marketing and filter bubbles

One of the fundamental processes which occur after collecting excessive amounts of personal data is profiling. Data analytics mostly are carried out through profiling, as it is done by smart computers and given algorithms, which calculate the results unilaterally, giving the collectors a certain freedom in shifting attention to other sectors of importance.

A universally accepted definition for "profiling" does not exist, as it is hard to define. Organisations and the European Commission have attempted to define racial, ethnic and terrorist profiling, nonetheless the definitions differ in the definitions themselves, for instance - the European Commission defines racial profiling as:

> "The use by the police, with no objective and reasonable justification, of grounds such as race, colour, language, religion, nationality or national or ethnic origin in control, surveillance or investigation activities"[27]

---

[22] BBC Webwise, What are cookies?, http://www.bbc.co.uk/webwise/guides/about-cookies, Accessed on 8th of April, 2018

[23] Arnold Roosendaal, Facebook Tracks and Traces everyone: Like This!, Tilburg Institute for Law, 2011, p.4. http://ssrn.com/abstract=1717563, Accessed on April 9th, 2018

[24] Ibid.

[25] Erik Brynjolfsson, Lorin Hitt and Heekyung Kim, Strength in Numbers: How Does Data-Driven Decision-Making Affect Firm Performance?, 2011, p.3. http://www.a51.nl/storage/pdf/SSRN_id1819486.pdf, Accessed on 8th of April, 2018

[26] Omer Tene, Jules Polonetsky, Big Data For All: Privacy and User Control In The Age Of Analytics, p..244. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip, Accessed on 8th of April, 2018.

[27] Council of Europe, European Commission against Racism and Intolerance, https://www.coe.int/t/dghl/monitoring/ecri/activities/GPR/EN/Recommendation_N11/Recommendation_11_en.asp, Accessed on 8th of April, 2018.

At the same time, in case R. v. Richards[28], racial profiling was defined by the Ontario Court of Appeals, as "Racial profiling is criminal profiling based on race.". [29] Nonetheless, as there is no universally accepted definition, it is safe to state and to rely on the explanation of profiling due to data mining or collecting:

> "a process by which large data bases of personal information are subjected to computerized searches using a set of specific criteria."[30]

This means, as all of the recorded data from actions on the internet are taken, afterwards analysed, and consequently computers according to specific algorithms are able to classify each individual into a certain group of category of people under which they may fall into, thus providing personalised services. Later on, the purposes and use of the profiles created differ, as they may have been created due to many reasons. The most common use of profiles is for targeted marketing. [31]For instance, if one person mostly buys books on amazon or ebay, ebay and amazon will start to recommend books in the "recommended for you" or "most popular in books" section, as it has calculated that it is the persons' field of interest and hobby, therefore It will not advertise house items or gardening tools. Another example is a well known application which is used by many professionals around the world – LinkedIn. LinkedIn also uses profiling, but on a different level from advertising and sales – by providing with job offers. While it provides a platform for professional profile building and connecting with other professionals, it charts trends in the labour market. Based on the positions which one undertakes, and interests, LinkedIn creates patterns of most likely interested job offers for each profile. [32]

While profiling may find out to be a useful tool for delivering as many relevant products and services to the user as possible, and while data analytics may become benefictial for both parties, nonetheless, it possesses its flaws which potentially may lead to restriction of individuals' rights. Algorithmic bias and the automatically created bubble of information isolates individuals from the rest of the information, keeping the individual in his "filter bubble". When the algorithm has calculated to classify one into one certain filter bubble, there exists very little chance to change anything manually, the websites simply do not offer anything outside the bubble and offer a very narrowed information. This is where the concerns and issues arise. Individuals are not aware of the fact that they are in a certain filter bubble and are being constantly targeted by "fake news" during elections, certain articles, or advertisements. [33]

---

[28] R. V. Richards, Ontario Court of Appeal, [1999] O.J. No. 1420, http://www.aclc.net/wp-content/uploads/R1._v._Richards_1999_O.J._No._1420.pdf, Accessed on 9th of April, 2018

[29] Andras Laszlo Pap, Profiling, Mining and Law Enforcement: Definitions, 50 Annales U. Sci. Budapestinensis Rolando Eotvos Nominatae 277, 2009, p. 278, http://heinonline.org/HOL/Page?handle=hein.journals/ausbud50&collection=journals&id=279&startid=&endid=304, Accessed on 9th of April, 2018.

[30] Ibid., p. 282

[31] Electronis privacy information center, Privacy and Consumer Profiling, https://epic.org/privacy/profiling/, Accessed on 2nd of May, 2018

[32] Loekke Morel, Alex Wan der Wolk, Big data analytics under the EU General Data Protection Regulation, 2017, p. 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3006570, Accessed on 9th of April, 2018

[33] The Guardinan, How Social Media Filter Bubbles And Algorithms Influence The Election, https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles, Accessed on 9th of Aptil, 2018

1.3. Data analytics and consequences of data analytics

Big data collection and filtering makes it easy to isolate individuals from other relevant and reputable information, thus giving the opportunity to influence individuals in their way of perceiving the world, or makes it easier to spread propaganda. Individuals read what they are given and assume that all other users are exposed to such content as well, consequently leading to think what is being read is true. Data analytics, under any circumstances, leave consequences, unfortunately, without the appropriate protection, the majority may turn out to be harmful.

Filtering, profiling, data collection and the inability to choose accessible information manually leads to discussions about user rights in this matter. If companies, organisations, the government have the tools to influence the platforms from which individuals' obtain information, it would be logical to assume that users also possess some certain rights in this field of matter. The concerns for privacy are reasonable, as individuals feel as if they are losing the sense of control over their personal data, giving rise to serious privacy risks.[34]

The first privacy risk is the growing incremental effect on privacy. Information and data from the data trails left behing are constantly being added to one's profile and linked to the identity of the person, gradually leading to a greater exposure to personal data. Researchers Narayanan and Shmatikov have explained[35]:

> "once any piece of data has been linked to a person's real identity, any association between this data and a virtual identity breaks the anonymity of the latter."[36]

Any person in the world can be linked to at least one fact which lies in the computer databases, which can be used to anyones' advantage. Paul Ohm believes that from the information which lies in the databases a "data base of ruin" is possible to create, and from the information accessible it becomes more and more easy to threaten, blackmail or steal the identities of individuals all around the world.[37] Identity theft is not an unknown phenomenon in the 21st century, as it becomes gradually easier to steal an individuals' identity from the information available and act in that particular individual's name. This poses risks to individual's right to security and the fundamental right to privacy.[38]

The second great concern derives from automated decision-making processes as they tend to interfere by auto-filling information about an individual and therefore exposing certain information on the Internet, which may not have to be exposed. Such actions may lead to potential discrimination or the narrowing of choice not only by the aforementioned advertising, but also decision making by banks and insurance companies related to a person's credit, insurance or job prospects.[39]

---

[34] Omer Tene, Jules Polonetsky, Big Data For All: Privacy and User Control In The Age Of Analytics, p..251. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip, Accessed on 9th of April, 2018

[35] Ibid., p . 14

[36] Ibid.

