

TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Jesse Juusela

**Risk Analysis of GDPR: Three Legislative Issues in One Regulation**

Master's Thesis

European Union and International Law

Supervisor: Tanel Kerikmäe, PhD

Tallinn 2018

I declare that the I have compiled the paper independently  
and all works, important standpoints and data by other authors  
have been properly referenced and the same paper  
has not been previously been presented for grading.  
The document length is 17138 words from the introduction to the end of conclusion.

Jesse Juusela .....  
(signature, date)  
Student code: 163734  
Student e-mail address: jesse.juusela@gmail.com

Supervisor: Tanel Kerikmäe, PhD  
The paper conforms to requirements in force

.....  
(signature, date)

Chairman of the Defence Committee:  
Permitted to the defence

.....  
(name, signature, date)

# TABLE OF CONTENTS

ABSTRACT .....	4
INTRODUCTION .....	5
1. GDPR DOESN'T SUPPORT THE LEGAL AIM OF THE SINGLE MARKET AND PROTECTS DATA UNNECESSARILY AGAINST THE PRINCIPLE OF PROPORTIONALITY .....	8
1.1. GDPR Does Not Support the Legal Aim of the Single Market .....	8
1.2. GDPR Protects Personal Data Unnecessarily Against Principle of Proportionality .....	11
2. LEGISLATIVE DRAFTING OF THE GDPR IS POORLY MADE AND IT MAKES IT UNCERTAIN AND FRAGMENTED .....	16
2.1. Delegated Acts in Essential Parts of the Regulation .....	16
2.2. Data Transfer and Confusion over Standard Contractual Clauses .....	18
2.3. GDPR Gives Fragmented Codification and Fails to Be One-Stop-Shop .....	25
3. GDPR UNDERMINES THE FREEDOM OF EXPRESSION AND INFORMATION PROVIDED BY ECHR, UDHR, THE CHARTER AND U.S. FIRST AMENDMENT.....	28
3.1. Freedom of Expression and the Right to Information: ECHR, UDHR and the Charter ....	29
3.2. Case Law: C-131/12 Google Spain v Mario Costeja González .....	39
3.3. First Amendment of the United States Constitution.....	41
CONCLUSION .....	45
LIST OF REFERENCES .....	49

## **ABSTRACT**

European General Data Protection Regulation (GDPR) is a tensely waited comprehensive piece of legislation. This thesis doesn't explain what the regulation means for companies or how to prepare for it. This paper aims to evaluate this upcoming regulation and its effects on EU's fundamental aims, principles and freedoms. The author identifies three legislative issues in the regulation and goes through them in separate chapters. The author strives to find answers to those issues by analysing relevant legislations and related landmark case laws. The author makes opinionated statements linked to the identified legislative issues, portraying vision of phenomenon where freedom of expression and information are reduced from the way of protectionism.

**Keywords:** GDPR Issues, Unnecessary Protection, Data Transfer, Fundamental Rights

## INTRODUCTION

Regulation (EU) 2016/679 European General Data Protection Regulation (GDPR) was done in Brussels on 27 April 2016 and comes into force 25<sup>th</sup> of May 2018. It is a comprehensive and ambitious piece of legislation to repeal Directive 95/46/EC and its over twenty years run in EU's data protection. New legislation is certainly needed to guide the Union's data protection in new digital era. Author evaluates this new coming regulation and its effects on EU's fundamental aims, principles and freedoms.

GDPR is a burning topic in business tables, academic writings and medias. It sets new comprehensive frames for concepts like processor, processing, controller, profiling, personal data, consent, filing system, personal data breach, data portability and cross-border processing. To comply with this regulation, it is demanded to take a risk-based approach to data protection and follow privacy by default orientation. Transparency and accountability need to be practiced while only gathering as much data that is necessary for the completion of a specific aim. When personal data was earlier understood as a social security number and biometric identification, GDPR places email addresses, photos, IP addresses, location data and online behaviour as personal data that will be protected. Giving consent must be simple and withdrawing it must be just as easy. GDPR provides data portability aiming to give the real power over own personal data for the individuals, it is one of the new ambitious concepts of this regulation. Just compliance itself is not enough for this regulation, but the controller or processor must also be able to demonstrate that compliance for authorities.<sup>1</sup>

Drafters of GDPR do not want anyone to be able to go around it, so they reach their data protecting arm to organizations based outside of the EU that offer goods or services to EU residents, processes their data or monitors behaviour. Service providers that process data

---

<sup>1</sup> The Eu General Data Protection Regulation (GDPR), it governance, Accessible:  
<https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation> , 19 March, 2018

concerning EU residents on behalf of other organization will also fall under this regulation no matter where they are located. An easy example of this kind of processor is a cloud service provider offering data storage.<sup>2</sup>

GDPR continues with strict administrative burdens assigning 72 hours' time to report to authorities when any kind of data breach is detected towards personal data. This is continued with an order to tell the individuals impacted also if the breach constitutes a high risk to their rights and freedoms. GDPR sets a mandatory appointment of a data protection officer for organisations with over 250 employees, organizations involved in high-risk processing, public authorities and organizations processing special categories of data. One real conversation piece of GDPR is the penalties up to 20 million euros or 4% of the annual turnover, whichever is higher.<sup>3</sup>

Where ever you go or whatever you read, GDPR is likely to be mentioned and these are the streamlining points that everyone talks about. This thesis does not explain what the regulation means to you or to your company and how you should prepare for it. It is the aim of the author to go deeper in the fundamentals of the European General Data Protection Regulation to see and analyse how it fits into our society, economy, fundamental values and politically charged atmosphere. This evaluation is based on related legislation, rules and relevant case law.

Three legislative issues detected in the regulation by this thesis are:

- 1) GDPR does not support the legal aim of single market and protects data unnecessarily against principle of proportionality.
- 2) Legislative drafting of the GDPR is poorly made and it makes it uncertain and fragmented.
- 3) GDPR undermines the freedom of expression and information, provided by ECHR, UDHR, THE CHARTER and U.S. First Amendment.

---

<sup>2</sup> The Eu General Data Protection Regulation (GDPR), its governance, 19 March, 2018, Accessible: <https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation>

<sup>3</sup> Nadeau M.(2018) General Data Protection Regulation (GDPR) requirements, deadlines and facts, CSO, Accessible: <https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html>, 18 February 2018

The author will look at these legislative issues in the next chapters one by one. Relevant legislations and their relations towards these identified legislative issues are in the centre of this paper. Landmark cases of data protection will be analysed for the support of creating comprehensive portrait of the GDPR's success and fails. This new data protection legislation is a product of long political debate and the author makes an opinionated notice of that linking the identified legislative issues to the rising phenomenon where freedom of expression and information are reduced from the way of swaddling protectionism of individuals.

# **1. GDPR DOESN'T SUPPORT THE LEGAL AIM OF THE SINGLE MARKET AND PROTECTS DATA UNNECESSARILY AGAINST THE PRINCIPLE OF PROPORTIONALITY**

EU is created for the purpose of a better single market for all, but a legislation like GDPR seems to work against this core aim of the single market and for the disadvantage of Europe's economy. EU has barely peeked its nose from the latest financial crisis and GDPR insists on taking the stool under the competitive asset of data economy in order to protect all possible personal data ever imagined. In author's humble opinion this regulation will kill innovation and entrepreneurship and move business away from EU.<sup>4</sup>

Commissioners are distant representatives of people of European Union and the excessive legislation is one of the core things that is causing anti support Union wide. GDPR has added fuel to those flames making member state citizens feel like their views and values are not being manifested correctly.<sup>5</sup> The author does not see GDPR as embodiment of the will of European people but as a travesty of ideological data protection activist. In contrast, EU does very little to regulate cryptocurrencies and lets anyone create their own cryptocurrencies, raise money for it in deceiving ways and then dump it leaving thousands in financial ruin. Instead, EU wants to protect the customers from Facebooks targeted yoga ads.

## **1.1. GDPR Does Not Support the Legal Aim of the Single Market**

We did not want to regulate privacy over freedom of speech in our analogue world before internet. Internet has been a huge stepping stone for advantage of human kind providing it with

---

<sup>4</sup> EU Commission, The European Single Market, Accessible: [https://ec.europa.eu/growth/single-market\\_en](https://ec.europa.eu/growth/single-market_en). 7.5.2018

<sup>5</sup> Clark R. (2017). What European Really Thing of the EU, The Spectator, Accessible: <https://www.spectator.co.uk/2017/07/what-europeans-really-think-of-the-eu/>. 7.5.2018

unseen possibilities to share and to receive information freely all over the world. When scientific discipline advances there usually is need for advancements in regulations also. The author thinks that where European General Data Protection Regulation goes off the rails, it is not just regulating and guarding the data protection but trying to pull the brakes on advancement of free speech and information at the same time. Throughout history the open and free societies are the most prosperous ones, more educated and more productive. It is a weird step backwards from drafters of GDPR to shackle that creative power mostly for disadvantage of the EU and its people.

International Chamber of Commerce ICC identifies how bad this regulation could be for the economy and undertakings in a single market trying to keep up with innovative uses of data. ICC encourages that the regulation should better identify the ways for data controllers to process individual's data lawfully by establishing legitimate interest. This would give undertakings necessary legal clarity that would lead to voluntary transparency and decrease the use of loopholes.<sup>6</sup>

Share economies are a good example how twenty-first century economy is free data driven and people are signing up in increasing manner. For example, Uber cars are popular around the globe where average people share their information and invite people to ride in their cars.<sup>7</sup> Airbnb is superseding conventional hotels world-wide. Its users share their names, locations, interests, household pictures and then invites strangers to live in their apartments. These shared economies are replacing the old conventional businesses and interests and what is central in them is that people willingly share their information, lifestyle and property with the world-wide economical network.<sup>8</sup> Tremendous popularity of these social share economies begs the question who wants GDPR to over protect the individual data and do so on the expense of expression and information.

GDPR has kept EU guessing for a long time and will continue to do so. This regulation skyrockets the administrative burden and cost when preparing for the regulation and in future when maintaining the compliance. GDPR has shifted the focus from good security to protection

---

<sup>6</sup> ICC commission on the Digital Economy, (2015). ICC Position on Legitimate Interest,

<sup>7</sup> Wallsten S. (2015), *The Competitive Effects of the Sharing Economy: How is Uber Changing Taxis?* Technology Policy Institute, Washington, DC

<sup>8</sup> Zervas G., Proserpio D., Byers J.W. (2017). *The Rise of the Sharing Economy: Estimating the Impact of Airbnb on the Hotel Industry*, *Journal of Marketing Research*, Vol54, No. 5, 687-705

practices. Previously data protection was seen as good internet security that safeguards against the criminals and misusers from exploiting sensitive data. This is why companies focused on cyber security protect the information. With GDPR the focus has shifted from protection against criminal and misuse of data to avoidance of sanctions and obsessively finding compliance gaps of GDPR. While EU companies are seizing some of their operations, dumping data that is not 100% necessary and employing consultants like never before, alarming percentage of them still feel they are not going to be able to comply. According to a report done by Ovum at the end of 2015, 66% of global IT companies were re-calculating the viability of their business strategies in EU because of the GDPR. Over 50% of the companies in that survey did not believe that they can meet the compliance requirements and will be fined.<sup>9</sup>

GDPR casts its shadows on EU trade deals as well, making it uncomfortable for the data driven economy of the single market. July 2017 marks the date of EU-Japan summit that moulds basis for the Japan EU Economic Partnership Agreement. Rules on data privacy are on the centre of that agreement and its success. Global data flow is in the centre of this deal and certainly with others as well. GDPR wants to be a land mark in data protection but the question is whether overambitious shrinks the possibilities of harmonious economical trade.<sup>10</sup> Svetlana Yakovleva writes in her Cambridge University Press publication that These General Agreements on Trade in Services GATS are necessary for EU's economy and GDPR might set too heavy burden on them. She notes that in order to complete these agreements EU might have to take a step back in its privacy regulation.<sup>11</sup> A concern of conflicting standards and principles between open markets is validly risen by Hosuk Lee-Makiyama, the Director of European Centre for International Political Economy ECIPE. He states that in pursuit of privacy GDPR is in verge of overreaching its objective making over strict standards for handling of personal data. He refers to studies that already show GDPR's negative impact on EU's economy and trade fighting against the purpose of the single market.<sup>12</sup>

George W. Voss writes in his article about GDPR's aim to further EU's digital agenda and provide economic advantages for single market. He writes that one of GDPR's aims is to

---

<sup>9</sup> Macrae A. (2016). GDPR- the good, the bad and the ugly, tripwire, Accessible:

<https://www.tripwire.com/state-of-security/security-awareness/gdpr-the-good-the-bad-and-the-ugly/>, 26.02.2018

<sup>10</sup> Bartl M., Irion K., (2017). The Japan EU Economic Partnership Agreement-. Flows of Personal Data to the Land of the Rising Sun, University of Amsterdam, CSECL, 1

<sup>11</sup> Yokovleva S. (2017). Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"? Cambridge University Press

<sup>12</sup> Makiyama H. L. (2012). Digital Trade in the U.S. and Global Economies', ECIPE

increase trust in EU's information services while protecting fundamental rights. Voss repeats EU's digital commissioners Neelie Kroes statement about single market, that new and bigger market need digital agenda that provides economic advantages. Kroes states that it is the trust that overpoweringly provides those advantages, which is not in line with the opinion of the author of this thesis. Author's opinion is that GDPR manages to promote only one fundamental right while stepping on others and declines EU's information services since undertakings will move their products and services in to more fertile breeding grounds.<sup>13</sup>

## **1.2. GDPR Protects Personal Data Unnecessarily Against Principle of Proportionality**

Social media is another great demonstration of the state of mind of the people. Vast majority of the people who have access to internet<sup>14</sup> is part of some social media platform, usually multiple.<sup>15</sup> Social media in its core means sharing your private information, pictures, locations, interests, ideas, profession, possessions et cetera. It seems to be an overpowering trend that people don't want to protect this kind of information at all cost but actually actively share it through internet platforms. It is undoubtedly sure that information that is sensitive, concerns a child, is offensive, is racist or hate speech must be censored accordingly by law. Author advocates that, but we already have laws covering those issues, and if they are not enough they should be made stronger but GDPR goes after data that it should not go after.

A regular sports club, a local football team for example, shares a picture on its website of the team playing at the summer practice. The point of this picture is to show that it is fun to join local social sporting activities and more people should join. Now if one person who is seen in the picture feels that his or her hair or outfit does not look good in this picture it is according to GDPR personal data of this person and the person is allowed to claim for the erasure of the

---

<sup>13</sup> Voss G., W. (2012). Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments, Business Law Today, Accessible: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/busiltom2012&div=96&id=&page=>. 10.5.2018

<sup>14</sup> Internet World Stats, (2017). World Internet Users and 2018 Population Stats, Accessible: <https://www.internetworldstats.com/stats.htm>. 7.5.2018

<sup>15</sup> Statista. Number of monthly active Facebook users worldwide as of 4th quarter 2017 (in millions) (2018) Accessible: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>. 7.5.2018

picture since it is against his or her data privacy.<sup>16</sup> The author argues that it is more important for the community to be able to present opportunities like this for its people to come and join the social, cultural or sporting activities than it is to protect the information that in this picture this person is playing football.

United Nations Universal Declaration of Human Rights Article 19, Charter of Fundamental Rights of the European Union Article 11, and European Convention on Human Rights Article 10 all state that freedom of expression should not be limited regardless of frontiers. Data protection is also a fundamental right and should be protected but GDPR seems to protect irrelevant data over relevant expression. Article 4 point 4 of GDPR sets new boundaries for term profiling. Analysing someone's financial wealth, work performance, interests, behaviour or location is profiling according to that Article.<sup>17</sup> Knowledge of financial wealth, salaries et cetera is important information and freedom to know those things is important for the people. Knowledge of salary is important information that guides person's decisions to pursue career, select the country to live, to mirror own wealth and plan the future of own financial survivor. If this information is hidden for a severe reason it is justified, but if it is hidden as a default as GDPR suggests the balance is not right. In default situation it is more important for the masses to have this information available than for an individual to hide it just because they feel like it. Hiding financials makes it easier to shelter hidden agendas in politics or economical deals for example.