[37] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, University of Colorado, 2010, p. 1748, https://www.uclalawreview.org/pdf/57-6-3.pdf

[38] The Universal Declaration of Human Rights, Adopted on 10 of December, 1948, Article 3 and Article 12

[39] Omer Tene, Jules Polonetsky, Big Data For All: Privacy and User Control In The Age Of Analytics, p..253. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip, Accessed on 9th of

The third risk has formed due to predictive analysis. Although predictive analysis may advantage in certain social policy areas, and it is a great help for law enforcement authorities in national security matters and for credit screening, it becomes an issue when the predictive analysis are created and formed from sensitive data. It may not raise any isues if one is offered to buy history books, based on the previous books purchased, on contrary, it is a completely different story in case of sending pregnancy and babby supply offers to a house where a women has not yet told the house hold about the expecting of a child.[40]

The aforementioned and other of such nature related issues have raised the questions on where to draw the line between "too much" and to what extent it is permissible to use and collect personal data. At a certain point, rights of an individual may be breached very quickly, hence the Directive 95/46/EC and the upcoming General Data Protection Regulation.

1.4. EU regulation regarding data protection prior GRPD

The EU data protection legislation and the EU Directive 95/46/EC 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 is based on the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter – Convention 108), as it was the first international legislation on data protection which was binding upon all of the Member States. [41]

Prior the Directive 95/46/EC, a set of fundamental rules and Guidelines regarding data protection had been set out and published by the The Organisation for Economic Co-operation and Development (OECD) – the Protection of Privacy and Transborder Flows of Personal Data. During the creation of the Directive, the rules laid down by OECD were taken into account as the fundamental rules for data protection and the basis for the shaping of the Directive. The Guidelines underlined principles as follows – the Limitation principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security safeguards principle, Openness Principle, Individual Participation Principle and the Accountability Principle. [42] The principles set out by the OECD remain relevant and in force up until this point in time, as they are the fundamentals of data protection.

For the purposes of harmonizing data protection laws accross the European Union and its Member States, as well as the transfer of data to third states, the Directive 95/46/EC was introduced. As the Directives' main goal was to bring together laws of the Member Sates, nonetheless, leaving room for interpretation. The room left for interpretation eventually became an issue, as numerous preliminary rulings were addressed to the European Court of Justice concerning the Directive rising a need for a new, better adjusted legislation.[43] Additionally to the Directive, due to the need for a regulation which regulated the electronic communications sector,

---

April, 2018
[40] Ibid., p. 16
[41] Monika Kuschewsky, Data Protection & Privacy: Second Edition, Thomson Reuters, 2014, p.255.
[42] EUGDPR, How Did We Get Here?, https://www.eugdpr.org/how-did-we-get-here-.html , Accessed on 16ht of April
[43] Ibid.

the Diective 2002/58/EC[44] or the 'ePrivacy Directive' was established.[45] The ePrivacy Directive regulates the processing of personal data in regards to direct marketing, as well the use of cookies. It requires the collector to receive consent from the data subject before the collection of cookies, for the fact that such services had been carried out by providing with clear and comprehensive information, collectors must provide users with the options to accept or not to accept the cookies, as well as the consent must be received from individuals before using the collected cookies for analytical purposes, and lastly giving the option to choose among what types of cookies are being deployed on their computers. [46]

It can be seen from the aforementioned, that prior General Data Protection, the Council had put effort to regulate the sectors of the electronic communications and the Internet, as cookies were introduces into legislation as a concept in 2002. While the Directive vaugly addresses such issues, Directive remains as a non-directly applicable regulation, except in cases where

> "the provisions of a Directive appear to be unconditional and sufficiently precise, they have direct effect if the Member State has failed to implement that Directive in domestic law by the end of the prescribed period."[47]

Such as statement was made by the ECJ in the ruling of the Case Federacion De Comercio Electronico Y Marketing Directo v. Administracion Del Estado, in which Spain referred a preliminary ruling to the ECJ on whether a specific Article of the Dirctive has direct effect.

1.4.1. Potential harm to Data Subject rights according to Directive 95/46/EC

To sum up all the issues arising from the continuously developing technologies, the most potentially harmful infringement of data subject rights is the infringement of an individuals' privacy. The concern for privacy is the fundamental basis from which derives the necessity of a new regulation. The imprecise use of data and the insecure use of data are only the consequences which derive from collected data about an individual. For imprecise use being the personalised algorithms and the poor application of personal data within the processes, and the insecure use being illegal use of personal data, such as for the purposes of identity theft. [48]

While the right to privacy is at risk, additionally, the lack of ability to control personal data flow is also present. The ePrivacy Directive provides with a provision for data collectors and processors to obtain the consent of the subject in case cookies are collected for analytical purposes. It does not mention the obligation to receive consent in processing and using data for analytical purposes, only the mere fact that cookies are collected with such an intent. While an

---

[44] 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), Official Journal L 201 , 31/07/2002 P. 0037 – 0047, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[45] Monika Kuschewsky, Data Protection & Privacy: Second Edition, Thomson Reuters, 2014, p.255.

[46] Ibid., p.269.

[47] Federacion De Comercio Electronico Y Marketing Directo (FECEMD) v. Administracion Del Estado, ("ASNEF")", C-469/10, https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, p.16., Accessed on 16th of April.

[48] Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert, Data Protection and Privacy: The Age of Intelligent Machines, Hart Publishing, 2017, p.68.

individual has the right to restrict the cookie-collection, an individual who has accepted the cookies will no longer be asked for his consent in terms of further use of cookies for analytical purposes. Nonetheless, the issue at its hand is not as simple as a denial of the collection of cookies, as collectors may come in different forms and from different locations.

One of the first issues which arose due to the regulation regarding cookies was the use of cookies by a non-European Economic Area company and the protection of data subjects' rights in such cases. The Directive does not address tis particular instance, and does not provide protection in cases a controller outside EEA deploys cookies on a subject's computer, and consequently collects data from users located in the European Union. The issue arises due to the lack of definition of the word "equipment".[49] The Directive 95/46/EC provides that Member States shall apply the Directive to the processing of personal data where:

> "[…] (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."[50]

Nonetheless, the Directive does not pose a specific definition for the concept of "equipment", which is mostly considered as physical equipment, hence not referable to the online realm, therefore rendering the chance of enforcing the Directive against a non-EEA country, such as the United States. Meaning that the Directive 95/46/EC does not provide an adequate protection of the rights of subjects located in the European Union from data collectors located outside EEA, as the territorial scope of the Directive mainly covers establishments formed in the in the European Union Member States. An additional lack of definition is found to be applicable also to the wording of "establishment". The Directive provides an obligation for controllers which are located in several Member States to undertake all the necessary measures to comply with the obligations provided by national law.[51] Therefore, it only admits the possibility of various establishments operated by one controller only in the borders of the European Union, as far as the national law applies to the establishment and the controller. Nonetheless, it is possible for a controller located outside the EEA to have establishments placed in the European Union, leaving a room for controllers to collect data from users without complying with the Directive.