Money and wealth is a force that drives the whole population and single market is created to promote that. Single market needs free information as default and GDPR protects privacy over information with no proportioned reason. Job performance is not allowed to be analysed in discriminating way. GDPR wants that any personal data cannot be used to analysing job performance if the individual so wants.<sup>18</sup> Prosperous data driven economy is built on education, personal skills and experience. In authors opinion it is more important for the citizens to know that an applicant for fireman is suspected three times of arson, but not charged, than for the individual to be able to hide it and get a career as a firefighter. It is more important for the citizens to know about the financial ruin created by a person who applies for bank's financial advisor than it is for the individual to hide to be able to get the specific job. It is more important

---

<sup>16</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC

<sup>17</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC

<sup>18</sup> Ibid

for citizens to know about the two-time alleged fraud of individual running for public office than it is for that individual to be able to seal that information and get the position. Hiding all personal information as default is not in balance with freedom of expression and right to information in author's opinion.

Principle of proportionality<sup>19</sup> in accordance with consolidated version of the Treaty on European Union Article 5 states that legislative measures should not go beyond what is necessary to achieve pursued aims. GDPR aims to protect individual's data in accordance with other fundamental rights. It is an opinion of the author that to give comprehensive data protection for individuals does not mean hundred percent coverage. It can be stated that individual's data is comprehensively protected even though some irrelevant information is not covered. This is where the author gives notice to the principle of proportionality. For EU to achieve comprehensive data protection it is not necessary to go after all this data that the regulation is now aiming to protect. The author sees that this regulation reflects the currently growing political mindset where free speech is stumped upon by over sensitive snowflake generation<sup>20</sup> that demands safe spaces and political correctness to over-run the freedom of speech. GDPR goes far beyond what is necessary to attain the balanced well-deserved level of protection over personal data and stretches boundaries of principle of proportionality.<sup>21</sup>

Later, the author will talk about the United States Constitution's First Amendment<sup>22</sup> and Sedler realisation for its origins. To summarize, Sedler finds that U.S.' strong constitutional protection of freedom of speech is manifestation of American humanistic values. That value is based on the history, experiences and culture of the American people. This observation serves the founding of this thesis that good legislation mirrors the humane sense of justice and this reflection ensures that the subjects of law will want to value, respect and obey the rules and not try to fight against them. GDPR walks all over free speech in its mission to protect individual's data by any cost.<sup>23</sup>

---

<sup>19</sup>EUR-LEX, Access to European Union Law, proportionality principle, Accessible: <https://eur-lex.europa.eu/summary/glossary/proportionality.html>. 7.5.2017

<sup>20</sup> Urban Dictionary, Generation Snowflake, Accessible: <https://www.urbandictionary.com/define.php?term=generatiossnowflake>. 7.5.2018

<sup>21</sup> EUR-LEX, Access to European Union Law, proportionality principle, Accessible: <https://eur-lex.europa.eu/summary/glossary/proportionality.html>. 7.5.2017

<sup>22</sup> United States Constitution. First amendment. FREEDOM OF RELIGION, SPEECH, PRESS, ASSEMBLY, AND PETITION. Passed by Congress September 25, 1789, Ratified December 15, 1791. The First 10 Amendments from the Bill of Rights. Accessible: <https://constitutioncenter.org/interactive-constitution/amendments/amendment-i>. 7.5.2018

<sup>23</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC

Later this will be connected to the fact that this regulation is going to have a hard time with U.S. companies, but this chapter focuses on the argument that EU's people and undertakings are virtually in panic and incredulity is a strong factor that this regulation does not mirror the values of EU's people by protecting data that does not need protecting, especially over free speech.<sup>24</sup>

Recent events around the social media giant Facebook are a cold hard presentation showing how little people around the world care about protecting any kind of user data that GDPR so badly wants to protect. Cambridge Analytica data breach was in news all around the globe in every news outlet. The story of how Facebook had collected user data like location, political interests, interests, hopes, fears and ideas people relate to and sold that data to firm Cambridge Analytica,<sup>25</sup> that tried to use the data in multiple political fields. To put it in scale this breach concerned data of 87 million users around the world making this a valid research object with such a high number of research targets.<sup>26</sup>

Facebook's market share dropped for a short while as investors thought this data breach might have some impact on the company's value since it was hyped in news constantly. However, the drop was a short hiccup in the share value since the event did not have any effect on users. In about a month Facebook value was back where it started before the breach scandal,<sup>27</sup> profits are rising, and user numbers are up. The author wants to point out these events in pursue on finding out whether GDPR protects the relevant personal data embodying the will of the Union's people or has it drifted away from the original aim. Right after going through one of the world's most reported scandals, Facebooks informed its monthly active users in first quarter rose to 2.2 billion, meaning 13 percent rise from a year earlier.<sup>28</sup>

This data breach scandal does not seem to be resulting in any data privacy law changes in U.S. GDPR compliance was mentioned in Capital Hill where Facebook CEO Mark Zuckerberg

---

24 Sedler R. (2006). An Essay on Freedom of Speech: The United States versus the Rest of the World, Michigan State Law Review, 377-378

25 Ingram D., Vengattil M. (2018). UPDATE 3-Facebook's rise in profits, users show's resilience after scandal, CNBC, Reuters, Accessible: <https://www.cnbc.com/2018/04/25/reuters-america-update-3-facebooks-rise-in-profits-users-shows-resilience-after-scandals.html>. 5.5.2018

26 Ibid

27 Nasdaq, Facebook Inc Class A Common Stock 3month. Accessible: <https://www.nasdaq.com/symbol/fb>. 10.5.2018

28 Ibid

testified before Congress.<sup>29</sup> Zuckerberg's answer was that they will comply with the Regulation but let's see how it will all play out.<sup>30</sup> This statement shows two things; firstly, that GDPR is so open ended and unclear that even world's largest companies haven't figured it out and secondly, Facebook will do all in its power to slip through the regulation and leave smaller players to comply with it.

Where this regulation really shoots off the target, in author's opinion, is the presentation of same over protecting rules for all different instances that have different aims and purposes. As will be mentioned more later, this regulation not only protects un-necessary data from media giants like Facebook and Google, but it gives same requirements for governmental institutions like small remote towns and their little league football teams.

---

<sup>29</sup> Volz D., April 10. 2018, Reuters, Facebook's Zuckerberg Faces Senate Hearing but Little Hope for Action <https://www.reuters.com/article/us-facebook-privacy-congress/facebooks-zuckerberg-faces-senate-hearing-but-little-hope-for-action-idUSKBN1HH08G>

<sup>30</sup> Jeong S. (2018). Zuckerberg says Facebook will extend European data protection worldwide- kind of. Accessible: <https://www.theverge.com/2018/4/11/17224492/zuckerberg-facebook-congress-gdpr-data-protection>. 2.5.2018

## **2. LEGISLATIVE DRAFTING OF THE GDPR IS POORLY MADE AND IT MAKES IT UNCERTAIN AND FRAGMENTED**

GDPR is like a day when you wake up with a left foot, it has all the theoretical potential to be a good, creative and successful day but the early mistakes will probably end up messing the whole day. Amounts of personal data is increasing with the usage of internet and it is understandable that regulators need to react and see that the laws are suitable for the changing surroundings. Data protection in general is important and there are sectors where tight laws are needed to cover them. Aims behind the European General Data Protection regulation GDPR are valid and successfully drafted data protection law would be a great mile stone and advantage for all. GDPR is nothing like that.

A good legislation rarely puts 28 nations on their toes, but GDPR manages to do that. This regulation has sparked much confusion and differing opinions EU wide, even among the specialist of the field. This confusion has been going on for two years and does not seem to clear up anytime soon since there will be upcoming delegated acts in central positions of the law and many aspects left open for member states to handle.