Data Subject's rights defined by the Directive 95/46/EC reach as far as to the right to access data defined by Article 12 and the right to object by Article 14.[52] Data Subject holds the right to receive information on what data is being processed, for which purposes, to request the blocking of the processing which does not occur in accordance with the Directive, and the right to ask for the erasure of data which have been disclosed to third parties without prior notification.[53]

---

[49] Peter Carey, E-privacy and Online Data Protection, Reed Elsevier, 2012, p.95

[50] 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, of 24 October 1995, Article 4 (c), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, Accessed on 7th April, 201

[51] 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, of 24 October 1995, Article 4 (a), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, Accessed on 7th April, 2018

[52] Ibid, Article 12, Article 14.

[53] Ibid., Article 12.

The rights provided for individuals are sufficient until the processing of data does not concern data collection on the Internet, as due to the aforementioned lack of scope of the Directive, it is nearly impossible to provide the necessary protection. As mentioned before, controllers and establishments may be established all around the world, and while the Directive precludes such an instance, it restricts individuals to exercise data subject rights laid down in Articles 12 and 14.

1.4.1.1. Google Spain C-131/12 and Weltimmo C-230/14

Due to the fact that data analytics occur in the online realm, the online realm does not hold any country-like border, therefore, it becomes difficult to control personal data flow. The data may be collected from data trails left behind from all around the world, thus it is important to address data transmission between different countries – countries affected by the Directive, and countries which are not subjected to such regulation. As the the first landmark cases in which the European Court of Justice came in contact with the issue of transatlantic data transmission within EEA and non-EEA companies, are Google Spain and Weltimmo cases.

In the case of Google Spain, an individual had stumbled upon the fact that when the individuals' name was typed into the Google search engine, the first two pages of the search engine showed results of a newspaper article which indicated his name for a realestate auction carried out due to the ongoing proceedings for the collection of his social security debts. Therefore, the individual brought an action in Spanish courts against Google Spain, Google Inc. and La Vanguardia newspaper, requesting the removal of the information from the search engines. Nonetheless, while the subsidiary company is located in Spain (Google Spain) and was registered as the controller and processor of data in the country and advertised sales in Spain, Google Inc. provides with search results based on user's search requests and is a US-based copmany.[54] Preliminary ruling to the European Court of Justice was requested, by referring the question on whether an "establishment" is considered a subsidiary located in the EU of a non-EU parent company, designated as its representative and controller, who forwards the data to the parent company afterwards. [55] The Court concluded that in this particular case Google Spain is to be considered as an establishment according to Article 4 (1) (a), as it engages in the effective and real exercise of activity through stable arrangements in Spain.[56] The Court explains:

> "The processing of personal data by the controller is also "carried out in the context of the activities" of an establishment, even though Google Spain is not involved in the processing at issue (carried out exclusively by Google Inc.) but rather only in advertising in Spain. Article 4(1)(a) does not require that the processing in question be carried out "by" the establishment concerned, but only "in the context of the activities" of the establishment."[57]

---

[54] Google Spain SL v. AEPD (The DPA) & Mario Costeja Gonzalez, C-131/12, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065, Accessed on 16th of April, 2018.
[55] Ibid.
[56] DPO, Summaries of EU Court Decisions Relating to Data Protectoin 2000-2015, Data Protection Officer, 2000-2015, p. 51., https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, Accessed on 16th of April, 2018.
[57] Ibid., p.

Moreover, in Weltimmo case a Slovakian company which holds websites concerning with property selling held a website in Hungary, in Hungarian language, bank accounts located in Hungary, as well as a mail box in Hungary and concerning Hungarian properties and real estate. The website provides a chance for individuals to place an advertisement free-of-charge for the first month, followed by an automated payment the next months. Many users had requested the cancellation of the advertisements in the beginning of the first month, nonetheless, Weltimmo (the Company), had ignored the requests and charged the users in spite of the recieved requests. The question referred was on whether the national law is applicable in a situation where the controller located in another Member State runs a website in Hungary, and tranfers data back to the controllers' Member State.[58] The Court ruled that the Article 4 (1) (a) of the Directive allows the application of the national data protection law in another Member State in cases where the controller excercises activity in the Member state.[59] The Court also noted:

> "To establish whether the controller has an establishment in that Member State, both the degree of stability of the arrangements and the effective exercise of activities in the other Member State must be interpreted in light of the specific nature of the economic activities and provision of services concerned, particularly for undertakings offering services exclusively over the internet. The presence of only one representative can suffice to constitute a stable arrangement if he/she acts with a sufficient degree of stability through the presence of the necessary equipment for the provision of the specific services concerned in the Member State. Further, the concept of "establishment" extends to any real and effective activity, even a minimal one, exercised through stable arrangements"[60]

Both cases caused a great concern in terms of the previously discussed privacy of an individual and an individuals' ability to control personal data. Hence, the Court decided upon the applicability of Hungarian law in this particular case, creating a precedent for applying national law for another Member State controller, rising a need for a more harmonised regulation, which is fully in the competence of European Union and is directly applicable to all of the Member States, therefore addressing the issue of data analytics and collection in a wider geographical scope to avoid potentially harming individuals' rights.

2. The development of General Data Protection Regulation

All of the consequences may be categorized in two main groups – imprecise and insecure use of data, which potentially may harm an individual. Such consequences are to be considered as a result from an infringement of right to privacy and the lack of control of personal data. Case law fostered the development of the General Data Protection Regulation, affirming that the Directive had aged for it's initial purposes.

---

[58] Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C‑230/14, http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN, Accessed on 16th of April, 2018

[59] DPO, Summaries of EU Court Decisions Relating to Data Protectoin 2000-2015, Data Protection Officer, 2000-2015, p. 51., https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, Accessed on 16th of April, 2018.

[60] DPO, Summaries of EU Court Decisions Relating to Data Protectoin 2000-2015, Data Protection Officer, 2000-2015, p. 51., https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, Accessed on 16th of April, 2018.