### **2.1. Delegated Acts in Essential Parts of the Regulation**

Proposal of the General Data Protection Regulation is based on the Article 16(1) of the Treaty of Functioning of the European Union (TFEU) which provides “everyone has the right to the protection of personal data concerning them”<sup>31</sup>. This proposal has raised not only practical issues but legislative ones. Legal scholars have pointed out as one of the legislative issues that the Commission’s position on this is not justified, and that the Regulation overpowers Commission’s competence in regulative areas. This can be seen as some of an institutional shift since

---

<sup>31</sup> Consolidated Version of the Treaty on the Functioning of the European Union, TFEU, Art 16(1)

Commission ordinarily only gives delegated acts in non-essential elements of the given legislation.<sup>32</sup> The author raises the question if an extensive authorization for Commission to give delegated acts is in accordance with the Article 290 of the Treaty on the Functioning of the European Union that provides “the essential elements of an area shall be reserved for the legislative act and accordingly shall not be the subject of a delegation of power”.<sup>33</sup>

As delegated acts are designed to amend or supplement non-essential elements in EU legislative acts, it is raising questions to see the Commission granted with delegative acts in central legal issues of the Regulation in Articles 12 and 43 and indirectly in Articles 25 and 42. One problem with leaving essential parts of the regulation to wait for the delegative act is that these provisions in regulation will remain unclear until adoption of these delegative acts. If there are too many delegative acts and implemented act to be done it is likely that the Commission cannot do them fast enough after the enactment of the GDPR. Also, the political wills and complexity of these legal issues will delay the adoption of the delegated acts. With GDPR there are fundamental freedoms of data protection, freedom of speech and freedom to provide services colliding.<sup>34</sup>

Lisbon Treaty amending the Treaty on European Union and the Treaty establishing the European Community made significant changes to ways Commission can make delegated acts. However, the Article 290 as pointed out still gives Commission power to give delegated acts to supplement the legislative acts in non-essential elements. One of the reasons is the fast schedule given for the European Parliament and Council to raise objection to these delegated acts, which normally is just a couple of months. When a too wide part of the legislation is given by the Commission’s delegative act, this timeframe for the European Parliament and Council to find technical problems from it is too short and there will be no time for the evaluation of the concrete functional errors. Delegated acts will complicate regulatory choices and distort the politics of the process.<sup>35</sup>

Gerrit Hornung states in his thesis that the overpowering of Commission with delegation power concerning GDPR in areas of data protection by design and by default Art 25 and in Articles 42

---

32 Hornung G. (2012). A General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft, of 25 January 2012, 9 SCRIPTed 64

33 Consolidated Version of the Treaty on the Functioning of the European Union, TFEU, Art 290

34 Kuner C. (2012). The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Bloomberg BNA Privacy and Security Law Report, 23

35 Craig P., De Burca G. (2011). EU Law Text, Cases and Materials. 5<sup>th</sup> ed. New York: Oxford University Press, 133-138

and 43 of certifications and certification authorities, is extremely worrying.<sup>36</sup> GDPR article 25(3) reads “*An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements*” add this with Article 42(5) stating that “*A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43*” and point 8 of the Art 43 states that “*The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1)*”<sup>37</sup> It surely looks like GDPR is only naming basic principles and assigns Commission to come up with many implementing acts that really determine the legal issues. Any of these legislative questions won’t be fully answered before Commission starts giving these delegated acts and dominos start to fall on their places.

Article 12 is about the transparent information. Delegated Act in here has great potential to put different member states and different organizations to start using multiple different ways for transparent information before Commission decides to create these standard icons and make all the previous efforts invalid. As the author has pointed out, the first drafts of GDPR were made in 2012 and the final version has been there for almost two years. In this author’s opinion there has been plenty of time to make these standardizations in pursue of creating good legislation.<sup>38</sup>

## **2.2. Data Transfer and Confusion over Standard Contractual Clauses**

In 2017, when GDPR was already given, the EU foreign trade in goods was 3735 billion EUR. With such a high number everyone must agree that the extra-EU trade is a central part of the single market’s functioning and should be considered in related legislation.<sup>39</sup> GDPR was given in

---

<sup>36</sup> Hornung G. (2012). A General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft, of 25 January 2012, 9 SCRIPTed 64

<sup>37</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC, Official Journal of the European Union

<sup>38</sup> Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC, Official Journal of the European Union

<sup>39</sup> Eurostat, Statistic Explained, (2018). International Trade in Goods, Accessible: [http://ec.europa.eu/eurostat/statistics-explained/index.php/International\\_trade\\_in\\_goods/fi](http://ec.europa.eu/eurostat/statistics-explained/index.php/International_trade_in_goods/fi) 1.5.2018

April 27, 2016 and while writing this, there is only a month left in its two-year transitional period. However, the smooth continuance of the extra-EU trade has not sorted out.<sup>40</sup>

Recital 101 of the regulation says that personal data flows to Union and out of it are necessary for the sake of international trade and cooperation. Recital 108 states that if there is no adequacy decision the controller or the processor should take measures to compensate for the lack of data protection in third country with appropriate safeguards for data subject. Such appropriate safeguards are standard data protection clauses adopted by the Commission or standard data protection clauses adopted by a supervisory authority and contractual clauses authorised by a supervisory authority.<sup>41</sup> What does and what will it mean concretely, that seems to be up for a question.

Almost every consulting firm and every law firm in Europe have spent the last two years giving opinions, advises and guidelines on how to prepare for the GDPR, what can be done, what is forbidden and what is required. While writing this, the author works also as a lawyer in a Finnish consulting firm and spends hundred percent of his time on issues related to GDPR. Author's own clients vary from SMEs to large corporations and governmental institutions. Issues within these clients vary but mass confusion and lack of instructions from Commission and national authorities can be seen everywhere.

A law firm Bryan Cave Leighton Paisner has presented a related post via their web page in a form of a basic advice written by one of their partners David Zetoony. In this advice he answers to a widely asked question, does old controller-processor standard contractual clauses<sup>42</sup> apply when GDPR starts to apply in 25<sup>th</sup> of May 2018. Zetoony's answer is that there are two additional requirements to be fulfilled according to GDPR. First, controller based on EEA must before transferring data to processor outside the EEA take steps to ensure that the jurisdiction in which data is going does have adequate level of protection, meaning level of protections afforded by the laws of the country.<sup>43</sup>

---

<sup>40</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC

<sup>41</sup> Ibid

<sup>42</sup> European Commission, Data transfer outside the EU, decision 2010/87/EU, Accessible: [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en). 5.5.2018

<sup>43</sup> Zetoony D., (2018). GDPR: The Most Frequently Asked Questions: Are the Standard Contractual Clauses Enough? Accessible: <https://www.bryancave.com/en/thought-leadership/gdpr-the-most-frequently-asked-questions-are-the-standard.html>. 5.5.2018

Zetoony continues that a legally binding and enforceable instrument can be created between governments for data transfer and gives an example of EU-US Privacy Shield. At this point of time when so called Schrems II case is waiting to happen the long-lasting solution to rely on Privacy Shield is fragile when its predecessors called Safe Harbours ragged remains are still on display.<sup>44</sup> EU-US Privacy Shield is currently being examined by the Article 29 Working Party.<sup>45</sup> This is pondered more in other parts of the thesis.

Zetoony's next answer is also in our great interest; "most common, is the use by the contracting parties of contract provisions that have been pre-approved by the EU Commission as contractually guaranteeing an adequate level of protection." Relating to this Zetoony states the second requirement imposed by the regulation. According to Zetoony, every service provider agreement has to contain 13 specific contractual provisions. EU-Commission's pre-approved standard contractual clauses<sup>46</sup> have been popular in the past and many still think these are valid for the new regulation. This is the sole point of the author that opinions around this are multiple and uncertainty remains around this critical phenomenon. Zetoony ends his advice stating that these EU-Commission's pre-approved standard contractual clauses are not valid anymore since they only incorporate some of the Article 28 requirements.<sup>47</sup>

Anna Myers writes about the same topic in The International Association of Privacy Professionals (IAPP) publication. Myers writes in her publication that GDPR provides cross-border data transfer outside EU/EEA by the way of appropriate safeguards similarly to Directive 95/46/EC. Publication states that in absence of an adequacy designation transfer can be done if controller utilizes certain safeguards under Article 49.<sup>48</sup>

---

44 Ibid

45 Bertermann N. ed (2016). EU General Data Protection Regulation, A First Introduction describing the major changes compared to today's German law, Practice Group IT & Digital Business

46 European Commission, Data transfer outside the EU, decision 2010/87/EU, Accessible: [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en). 5.5.2018