The case Maximillian Schrems v. Data Protection Commissioner is considered as landmark case in terms of defining the "adequate level of protection" and for finding "Safe Harbour" principle as invalid. Schrems is the basis of the General Data Protection Regulation's strict grounds for 'Consent' and 'Right to Access'. In Schrems, an Austrian student brought an action against Facebook Inc. at the Irish High Court. Facebook Inc. is known to be located in the USA with it's subsidiary located in Ireland. Schrems sued Facebook Inc. on the basis of Facebook not providing adequate protection of personal data during the data transmission to USA, as the NSA had access to the personal data in the process. [61] The Court in its ruling admitted – while Article 25 (6) does not require Third countries to ensure the exact level of protection as the Directive:

> "(6) The Commission may find, […] that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5 , for the protection of the private lives and basic freedoms and rights of individuals."[62]

It, nonetheless does demand the countries to guarantee a similar or equivalent protection of fundamental rights and freedoms of the individuals. [63] As well, as it must be regularly analysed on whether the adequacy is legally justified. [64] In regards to the Safe Harbour principle, the Court found that the NSA and state authorities had access to data and were able to process it for other purposes than initially transferred, far from the necessary, for national security purposes:

> "Decision 2000/520 does not contain sufficient findings regarding US measures which ensure adequacy by reason of domestic law or international commitments. Rather, it enables interference with fundamental right to respect for private life of persons whose personal data is or could be transferred from the EU to the US."[65]

Therefore, to provide the adequate protection, and which is known to be one of the most substantial changes in the European data protection law – the indtroduction of the General Data Protection Regulation marks significant changes in the scope of the previous legislation, by eliminating the risk of excercising the collection of personal data and the use of personal data in data analytics, without the possibility for individuals' to be protected by the Directive, all of it which stems from the Court decisions of the Google Spain and Schrems case.

---

[61] Maximillian Schrems v. Data Protection Commissioner, Digital Rights Ireland, C-362/14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=23555

[62] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, Article 25 (6), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN, Accessed on 19th of April, 2018

[63] DPO, Summaries of EU Court Decisions Relating to Data Protectoin 2000-2015, Data Protection Officer, 2000-2015, p. 48., https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, Accessed on 19th of April, 2018.

[64] Ibid.

[65] Ibid.

2.1. General Data Protection Regulation and Collection of personal data

The GDPR is designed to fit the modern technology era, to protect individual's right to privacy, and to provide a more transparent personal data processing, as well as ensure data subjects with more control over personal data.

Apart from the fact that the Regulation is directly applicable, the most significant change of the newly introduced changes is the extra-territoriality principle. Previously, the scope of the Directive had been limited due to the provision of it being applicable only to data controllers located and based in European Union.[66] The GDRP, on the other hand, on Article 3 (2) lays down the Territorial scope being that it affects any establishement in the world, may it not be established in the European Union, as long as it processes data of data subjects located in the European Union.[67] Alongside with the biggest change – the extra-teritoriality principle – the GDPR introduces Penalties and stricter rules for receiving the consent of the data subject, which had not existed in the Directive. Additionally, in regards to data analytics, the GDPR finally defines the term "profiling", which previously had not been a recognised concept according to the Directive. Profiling is defined as any automated data processing, and the use of data analytics to evaluate certain elements of an individual in order to predict the performance in certain fields of life. [68]

The General Data Protection Regulation offers a wide scope of protection of individuals' rights. Specifically it is Chapter 3 of the GDPR which covers rights of the data subject. The key principles which have been introduced, are: the obligation to notify data subjects of data breach; Data subject's right to access; Right to be forgotten, or the right to request erasure of data; Data portability; Privacy by design or the data minisation, and finally it regulates the right to object and the automated individual decision-making. [69] All of the changes are designed to give more power to the data subject over personal data. With regards to the online realm and data analytics, the most important from the aforementioned rights are the right to access, right to be forgotten, and the right to be informed.

Right to access is laid down in Section 2 of the GDPR, Article 15, which grants the right to the data subject to obtain information from the data controller about what personal data is being processed and in certain cases to access the information for what purposes, the length of the processing, etc. Article 15 (1) (h) is specifically devoted to automatic-decision making, and reads as follows:

> "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

[66] Ivan Klekovic, EU GDPR vs. European data protection Directive, EUGDRP Academy, 2017, https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/, Accessed on 19th of April, 2018.
[67] Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 3 (2)
[68] Ibid., Article 4,
[69] EUGDPR, GDPR Key Changes, https://www.eugdpr.org/key-changes.html, Accessed on 19th of April, 2018

> involved, as well as the significance and the envisaged consequences of such processing for the data subject."[70]

Additionally, right to be forgotten is regulated by Article 17, which grants data subjects with the right to request for erasure. Meaning that any individual may request the erasure or personal data, if it is known to be in the possession of an entity. The establishment must take all the necessary measures to ensure the implementation of such rights and to guarantee the right to be forgotten. [71] Moreover, the right to be informed is regulated by Article 13 and Article 14 of the GDPR, and in regards to automated decision making, a right to be informed has been granted in Article 13 (2) (f), as well as Article 14(2) (g). Article 13 and 14 provide that the data subject, regardless of whether the data have been obtained from the data subject or not, must be informed about automated decision-making processes, or in other words – individuals must be informed if profiling or any data analytics are to be carried out using their personal data. Nonetheless, the right to inform does not entail a right to an explanation, on which an in-depth analysis will be carried out further in the work.

2.1.1. Data subjects' right not to be subjected to automated decision-making.

With the GDPR coming into force, individuals anticipate for transparency in data processing, being able to control personal data flow and the ability to be informed about how the data is being processed, where and how, including the right of not being subjected to automated-decision making and profiling. For such purposes, the GDPR introduces Section 4, Article 22 "Automated individual decision-making, including profiling" which is designed to handle automated-decision making and data analytics.[72]Article 22 provides that an individual holds the right not to be subjected to automated decision-making, especially automated decision-making with special categories of data (sensitive data), unless the data subject has given explicit consent, it is necessary to fulfil obligations of a contract, or the action is permitted by a Member State. Furthermore, Article 22 (3) lays down the obligation to safeguard individuals' rights.

Heretofore it has been concluded that GDPR has introduced the right to be informed about the automated decision-making process which is about to take place, the right to not be subjected to data analytics, and according to Article 22 (3), data subject holds the right to obtain human intervention by expressing point of view.[73] But, it does not explicitly entail data subjects to the anticipated "right to explanation" as initially hoped for and for which it is widely discussed about. Currently the GDPR only obligates entities to inform individuals of a process which is to be carried out, that such a process is ongoing or to simply not be subjected to it. Data subjects are entitled to receive limited information in regards to automated-decision making processes according to Articles 13-15.

---

[70] Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 15 (1) (h)

[71] Ibid., Article 17

[72] Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 22.

[73] Ibid.

The concept of "right to explanation" has appeared to be topical among enterpreneurs and AI enthusiasts due to its appearance in Recital 71 of the General Data Protection Regulation, as it provides that the data subject holds the right to "[…] to obtain an explanation of the decision reached after such assessment and to challenge the decision"[74]. This particular statement raises individuals to believe that after the coming into force of the Regulation, data subjects will hold such rights. Meaning, that if a bank carries out data analytics in regards to granting loans or credit, and if the technologies carrying out such activities come to a decision to deny the granting of a loan, the individual expects explanation on how the machine has come to such conclusions, and for what reasons. [75] Nonetheless, it proves to be an erroneous statement to be made as data subjects are not granted with such rights according to the new Regulation.

2.1.2. The non-existing right to explanation

As the work puts an emphasis on the potential harm to rights of individuals in regards to data analytics, and on whether the GDPR addresses more effectively the the issue of data processing in the online realm, it is important to sort out the discussion on whether the right to explanation is present, as it is a substantially important right which may potentially be granted. The original claim on the existing "right to explanation" was made by Bryce Goodman and Seth Flaxman by stating as follows:

> "[…]The law will also effectively create a "right to explanation," whereby a user can ask for an explanation of an algorithmic decision that was made about them. We argue that while this law will pose large challenges for industry, it highlights opportunities for computer scientists to take the lead in designing algorithms and evaluation frameworks which avoid discrimination and enable explanation."[76]

Nonetheless, before analysing why the right to explanation is a non-existing concept in the GDPR, it is crucial to understand the meaning behind "the right of explanation" in terms of data analytics.

Two types of explanations may be obtained in this particular scenario – an explanation on system functionality, and an explanation on specific decisions. The explanation on system functionality encompasses information about how the decision-making machines function, the logic behind it, criteria and other overall information about the structure of data analytics. The later – explanation on specific decisions – are the reasons behind decisions made by the machine, the rationale, information about profiling groups which have been formed from the obtained personal information, and other information which may be provided about the decisions made. [77] The difference between two of the explanations lay in between the fact that the first may be given

---

[74] Ibid., Recital 71, https://gdpr-info.eu/recitals/no-71/, Accessed on 20th of April, 2018.
[75] CSO from IDG, What does the GDPR and the "right to explanation" mean for AI?, 2018, https://www.csoonline.com/article/3254130/compliance/what-does-the-gdpr-and-the-right-to-explanation-mean-for-ai.html, Accessed on 20th of April, 2018
[76] Bryce Goodman, Seth Flaxman, European Union regulations on algorithmic decision-making and a "right to explanation", Oxford Internet Institute, Oxford, 2016, p.1, https://arxiv.org/pdf/1606.08813.pdf, Accessed on April 20th, 2018.
[77] Sandra Wachter,Brent Mittelstadt,Luciano Floridi, Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, International Data Privacy Law, 2017, p. 6., https://ssrn.com/abstract=2903469, Accessed on 20th of April, 2018.

before the data analytics have been carried out and after the decisions have been made, but the second explanation – the explanation on specific decisions – is only possible to be given after a decision already has been made by the machine. The aforementioned example of a credit-loaning entity may be applied in this particular situation. It is possible to provide with an explanation about the functionality of data analytics prior the machine has made a decision on whether or not to grant the loan – the principles on which the machine works, what data is necessary for it to calculate the results, but it is not possible to give an explanation on specific decisions until the machine has given a specific and final answer. [78] From this it can be observed, that while the concept may be understood in two interpretations, it also encompasses different timing at its core, which is crucial in the light of GDPR and finding the legal basis for the "right to explanation"

While the claim has appeared due to wording in Recital 71 in connection with Article 22 (3) and Articles 13-15, GDPR itself does not explicitly provide with such a right, but why is it not legally binding if it has been included in Recitals by the Commission itself?

The explanation lies within the legal status of Recitals. Recitails are of explanatory nature, considered more as guidelines in order to understand the aims of the legislation, while Recitals themselves remain as not legally binding.[79] While the European Court of Justice may use Recitals in order to acknowledge the aim of the Directive in preliminary rulings, before the ECJ and the Court it is a matter of interpretation and remains as not legally binding upon individuals.[80] Currently Article 22 (3), or the safeguards, provide as follows:

> "In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[81]

While Recital 71 in response to Article 22 (3) provides:

> "In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."[82]

As it can be observed, the wording differs, as the Article solely includes "the right to obtain human intervention", on contrary, the Recital in addition includes "the right to […] to obtain an explanation". The greatest difference is that the later is not legally binding, although it includes such a right. Klimas and Vaiciukaite have explained:

---

[78] Ibid.
[79] EUROPA, Guide to the Approximation of EU Environmental Legislation ANNEX I , 2015, http://ec.europa.eu/environment/archives/guide/annex1.htm, Accessed on 22nd of April, 2018.
[80] Amberhawk, The Recitals are Essential to Your Understanding of the General Data Protection Regulation, 2016, http://amberhawk.typepad.com/amberhawk/2016/01/the-recitals-are-essential-to-your-understanding-the-general-data-protection-regulation.html, Accessed on 22nd of April 2018
[81] Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 22 (3).
[82] Ibid., Recital 71, , https://gdpr-info.eu/recitals/no-71/, Accessed on 22nd of April, 2018.

> "Recitals have no independent operative effect. This is not so much a function of interpretation as it is of the nature of recitals; by definition, recitals are not operative provisions of themselves "[83]

Furthermore, such a statement can be supportet by case law, which has also proven the legal status of Recitals – in Case C-162/97 *Criminal proceedings against Gunnar Nilsson and Others*, in which Sweden requested for a preliminary ruling to the ECJ in regards to Recitals, as a Recital outlined an exemption for a Member State to prohibit the use of a product in case the use of the product could end in an undesirable pedigree, while the Directive 87/328 did not preclude such actions[84], the ECJ concluded:

> "On this point, it must be stated that the preamble to a Community act has no binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question. "[85]

Additionally, in Case *Casa Fleischhandels-GmbH v. Bundesanstalt für landwirtschaftliche Marktordnung* ECJ specifically notes: "Whilst a recital in the preamble to a regulation may cast light on the interpretation to be given to a legal rule, it cannot in itself constitute such a rule"[86] Therefore, it can be concluded that according to General Data Protection Regulation and the Recital 71 - the right to obtain explanation is not and existant and legally binding right, which may cause disappointment among individuals which had formed legitimate expectations due to Recital 71. The provision laid down in Recital 71 is only a matter of interpretation, which unlikely will result in granting of such a right. The implementation of such a right may cause controllers to be subjected to the exposing of the design of the algorithms for which they use, eventually harming their businesses, and thus allowing competitors to gain the necessary information in order to design identical or improved algorithms.[87]

2.2. Potential harm to Data subjects' rights according to GDPR

One of the first potential disillusions which are to be ruined regarding the General Data Protection Regulation and which is found to be without any supporting grounds is the claim that the right to obtain explanation does not exist, leaving the General Data Protection Regulation not significantly different from the Directive in regards to data analytics, as Article 15 of the Directive[88], which lays down the provisions for automated individual decisions, only lacks the

---

[83] P. 25.
[84] Tadas Klimas, Jūrate Vaičiukaite, The Law of Recitals in European Community Legislation, ILSA Journal of Intenraional and Comparative Law, 2008, p. 24, https://ssrn.com/abstract=1159604, Accessed on 22nd of April, 2018.
[85] Criminal proceedings against Gunnar Nilsson and Others, C-162/97, European Court of Justice, 1998, p. 54, http://curia.europa.eu/juris/showPdf.jsf?text=&docid=44220&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=198280, Accessed on 22nd of April, 2018
[86] Casa Fleischhandel v. Bundesanstalt für landwirtschaftliche Marktordnung, Case 215/88, European Court of Justice ECR 2789 [31], https://eur-lex.europa.eu/resource.html?uri=cellar:bff0427d-b75d-46bf-8015-7eeddf6f9ca8.0002.06/DOC_1&format=PDF, Accessed on 22nd of April, 2018.
[87] Jenna Burrell, How the machine 'thinks': Understanding opacity in machine learning algorithms, Big Data & Society, 2016, p.4., http://journals.sagepub.com/doi/pdf/10.1177/2053951715622512, Accessed on 24th of April, 2018.
[88] 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, of 24 October

opportunity to express one's views. Meaning, that while the safeguard to express views has been added, along with the fact that no longer a contract on the side of data subject is necessary, only leaving explicit consent as the pre-condition for automated-decision making to be lawful – the wording in the GDPR does not significantly differ. [89] Leaving individuals with limited rights in regards to data analytics.