47 Zetoony D., (2018). GDPR: The Most Frequently Asked Questions: Are the Standard Contractual Clauses Enough? Accessible: <https://www.bryancave.com/en/thought-leadership/gdpr-the-most-frequently-asked-questions-are-the-standard.html>. 5.5.2018

48 Myers A., (2016). Top 10 operational impacts of the GDPR: Part 4- Cross-border data transfer, The International Association of Privacy Professionals (IAPP), Accessible: <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/> 5.5.2018

Two of these mentioned safeguards are standard data protection contractual clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2). Other is the standard data protection contractual clauses adopted by supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2). Publication continues that new changes under GDPR reduces the administrative burden around the standard data protection contractual clauses since these do not require prior authorization of supervisory authorities and such clauses can be adopted by the European Commission as well as by national supervisory authorities. Existing standard contract clauses may remain valid, but GDPR leaves open the possibility of repealing them.<sup>49</sup> Simona Chirica lists the same terms for the data transfer outside EU/EEA. He refers to use of standard data protection clauses adopted by Commission or supervisory authority but does not clarify the timely scope. Does he mean new ones that are hopefully coming in some point or use of old ones.<sup>50</sup>

20 days to go until GDPR starts to apply and on Commission's official web page there is still decision 2010/87/EU given as a way to international data transfer using model contract, no mention of it ending or no mention for the replacement.<sup>51</sup> Article 98 of the Regulation (EU) 2016/679 General Data Protection Regulation states that Commission shall, if appropriate, give legislative proposals to amend other Union legal acts on the protection of personal data, special emphasis given to the free movement of such data.<sup>52</sup> The author would like to think that this means that the standard data protection contractual clause by decision 2010/87/EU would still be valid until renewed so that the trade in the single market could continue effectively.

Authors Lisa J. Sotto and Cristopher D. Hydak have published an article in Corporate Compliance Insight under title of EU-US Privacy Shield: A Path Forward, Risks Benefits and the Future of the Agreement. The authors state that some US companies are wondering whether to sign in for the new Privacy Shield or use the Standard Contractual Clauses that they had to start using in between when the safe harbour had cancelled, and Privacy Shield was not concluded. The reason for US companies' hesitation is the looming thought that Privacy Shield will be

---

<sup>49</sup> Ibid

<sup>50</sup> Chirica S. (2017). The main novelties and implications of the new general data protection regulation, *perspectives of Business Law Journal*, Vol 6 issue 1, 14-15

<sup>51</sup> European Commission, Data transfer outside the EU, decision 2010/87/EU, Accessible: [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en). 5.5.2018

<sup>52</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC

cancelled by the ECJ in near future. With this statement the authors clearly have an opinion that the old standard contractual clauses will be valid with the GDPR.<sup>53</sup>

As pointed out earlier, the author of this thesis currently works as a lawyer in a Finnish consulting firm and deals mainly with GDPR issues. It is highly unlikely that Finland is relatively behind related to this regulation and its confident compliance than other EU member states and Finland certainly is confused overall, particularly about the transfer outside EU/EEA area. This uncertainty is true with authorities, governmental organisations and large corporations with multiple inhouse lawyers. The author has pointed out many times already that GDPR leaves vital parts for Commissions delegated acts, for later decisions and certifications or just blank. Regulation was a result of years of compromising, it was made final almost two years ago<sup>54</sup> and still when the transitional period is about to end the legislators and Commission have not finalised the entirety to the state of clear and usable, not even close. Delegated act not made, certification bodies not placed, certifications not made, clarifying decisions still underway, Decisions of countries with adequate level of protection not renewed, standard contractual clauses behind doubt and uncertainty and not a clue how to stitch this all together with the freedom of speech and right to information.

To strengthen this view of uncertainty in whole Union it must be noted that governments of different member states are giving different guidelines for the usage of standard contractual clauses. To give an example, data protection agencies of member states like UK, Estonia, Netherlands and Sweden are recommending that companies continue using old standard contractual clauses hinting that they are not going to rush evaluate complaints before clear replacements are given. In contrast France for example is already investigating complaints related to these. Whatever is the message of a member state it is always possible for European Data Protection Agencies to challenge that.<sup>55</sup>

Bräutigam Tobias and Miettinen Samuli have written in Helsinki University law faculty's release that after case Schrems standard contractual clauses have become widely used form of

---

<sup>53</sup> Sotto L. J., Hydak C. D. (2016). EU-US Privacy Shield: A Path Forward, Risks Benefits and the Future of the Agreement, Hunton & Williams, Corporate Compliance Insight, 6

<sup>54</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC, Official Journal of the European Union

<sup>55</sup> Weiss M. A., Archick K. (2016). U.S.-EU Data Privacy: From Safe Harbour to Privacy Shield, Congressional Research Service, 15

transferring data outside the EU/EEA and still remain so. They also point out other interesting piece of information that author sees relevant.<sup>56</sup> As Zetoony had mentioned old standard data protection contractual clause covers some of the regulations requirements but not all. Bräutigam and Miettinen state that standard contractual clauses cannot be altered. One of the possible solutions that the author himself has wondered is to use the old contractual clauses adding the GDPR Article 29 requirements to it. To challenge the opinion of Bräutigam and Miettinen the author wants to point out the recital 109 from the GDPR. It states that the possibility to use standard data-protection clauses that are adopted by the Commission or by the supervisory authority should not prevent the controller or processor from including these standard data-protection clauses in a wider contract or from adding other clauses or additional safeguards to them, provided that they do not contradict directly or indirectly the standard contractual clauses adopted by the Commission or by the supervisory authority or prejudice the fundamental rights or freedoms of the data subject. Recital adds that “controllers and processors should be encouraged to provide additional safeguard via contractual commitments that supplements standard protection clauses.” Interpreting the recital 109 the author sees the aim and meaning of GDPR to allow the use of old standard data-protection clauses and complementing them with the requirements of Article 29.<sup>57</sup>

To present one more spring of doubt to the scheme the author turns the focus on case law against Facebook related to data transfer out of EU/EEA. So-called Schrems case was about an individual named Maximillian Schrems lawsuit against relevant data protection Commissioner. High Court of Ireland sent a request for a preliminary ruling for European Court of Justice. Schrems’ argument was based on EU data protection directive that does not allow data transfer outside EU unless adequate protection is guaranteed. At the time Facebook moved personal data based on EU-US Safe Harbour decision. With the ECJ judgement US data protection was deemed invalid and Safe Harbour cancelled. Founding’s of CJEU has been used in the drafting of the GDPR.<sup>58</sup>

Now this case law seems to get a sequel named Schrems II, which is really on this thesis’ interest. On October 2017 the High Court of Ireland has this time granted a request from Irish Data Protection Commissioner for reference to the CJEU for a ruling on validity of the Standard

---

<sup>56</sup> Bräutigam T., Miettinen S., (eds), (2016). The Land of Confusion: International Data Transfers between Schrems and the GDPR, University of Helsinki Faculty of Law

<sup>57</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC

<sup>58</sup> Court Decision, 6.10.2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650

Contractual Clauses for transfer of personal data. Point of this argument is that Standard Contractual Clauses cannot provide adequate level of protection since national laws of the third country will override them. High Court has not yet determined the precise question that it will refer to the CJEU. It is well estimated that this process will take couple of years, and in the meantime, Commission won't give any decisions of its own either. This might not only destroy the Privacy Shield<sup>59</sup> and the Standard Contractual Clauses but if Article 47 is interpreted in a way that invalidates these forms of data transfer it is hard to imagine other solutions that changing the Article 47 or hoping that all other countries magically adapts adequate levels of personal data protection. This stalemate is not welcome to the already confused data protection regime under GDPR.<sup>60</sup>

Marko Popovic has presented the same facts of the so called Schrems II case and similar concerns for the validity of Privacy Shield<sup>61</sup> after the case. He also points out the larger scale of barriers in future data transfer out of EU with standard contractual clauses<sup>62</sup> if Maximilian Schrems wins the case. What is different in his publication is the straight forward statement that the standard contractual clauses will be effective until the judgement.<sup>63</sup>

GDPR has presented a great idea of marking possible standard icons to be used in unconventional consent requests.<sup>64</sup> This kind of actual answer to a problem is what good legislation should make in reality. Instead, GDPR suggests something like that maybe to be done in the future by some authority after the legislation has started to apply. GDPR has been crafted since 2012 so why not to make these symbols in advance and then reference them in the regulation. That would be more of transparent, good way of making legislation and creating predictable legislation. This just goes to show again the failed attempt of this regulation to create anything concrete and unified for the Union.<sup>65</sup> So if the drafters of GDPR have solutions to

---

<sup>59</sup> The International trade administration ITA, Department of Commerce. Privacy Shield Framework. Accessible: <https://www.privacyshield.gov/welcome>. 7.5.2018

<sup>60</sup> Tétrault M., (2017), Here We Go Again: Schrems 2 Puts the Model Clauses for Transfer of EU Personal Data in Doubt Lexology, London UK, last revised 6.5.2018

<sup>61</sup> The International trade administration ITA, Department of Commerce. Privacy Shield Framework. Accessible: <https://www.privacyshield.gov/welcome>. 7.5.2018

<sup>62</sup> European Commission, Data transfer outside the EU, decision 2010/87/EU, Accessible: [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en). 5.5.2018

<sup>63</sup> Popovic M., (2018), Standard contractual clauses challenged by GDPR and scritinized by CJEU, Lexology, London UK, last revised 6.5.2018

<sup>64</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC

<sup>65</sup> Koops B.J. (2014). The trouble with European data protection law, International data privacy law, 4

problems why don't they initiate them instead of making this monster of a law with no answers but over reaching aims of data protection.

An ICC report from a month before releasing the final version of the regulation has listed articles that are expected to have delegated or implemented acts. In GDPR draft there are 5 potentially delegated acts to be, in Articles 8(3), 8(4), 9(3), 26(5), and 42(3). This means that drafters have decided to let go of some of them, but as mentioned couple still remain and in central places. No matter if these acts will remain delegated acts ICC recommends companies to give special attention because they can have important consequences for businesses. ICC has identified that this regulation will cause a major stir in the single market and aims to give extra guidance for the undertakings and expects that with any luck EU officials will offer much more clarification.<sup>66</sup>

### **2.3. GDPR Gives Fragmented Codification and Fails to Be One-Stop-Shop**

As mentioned, GDPR aims to be unifying legislation and is for that reason chosen to be done as a regulation. One of its aims is to be one-stop-shop for the EU digital single market. That is a great idea and that's what makes it so sad that the execution seems so bad. One set of clear data protection rules that are well drafted and balanced for the whole EU would be a dream for the administrative instances of the member states and especially for the undertakings of digital single market.

Article 85 of the GDPR basically just hands the ball back to member states stating that they have to come up with legislation and agreements to protect the freedom of expression and right to receive information while making sure to follow the data protection steps of the regulation. It is painfully amusing to notice that this "unifying" regulation that is too vague has got everyone confused while providing no unity for the single market. For the member states it is a mountain to climb, to draft a set of rules that comply with the directly applicable regulation but still would manage somehow to support the other fundamental freedoms. For companies this is just more administrative costs in the fear of sanctions and no single set of rules for cross-border action.<sup>67</sup>

---

<sup>66</sup> Alhadef J. (2016). Foreword from the Chair of the ICC Commission on the Digital Economy, Paris

<sup>67</sup> Boucher T. (2017). Balancing right under GDPR, Medium, Accessible:  
<https://medium.com/@timboucher/balancing-rights-under-gdpr-458fb025de5b>. 19.2.2018

One set of rules provided by the regulation that would be balanced with freedom of expression and right to information would be the way for GDPR to help also the third country undertakings to comply and get on board with the regulation. As will be mentioned later, U.S. for example has supreme respect for these other freedoms mentioned. If GDPR would provide a clear balanced way to offer data protection while respecting freedom of speech it would be possible to get the other countries on board also. EU has major free trade agreements with other world economies and one clear, balanced, working set of data protection rules might fit in with those trade deals. GDPR on the other hand has made such a bad reputation for itself with its unclear fragmentation that no one wants it. For U.S. it is important to estimate if the data protection law infringes the freedom of speech. Now that GDPR leaves it up to every member state to balance it out with the free speech it is hard for the U.S. to estimate the right balance 28 times.<sup>68</sup>

The author sees Art 85 as one of the fragmenting parts of the regulation where this idea of one-stop-shop is no more than a memory. This article straight forward says that all the individual member states must manage to create their own rules securing the freedom of expression towards data protection while complying with the GDPR. This will mean devastation for the freedom of expression as will be explained more comprehensively in fourth chapter. But besides undermining other fundamental rights, Article 85 will create massive amounts of varying legislation around many different legal areas that have something to do with data protection and free speech and in every 28 member states.

GDPR at the moment gives same set of rules for businesses and state organisations. As sort of one stop-shop for the whole EU another way to approach this would give one set of rules for profit seeking businesses and completely other set of rules for administrative state organisations. U.S.' way of giving industry-based rules could also work better than the GDPR seems to do at the moment.

If GDPR would be done in separate categories like mentioned before it would still be a one-stop-shop as in one stop for all the state organisations, one-stop for all the profit seeking businesses or separately one-stop-shop for all the players in specific industry covering the whole EU single market. The author has seen in first-hand the differences of operating with large corporations and small towns and communal municipals. GDPRs one-stop-shop at the moment is one-stop-landfill

---

<sup>68</sup> Nolan K. (2015) GDPR: Harmonization or Fragmentation? Applicable law problems in EU Data Protection Law, *Berkley Technology Law Journal*, University of California, Berkley

for all to get pissed off and confused. One overreaching regulation in author's opinion is not the best legislative way to secure EU's data protection, but it should be done in a more targeted way. U.S. system of specific data protection tailored for specific sectors could be a better way to go, especially if EU would just take the targeted area but make it stronger and more comprehensive than the United States.<sup>69</sup>

Facebook and Google combined generate half of the world's marketing income. They also are free products and services used all around the world and still among the world's most valuable companies. This combination clearly means that since people don't pay with money they pay with their personal information that is used for advertisements.<sup>70</sup> The most important case laws related to personal data are also against these two media giants as this thesis also presents. These case laws have affected the creation and drafting of GDPR and are actually currently shaping GDPR's future in data transfer.

It is clear that the major will and need for this new European General Data Protection Regulation comes from a need and desire to control these and other media giants. As the author has stated before and will again, there is a clear need for a new regulation and safeguard for some personal data to be protected and one-stop-shop kind of unified for all resolution would be nice. To clarify author's point it should be stated that previous facts considered it is not a functional resolution to make one massive piece of legislation to govern these almost opposite instances.

---

<sup>69</sup> Ingram D., Vengattil M. (2018). UPDATE 3-Facebook's rise in profits, users show resilience after scandals, Reuters, Accessible: <https://www.cnbc.com/2018/04/25/reuters-america-update-3-facebooks-rise-in-profits-users-shows-resilience-after-scandals.html>. 6.5.2018

<sup>70</sup> Ibid

### **3. GDPR UNDERMINES THE FREEDOM OF EXPRESSION AND INFORMATION PROVIDED BY ECHR, UDHR, THE CHARTER AND U.S. FIRST AMENDMENT**

Freedom of expression and the right to information is rooted deep in civilized world. It is protected in United Nations Universal Declaration of Human Rights Article 19<sup>71</sup>, in Charter of Fundamental Rights of the European Union Article 11 and in European Convention on Human Rights Article 10.<sup>72</sup> Since GDPR aims to have broad scope and have its effect also on controllers and processors that are not established in the Union if the data subjects are in the Union this list should also mention United States bill of rights First Amendment.<sup>73</sup>

Throughout the ages the freedom of speech has been protected by the importance of open discussion and discovery of truth. This is how free speech principle has maintained relevance for a long time and widely among different nations. It is feared that if free expression is restricted more than absolutely necessary the society then prevents the ascertainment and publication of accurate facts and valuable opinion. Truth can be considered just as pure fundamental good or as force to strive utilitarian consideration of progress and development of society. If speech is suppressed like GDPR seems to do the alternative speech will be objected and deleted due to its objective false. This will lead to wrongful situation where people holding true beliefs will no more be challenged.<sup>74</sup> Free speech related to religion is usually beliefs and opinions, not verifiable facts, but they are better protected. There are beliefs and opinions in this world that are not religious and also cannot be verified but should not still be discriminated against like GDPR aims to do if it is anyway related to individual data.