The second element to understand is that the rights of subjects are not absolute and potentially may collide with the rights which may be exercised by the controllers – as the right to freedom of expression or information, which may cause issues in the process of excercising data subject's right to request for erasue. Such instances may be more relevant to the industries of media, nonetheless in specific cases it may become relevant in cases of data analytics. Data subject rights are more considered as contextual, a great example is the right to withdraw consent, which is provided by Article 7 (3) of the Regulation. While the Regulation provides the with the opportunity to exercise such a right at any given time, a given consent is only one of the grounds to which processing would be found lawful – meaning, that if any other of the provisions serve as a ground for processing, withdrawal of consent cannot longer be excercised at any time.[90] Therefore, in cases any of the other grounds apply, individuals can no longer exercise the right to withdraw consent.

Furthermore, while Article 22 of the GDPR regulates automated-decision making, including profiling, it leaves room for interpretation, as Article 22 only regulates "profiling […] which produces legal effects concerning him or her or similarly significantly affects him or her"[91] Only a part of data processing, also profiling may cause significant effect on an individual, and it is a matter of interpretation. It has been clearly noted by Recital 71, as an example, that an action which may constitute a significant effect would be a case in which an individual would be refused to access an online credit card application[92], but does profiling cause a significant effect if from two individuals, only one is offered a discount in a online shopping page due to the fact that he has bought something recently, but the later has not? [93] The wording on the GDPR is to be interpretd quite subjectively, therefore the Article 29 Working Party has issued guidelines specifically on Profiling and Automated-decision making, explaining in which cases it is to be

---

1995, Article 15, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, Accessed on 7th April, 201

[89] Sandra Wachter,Brent Mittelstadt,Luciano Floridi, Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, International Data Privacy Law, 2017, p. 13., https://ssrn.com/abstract=2903469, Accessed on 20th of April, 2018.

[90] I-Scoop, Data subject rights and personal information: data subject rights under the GDPR, https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/#Data_subject_rights_are_contextual_rights_obligations_and_circumstances, Accessed on 24th of April, 2018

[91] Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 22, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[92] Information Commissioners Office, Feedback request – profiling and automated decision-making, p.7. https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf, Accessed on 27th of April, 2018.

[93] Slaughter and May, Tracking, watching, predicting… lawfully: responsible profiling under the GDPR, 2017, p .3. https://www.slaughterandmay.com/media/2536527/profiling-under-the-gdpr-september-2017.pdf, Accessed on 27th of April, 2018.

constituted as a significant effect. The guidelines, firstly explain that profiling is to be understood in two ways, for one being decision-making based on profiling and the other being decisions made solely through automated decision-making means, including profiling, where in the first humans take part in the decision-making processes, but on the later it is only the machine which is to make the final decision.[94] It is to be conlcluded, that according to the wording included in Article 22, it only regulates the later, leaving decision making based on profiling not covered by Article 22. Nonetheless, it does not allow one to avoid Article 22 provisions by simulating the involvement of an individual, as the Working Party notes:

> "To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data."[95]

In regards to the significant effect arising from profiling, the Working Party lists the following as criteria from which to take guidance.

> " […] the decision must have the potential to:
> 1) significantly affect the circumstances, behaviour or choices of the individuals concerned;
> 2) have a prolonged or permanent impact on the data subject; or
> 3)at its most extreme, lead to the exclusion or discrimination of individuals.
>
> It is difficult to be precise about what would be considered sufficiently significant to meet the threshold, although the following decisions could fall into this category:
> 1)decisions that affect someone's financial circumstances, such as their eligibility to credit;
> 2) decisions that affect someone's access to health services;
> 3)decisions that deny someone an employment opportunity or put them at a serious disadvantage;
> 4) decisions that affect someone's access to education, for example university admissions."[96]

Finally, it is to be concluded that Article 22 does not regulate all types of profiling, therefore provisions laid down by Article 22 are not applicable for decision-making due to profiling in its nature. Profiling as a form of data processing is therefore only regulated by Article 6 and the lawful basis for which personal data may be processed under. [97]

Overall, regardless of the limitations in data subject's rights, and the confusion over which Articles regulate what type of data processing actions, the General Data Protection Regulation provides protection of data subjects' rights in regards to online data protection,

---

[94] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), P.9. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, Accessed on 27th of April, 2018.
[95] Ibid, p. 21.
[96] Ibid., p. 22.
[97] Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

limiting the rights to the necessary extent. The General Data Protection Regulation has been designed to fight the potential harms which may have been present during the time of the Directive, which will be more analysed in the last part of the Thesis. According to the Regulation, controllers are subjected to comply with more strict rules.

3. Comparison and the effectiveness of General Data Protection Regulation

The General Data Protection Regulation poses strict rules to data controllers, which may turn out to be costly in terms of time and monetary funds.

A significant change is the introducing of fines, which eventually will motivate data controllers to comply with the Regulation. Non-compliance, breach of data subject's rights or simply data breach are subjected to penalties in the amount of 4% from the annual turnover or up to 20 million euros[98], allowing data subjects to feel more secure about their data being in the hands of controllers. Additionally, controllers which constantly process personal data or sensitive data must hire a Data Protection Officer (DPO) in order to ensure the compliance with the GDPR, consequently ensuring the protection of data subjects' personal data. The additionally introduced safety measures and procedures of caution will reduce any leakage of personal data, eliminating the risks analysed in section 1.3. and the potential harm to data subjects' rights in section 1.4.1. of the Thesis.

Continuing on the discussion about whether the GDPR has been designed to provide sufficient protection and to fight the previously analysed potential harms, it is needed to carry out a comparison between both legislative acts and the previously analysed information in sections above. The first potential harm to individuals' rights as it has been noted in Section 1.4.1. is the risk to privacy and the lack of necessity to receive consent before data collecting, as the ePrivacy Directive does not provide a sufficient protection in regards to this particular issue. The GDPR, on the other hand, strives to eliminate such a risk by introducing the necessity for explicit consent, where consent is considered to be received under more strict conditions, which are laid down in Article 7 of the GDPR. [99] Therefore, in regards to data collection from data trails left behind, the conditions are to be applicable, making it significantly harder to unnecessarily collect data for analytical purposes. The aim is to provide citizens with the opportunity to use technologies without worrying about their data being unnecessarily collected from their actions on the Internet, but rather be informed of such actions and to choose on whether they are willing to be subjected to such actions. All in all, The GDPR addresses the issue of potentially breaching the right of privacy and to protect unlawful data collection, about which one may not be aware of.

The second issue, as it has been concluded, is the lack of extra-territoriality principle. While non-EEA contries are able to process data, the Directive does not provide protection for

[98]GDPREU, Fines and Penalties, https://www.gdpreu.org/compliance/fines-and-penalties/, Accessed on 27th of April, 2018.

[99]Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 7, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

individuals' outside European Union, nonetheless, as the Internet consists of various pages and applications controlled by data controllers all around the world, the necessity for such a protection is crucial, for which the GDPR has also shifted its attention to. The broadening of the scope of the Regulation provides with additional protection for EU citizens, as it protects from any legal or private entity within or outside the European Union, as the entities are also bound by the Regulation. This particular issue potentially resolves the issue of being only partially protected and being able to exercise data protection law rights under EU law. While data subjects hold certain rights under EU law, their ability to exercise rights is limited. While the Directive is in force, any company may be established outside EEA and not be subjected to the Directive, but unfortunately, Cookies which are deployed from the Internet, ease the collection of personal data directly from EU citizens which regularly visit non-EEA country sites.

The third concern on the potentially discriminating automated-decision making processes which auto-fill information about the data subject is addressed by Article 22 of the GDPR. [100] While it precludes the right not to be subjected to such automated-decision making, with an exception where explicit consent is received, due to the performing of a conract or if it has been authorised by a Member State, it has introduced the safeguards in which controllers' must protect the rights of individuals and to allow data subjects to exercise their right to obtain human intervention. Meaning that the GDPR has finally introduced the right to obtain human intervention, which is not present in the Directive. While the GDPR does not grant subjects' with a right to explanation, explained in Section 2.1.2., it does grant the right to obtain intervention – or to be informed about processes in which the data are being used and to express the point of view. This particular right protects individuals from an abusive use of personal data. For instance, if an individual has given consent for data analytics, but the person does not hold the right to obtain explanation and to know how exactly the process is carried out, as well as does not hold the right to contest the decision or to express views, the controller, along with the received consent might use the data for purposes which may or may not be in conflict with the individuals' views. Therefore, the right to obtain intervention to some extent and to express views is sufficiently enough to protect data subjects' rights, regardless of the fact that a right to explanation may be denied. The right to contest automated-decision making processes reduces the risk of exposing particular information on the Internet, for which the individual may not be satisfied of. The GDPR additionally has introduced therefore the right to be forgotten, in order for individuals to be able to remove unwanted information from the Interned, which may be posted due to automated-decision making processes.

The fourth risk, which is predictive analysis and profiling, on the other hand is debatable. As it has been concluded in Section 2.2. of the work – profiling in its nature is to be divided in two sub-groups and types, which, in the light of the GDPR are, in fact, regulated by two different Articles. While Article 22 on solely automated decision-making due to profiling requires explicit consent, the decision-making due to profiling with human intervention does not require for explicit consent to be acquired. Article 6 of the GDPR provides that the processing shall be lawful if:

[100] Ibid., Article 22.

> "The data subject has given consent to the processing of his or her personal data for one or more specific purpose"[101]

The issue with such difference lying between the wording of *explicit consent* and *consent* is that they do not fall under the same definition, although both are similar in nature and hold a very thin line in-between.[102] The Working Party issued guidelines in November of 2017 on the interpretation of the types of consent needed, by commenting on the understanding of explicit consent, as follows:

> "The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement."[103]

But, nonetheless, it does not pose an obligation for entities operating in online realm to receive written statements, as Working Party notes, it is possible to obtain explicit consent in various ways, as for sending an e-mail or to send an electronically signed document to the controller. [104] The difference within *explicit consent* and *consent* is the mere fact that explicit consent must be physically proven as opposed to the regular consent given, which may be given orally. Therefore, while Article 22 protects the rights of individuals regarding solely automated-decision making, including profiling, it does not cover all of the possible profiling cases, and by including human intervention, it becomes possible to avoid Article 22 provided safeguards, consequently escaping the obligation to request for explicit consent.

---

[101] Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[102] i-Scoop, Consent under the GDPR: valid, freely given, specific, informed and active consent, https://www.i-scoop.eu/gdpr/consent-gdpr/#Valid_consent_specific_consent_specific_purposes_and_purpose_limitation, Accessed on 27th of April, 2018.

[103] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018, p. 18. https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf, Accessed on April 27, 2018

[104] Ibid.

Conclusion

To conclude, the General Data Protection Regulation successfully addresses the risks to which Directive 95/46/EC initially has been exposed to. From the analysis carried out in the Thesis, it is to be observed that the power relationship between data controllers and data subjects is gradually shifting, in benefit of the data subjects. Along with the fact that the Regulation has been established to addess the particular issues, which include aspects of the online realm, controllers are obligated to provide data subjects with the opportunity to exercise rights which are granted by the Regulation, such as the right to obtain information, excersice the right of human intervention in automated-decision making processes, including profiling, therefore providing data subjects with more control over their personal data. Nonetheless, while data subjects are granted with a certain amount of control, it may cause difficulties to implement the Regulation to a significant part of data controllers, as it may turn out to be costly – specifically actions which include the hiring of a Data Protection Officer, and the providing of such options.

In regards to the question on whether General Data Protection Regulation better addresses the potential harm to data subjects rights arising from the collection of their personal data from the data trail left behind and of its use in data analytics – basing the conclusion on analysis carried out throughout the work, it is to be concluded that the Regulation sufficiently has targeted the issue in the most part. While most of the issues have been tackled – the lack of scope, the need for the right to be informed, as well as the right to gain control over personal data, findings of the analysis show that profiling lacks more detailed provisions, as under certain circumstances – by engaging individuals in the process of profiling – it may prove to be effortless to avoid the obligations which are laid down in the Regulations' Article 22 on automated-decision making and profiling. The avoidance of Article 22 results in individuals' not being protected by Article 22 (3) safeguards, which include the right to express views and obtain human intervention. Nonetheless, as the human intervention must be proven to be significant, the necessity to prove the involvement of being more than a guesture poses as an obstacle, but it does not make such an action impossible. In regards to data analytics, data subjects are to be informed by such on-going or potentially upcoming processes, as well as the data which has been collected, resolving the "right to privacy" breach issue.