---

<sup>71</sup> United Nations General Assembly, Universal Declaration of Human Rights, 10 December 1948 Paris, Art10

<sup>72</sup> European Convention on Human Rights, Article 10, European Court of Human Rights Council of Europe, Strasbourg

<sup>73</sup> Congress of the United States, United States Constitution 1787, Bill of Rights, First Amendment

<sup>74</sup> Barendt E. (2005). Freedom of Speech, Oxford University Press, 526-529

The New York Times reported misuse of individual data at the time of U.S. elections in 2016 by Facebook. Facebook has according to news handed over user data as it does, and this data was used in pursue of effecting the outcome of the elections. Scale of the data is around 50 million users of Facebook and that is the biggest story here. It is not sure if this has had any effects on people's behaviour or the election results at the end, but the free large-scale exploitation is sure. One way of trying to affect the voters was sending fake news to them that was analysed based on their opinions and behaviour. These kinds of news are the reason for EU to renew old data protection directive with GDPR.<sup>75</sup>

While it is necessary to do legislative actions to prevent these kinds of exploiting data insults, the author wants to point out that the purpose does not sanctify the means. With this the author wants to remind that there are other ways than one that GDPR has chosen to reach the desired outcome but without violating other freedoms on the way. This regulations answers to data exploitations is to set the default of personal data in minimum, make deleting of data easy through objection and erasure and see how it goes. When EU has some information on how this is working, some delegated acts will be put in place to repair the gaps. The earlier chapter has already pointed out the legislative issues that rise from delegated acts in such essential places of legislation. This chapter focuses on the other issue of this legislation. As a metaphor some parents decide to hush about the uncomfortable subject matters in their efforts to raise their children like alcohol and sexuality. This is parable for GDPR that hushes about the infringements of other fundamental rights. Other parents decide that open conversation on the topics and access to information is a better way to confront these difficult situations. That is parable to previously mentioned importance of open discussion and discovery of truth, the force to strive utilitarian consideration of progress and development of a society.

### **3.1. Freedom of Expression and the Right to Information: ECHR, UDHR and the Charter**

In her thesis ICL Journal Vol 10 1/2016 Hannah Grafl has written about the Austrian Data Protection Act § 28 para 2 (DSG2000) violating the European Convention on Human Rights

---

<sup>75</sup> Rosenberg M., Frenkel S. (2018). Facebook's Role in Data Misuse Sets Off Storms on Two Continents, The New York Times, Accessible: <https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html>, 21.3.2018

Article 10. Basis for this claim is in Austrian case law where Austrian Constitutional Court in its judgement of 8 October 2015, G264/2015 weighted these two legislations against each other.<sup>76</sup> The applicant has an internet portal where Austrian doctors are listed. Listing contains names, locations, etc. and allows signed members to publish evaluations and reports of their experiences of these individual doctors. Plaintiff in the constitutional proceeding seeks to erase publications on the website according to Austrian Data Protection Act DSG 2000. Procedure has moved from Vienna regional Civil Court to Austrian Constitutional Court. Applicant in the Constitutional Court claimed that the application of Austrian Data Protection Act § 28 para 2 (*BGBL. I Nr. 165/1999*) infringed his right provided in ECHR Article 10.<sup>77</sup>

European Convention on Human Rights Article 10 provides “everyone has the right to freedom of expression. This right shall include freedom to hold and to receive and impart information and ideas without interference by public authority and regardless of frontiers.”<sup>78</sup> Austrian Data Protection Act § 28 para 2 provided Right to Object. “Insofar as a use of data is not authorized by law, every data subject shall have the right to raise an objection with the controller of the data application against the use of data because of an infringement of an overriding interest in secrecy deserving protection arising from his special situation” continued that “data subject can object at any time and without any need to give reason for his desire”<sup>79</sup>

The author sees a close relation with Austrian Data Protection Act § 28 para 2 Right to Object and European General Data Protection Regulation Articles 21 Right to Object and Article 17 Right to Erasure (“Right to be Forgotten”). Wording in these two laws providing right to object is almost identical creating same kind of restrictions towards Art 10 of ECHR. GDPR is very consumer centric and seems to provide individuals with extensive rights to object and erasure on the expense of freedom of expression.

---

<sup>76</sup>Grafl H. (2016). Unconditional Right to Object to the Inclusion of Data in a Publicly Available Data Application Violates Art 10 ECHR, *ICL Journal*, Vol 10, 1/2016, 2-3

<sup>77</sup> Verfassungsgerichtshof Österreich, G 264/2015, 08.10.2015

<sup>78</sup> European Court of Human Rights Council of Europe, European Convention on Human Rights, Article 10, , Strasbourg

<sup>79</sup> Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000)

Accessible: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>  
10.2.2018

Grafl examines the Austrian Constitutional court's decision where the Austrian Data Protection act is deemed by the court to intervene with Art 10 of the ECHR.<sup>80</sup> Author wants to point out the similarity of the Austrian Data Protection act and upcoming European General Data Protection Regulation, to raise a question of legitimacy of EU's new Regulation that is a scary political compromise done on the expense of other fundamental freedoms. This case by the Austrian Constitutional Court is recent, it has gone through multiple high judicial institutions and since it is within a member state of the EU, the legislators of the GDPR should have noticed and learnt from it.<sup>81</sup>

Constitutional court of Vienna could not find a balance between various interests and as a result abolished Austrian Data Protection Act § 28 para 2.<sup>82</sup> GDPR does not give any additional provisions that would give clear answers to issues on this particular case or any future case with similar clash with fundamental rights provided in Art 10 of ECHR.<sup>83</sup>

Drafters of European General Data Protection Regulation have evidently made a decision for the people of EU to value the data protection over the other fundamental rights and principles instead of trying to balance them out. So far GDPR seems to be drafted badly to work as unifying Regulation. It does not follow a good legislative process leaving vital parts to be later filled by the Commission with delegated and implemented acts.<sup>84</sup> It shifts legislative competence extensively to Commission raising eyebrows in political fields. Freedom of expression including freedom to receive information is the historic basis for our developed democratic nations. Internet of Things has certainly shaped ways of information, but it is still has the same vital freedom to preserve if we still want to continue forward as free civilization. With that in mind, the author continues on the subject of freedom of expression.

Freedom of expression is a classic first-generation right and it is closely linked to public access.<sup>85</sup> Public access to documents has its idea on freedom to receive information which has

---

<sup>80</sup> Grafl H. (2016). Unconditional Right to Object to the Inclusion of Data in a Publicly Available Data Application Violates Art 10 ECHR, ICL Journal, Vol 10, 1/2016, 2-3

<sup>81</sup> Ibid

<sup>82</sup> Verfassungsgerichtshof Österreich, G 264/2015, 08.10.2015

<sup>83</sup> Ibid

<sup>84</sup> Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC, Official Journal of the European Union

<sup>85</sup> United Nations General Assembly, United Nations Universal Declaration of Human Rights, Article 19, Accessible: <http://www.un.org/en/universal-declaration-human-rights/>. 8.5.2018

been a necessary tool for the people of free world to seek information.<sup>86</sup> Earlier the thesis talked about the case in Austrian constitutional court, how the Austrian data protection act was found to violate ECHR Art 10 providing freedom of expression<sup>87</sup> and how considering the phrasing of the GDPR it is probable that the Austrian constitutional court or some other court for that matter would not find the balance between the ECHR Art 10 and GDPR either. The case concerned a doctor who wanted his information to be removed from a web portal as his right to privacy had been violated. According to GDPR whether the data in portal was given with consent by the doctor himself or required elsewhere the data subject should have the right to object to it according to Article 21 and right to erasure of the data according to Art 17. GDPR does have some exceptions in Art 17 (3) (a) and (f) concerning freedom of expression and information and reason of public interest. Taking into account the tone and the recitals in this regulation it is clear that these really are rare exceptions and the overriding aim and purpose is to protect the data at all cost.<sup>88</sup>