All in all, the emergence of the General Data Protection Regulation deprives data controllers of the opportunity to use personal data for commercial purposes without disclosing the fact to the data subject. Therefore, from the perspective of data subjects, the Regulation indeed tackles the potential issues which could harm the rights of individuals successfully, on contrary, from the perspective of data controllers – the Regulation imposes limitations on actions which may have been possible to carry out prior Regulation,as well as adds additional costs for the enterprises, nonetheless, this work does not carry out alanysis on the impact of the Regulation to data controllers, therefore concluding that the Regulation provides sufficient protection of data subjects' rights in regards to data analytics from the personal data collected from data trail left behind.

Bibliography

Primary Sources

1. 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, of 24 October 1995
2. Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June.
3. Working Party document No WP 105: "Working document on data protection issues related to RFID technology", adopted on 19.1.2005.
4. The Universal Declaration of Human Rights, Adopted on 10 of December, 1948
5. R. V. Richards, Ontario Court of Appeal, [1999] O.J. No. 1420.
6. 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), Official Journal L 201 , 31/07/2002 P. 0037 – 0047.
7. Federacion De Comercio Electronico Y Marketing Directo (FECEMD) v. Administracion Del Estado, ("ASNEF")", C-469/10.
8. Google Spain SL v. AEPD (The DPA) & Mario Costeja Gonzalez, C-131/12.
9. Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C‑230/14.
10. Maximillian Schrems v. Data Protection Commissioner, Digital Rights Ireland, C-362/14,
11. Regulation (EU) 2016/679 of the European Parliament and of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
12. Casa Fleischhandel v. Bundesanstalt für landwirtschaftliche Marktordnung, Case 215/88, European Court of Justice ECR 2789 [31].
13. Criminal proceedings against Gunnar Nilsson and Others, C-162/97, European Court of Justice, 1998.
14. Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01).
15. Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018.

Secondary Sources

16. Peter Carey, Data Protection: Fourth Edition – A Practical Guide to UK and EU Law, Oxford University press, 2015.
17. Monika Kuschewsky, Data Protection & Privacy: Second Edition, Thomson Reuters, 2014.

18. Data State Inspectorate, DSI Recommendation "Personal data definition", Riga, 2008, p. 4.
19. Arnold Roosendaal, Facebook Tracks and Traces everyone: Like This!, Tilburg Institute for Law, 2011.
20. Erik Brynjolfsson, Lorin Hitt and Heekyung Kim, Strength in Numbers: How Does Data-Driven Decision-Making Affect Firm Performance?, 2011.
21. Omer Tene, Jules Polonetsky, Big Data For All: Privacy and User Control In The Age Of Analytics.
22. Andras Laszlo Pap, Profiling, Mining and Law Enforcement: Definitions, 50 Annales U. Sci. Budapestinensis Rolando Eotvos Nominatae 277, 2009.
23. Loekke Morel, Alex Wan der Wolk, Big data analytics under the EU General Data Protection Regulation, 2017.
24. Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, University of Colorado, 2010.
25. Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert, Data Protection and Privacy: The Age of Intelligent Machines, Hart Publishing, 2017.
26. DPO, Summaries of EU Court Decisions Relating to Data Protectoin 2000-2015, Data Protection Officer, 2000-2015.
27. Sandra Wachter,Brent Mittelstadt,Luciano Floridi, Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, International Data Privacy Law, 2017.
28. Bryce Goodman, Seth Flaxman, European Union regulations on algorithmic decision-making and a "right to explanation", Oxford Internet Institute, Oxford, 2016.
29. Tadas Klimas, Jūrate Vaičiukaite, The Law of Recitals in European Community Legislation, ILSA Journal of Intenraional and Comparative Law, 2008.
30. Jenna Burrell, How the machine 'thinks': Understandingopacity in machine learning algorithms, Big Data & Society, 2016.
31. Sandra Wachter,Brent Mittelstadt,Luciano Floridi, Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, International Data Privacy Law, 2017.
32. Information Commissioners Office, Feedback request – profiling and automated decision-making, p.7.
33. Agnese Buboviča, Arnis Puksts, Fizisko personu datu aizsardzības speciālista apmācība prezentācija 1. – personas datu tiesību attīstības jēdziens, termini un definīcijas, kas saistītas ar personas datu aizsardzību, 2018

Internet Sources

34. Data Protection Commissioner, EU Directive 95/46/EC - The Data Protection Directive, https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm,
35. European Commission, Applying EU law, https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en,
36. European Commission, What personal data is considered sensitive?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-

organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en,
37. Le VPN, Big Data: Why Do Companies Collect And Store Personal Data, https://www.le-vpn.com/why-companies-collect-big-data/,
38. Jason Morris and Ed Lavandera, Why big companies buy, sell your data, CNN, https://edition.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html,
39. BBC Webwise, What are cookies?, http://www.bbc.co.uk/webwise/guides/about-cookies,
40. The Guardinan, How Social Media Filter Bubbles And Algorithms Influence The Election, https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles,
41. EUGDPR, How Did We Get Here?, https://www.eugdpr.org/how-did-we-get-here-.html
42. Ivan Klekovic, EU GDPR vs. European data protection Directive, EUGDRP Academy, 2017, https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/,
43. EUGDPR, GDPR Key Changes, https://www.eugdpr.org/key-changes.html,
44. CSO from IDG, What does the GDPR and the "right to explanation" mean for AI?, 2018, https://www.csoonline.com/article/3254130/compliance/what-does-the-gdpr-and-the-right-to-explanation-mean-for-ai.html,
45. EUROPA, Guide to the Approximation of EU Environmental Legislation ANNEX I , 2015, http://ec.europa.eu/environment/archives/guide/annex1.htm, Accessed on 22nd of April, 2018.
46. Amberhawk, The Recitals are Essential to Your Understanding of the General Data Protection Regulation, 2016, http://amberhawk.typepad.com/amberhawk/2016/01/the-recitals-are-essential-to-your-understanding-the-general-data-protection-regulation.html, Accessed on 22nd of April 2018
47. I-Scoop, Data subject rights and personal information: data subject rights under the GDPR, https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/#Data_subject_rights_are_contextual_rights_obligations_and_circumstances
48. Slaughter and May, Tracking, watching, predicting… lawfully: responsible profiling under the GDPR, 2017, p .3. https://www.slaughterandmay.com/media/2536527/profiling-under-the-gdpr-september-2017.pdf,
49. i-Scoop, Consent under the GDPR: valid, freely given, specific, informed and active consent, https://www.i-scoop.eu/gdpr/consent-gdpr/#Valid_consent_specific_consent_specific_purposes_and_purpose_limitation,
50. GDPREU, Fines and Penalties, https://www.gdpreu.org/compliance/fines-and-penalties/
51. Electronic privacy information center, Privacy and Consumer Profiling, https://epic.org/privacy/profiling/,
52. European Union Agency for Network and Information Security, Article 29 Working Party, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/article-29-working-party
53. Council of Europe, European Commission against Racism and Intolerance, https://www.coe.int/t/dghl/monitoring/ecri/activities/GPR/EN/Recommendation_N11/Recommendation_11_en.asp