After GDPR starts to apply in 25<sup>th</sup> of May 2018, less can be expected to be protected by the freedom of speech or the freedom to information by the citizens. In the related Austrian case the privately held website clearly violates GDPR general rights but the information provided by the website should be considered a valid exception by Art 17 (3) (a) and (f) concerning freedom of expression and information and reason of public interest. Some might need the information to be sure they get the best professional to treat themselves or their close ones. Some might need the information to be able to choose a doctor they feel safe to share their medical issues. Doctors are just humans, and they have differences in their ways of practice. If a mother wants to avoid sending her child to perfectly capable doctor in theory but who has had complaints about incorrect use of language, is it good enough reason for public interest. Should the public know about the doctor who treats children and uses inappropriate language, or should the privacy of that doctor go first?<sup>89</sup>

If a banker or a financial broker has not broken laws but has received lots of complaints because customers do feel like they have been ripped off by the hidden expenses that were shown but

---

<sup>86</sup> Docksey C. (2016). Four fundamental rights: finding the balance, *International Data Privacy Law* Vol6 No 3, 2-3

<sup>87</sup> Graf H. (2016). Unconditional Right to Object to the Inclusion of Data in a Publicly Available Data Application Violates Art 10 ECHR, *ICL Journal*, Vol 10, 1/2016, 2-3

<sup>88</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC

<sup>89</sup> Weston M. (2017). *The Right to Be Forgotten: Analyzing Conflicts Between Free Expression and Privacy Rights*, Brigham Young University, 33

time after time customers have been disappointed afterwards, should these complaints along with name, company name address be available for the public or should the individual's data be protected? It seems that makers of GDPR have decided that the data protection is everything and the public does not need this information so badly.<sup>90</sup>

A person who has for example made multiple bankruptcies, had dealings with drugs, been part of extremist organization, promotes racism or treats women unequally, accused of child molestation or has committed frauds in his past, can according to GDPR be forgotten and delete all this information and next year run for public office. A less extreme version of publicly needed information could be the century long advocacy of legality of guns for example on social media and other platforms. Again, this person can according to GDPR demand that all to be erased from the public knowledge and run for public office as gun opposition representative next day. EU legislators have decided that it is more important to protect individual's data than protect the freedom of expression and right to receive information.<sup>91</sup>

If twenty-first century habits related to internet are examined it is not clear for the impartial viewer that the greater part of population values data protection over the freedom of expression and right to receive information. Most user of internet know that Facebook will follow their interest and give that data to other companies for advertising. Other way for Facebook would be starting to take monthly charges for use. It is the authors view that in this scenario majority of users would prefer the free use with the cost of targeted advertisements. Most of this data GDPR is so eager to ban is country location, viewed product information, interests in sports et cetera. Here the access to social media information is chosen over the protection of data that the individual does not really care about.

Websites and applications have long before asked the consent of the users and the routine thing that many does is to click the consent without reading. It is not because they don't understand the text and conditions they are agreeing for, but it is because individuals value the access to information way more that the protection of their personal data concerning gender, location or which food they prefer. GDPR definitely has good aims and some successful parts in it but it is way overshooting in many areas.<sup>92</sup>

---

<sup>90</sup> Ibid

<sup>91</sup> Ibid

<sup>92</sup> Koops B.J. (2014). The trouble with European data protection law, *International data privacy law*, 2

According to studies losing rights to data isn't good enough reason for most users to even bother to glance through the online contracts. Communications professors Jonathan Obart of York University and Anne Oeldorf-Hirsch of the University of Connecticut made an experiment with over 500 students related to consent giving in internet. Test's aim was to see if people read the terms and conditions on web pages. As was predicted, very few did. The supposedly shocking twist in the research was that the part of the terms and conditions that most agreed was to give away their first-born child. For the benefit of this thesis the results and the twist just show what the author has already advocated. People don't read the internet terms and conditions because they usually only contain consent of giving some "personal data" for the use of a company. People don't care if their location, education, name or consumer preferences, that are with GDPR considered as personal data, are given for the company. People only cared about the hoax of giving away their first-born child. We don't need excessive data protection regulations to find that this one term and condition was illegal and won't be respected in the court of law. This test supports what the author advocates that for normal people the protection of this kind of personal data is not important and it should not be protected in expense of freedom of expression and right to information.<sup>93</sup>

One critical way of how GDPR advances imbalance between data protection and freedom of expression and information is through Data Protection Agency DPA. GDPR provides legal mandate for DPAs to "protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data." DPAs are staffed with data protection professionals that probably have now extensive knowledge on rights of expression and information and their jobs are to regulate the processing of personal data. GDPR does not set requirements for DPAs to have extensive legal mandates for balancing free expression and relevant professionals. If DPAs don't have strong legal mandate to balance data protection with expression and don't have professionals for that it is reasonable to expect that the data protection will over rule expression. In top of that the situations in future will probably be more one sided when person demanding privacy rights are in front of DPAs but the person who might want to claim expression or information rights is absent from the hearing. In the opposite position is left the rights of expression and information. GDPR does not point publicly funded, competent free expression

---

<sup>93</sup> David Berredy. (2017). Click to agree with what? No one reads terms of service, studies confirm, The Guardian. Accessible: <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>. 5.5.2018

agency that would have the same kind of mandate to protect the opposite freedoms and rights like the data protection has. There is no balancing European General Data Protection Regulation stating similar detailed enforcement mechanisms. It is false for GDPR to present itself as an unbiased balancing act.<sup>94</sup>

GDPR crafters have been so excited in their mission to be the best at data protection that they forgot the rest of the international values people hold. The crafters probably went out to make rules about how inadequate, irrelevant and excessive information of individuals could be erased accordingly. Judgement of the European Court of Justice in 2014, google Spain v. Mario Costeja Gonzales gave reason for action, but somewhere things got a bit carried away and ended up permitting the deletion of lawfully published truthful information. New GDPR rules set the erasure as default setting obviating data processors and controllers time to consider the legitimacy of the request. With such a short response time given and considering the amount of erasure requests it is certain that this will be used wrongly eliminating data that should remain for public notice.<sup>95</sup>

Aylin Akturk and Jeremy Malcolm have presented an alarming scenario in their publication in the Electronic Frontier Foundation release. This scenario presents horrifyingly absurd violation of freedom of speech and right to receive information created by the GDPR. In this example, someone posts information on Facebook, Twitter, YouTube, Google or some other platform. Other person who for some reason wants it to be taken down requests the intermediary for removal according to Art 17. As pointed out these erasures will be done for wrong reasons and the scale of the coming requests won't give time for the intermediary to consider the legitimacy. GDPR seems to require for intermediary to inform all the downstream publishers and recipients of that content about the objection. Then they have to according Art 14 and 15 disclose for the person who requested the removal of the information where the data originated meaning the information of the uploader, which is noticeably paradoxical. To make this even more surrealistic disbalance of rights, the intermediary does not have to inform the uploader about the removal of his content that he has made in exercise of his right to freedom of expression.<sup>96</sup>

---

<sup>94</sup> Keller D. (2015). Free expression gaps in the General Data Protection Regulation, Internet Policy review, *Journal of internet Regulation*

<sup>95</sup> Akturk A., Malcolm J. (2017). Unintended Consequences, European-Style: How the New EU Data Protection Regulation will be Misused to Censor Speech, Electronic Frontier Foundation

<sup>96</sup> Ibid

GDPR rules of objection and erasure are combined with massive penalties of 4% of annual turnover for the non-compliance.<sup>97</sup> This creates a scenario where intermediaries don't want to take any chances with the requests of the objection or erasure. On the other side of this unfortunate setting is the freedom of speech and right to receive information. These intermediaries do not have the same kind of pressure to protect the uploaded content for the protection of these opposite rights and freedoms. Result of this unbalance is that the intermediaries will want to obey every request of objection and erasure without checking who can claim them and should or could have they protected it. Needless to say, this will perish the freedom of speech and right to receive information and the transparency and reliability that comes with it.<sup>98</sup>

While data protection is an important subject and needs to be taken care of, the drafters of GDPR should have had more interaction with practitioners focused on other parts of internet law than just data protection. This regulation covers a lot of ground<sup>99</sup> varying from data objection, data erasure, data portability, coordination of national Data Protection Agencies, company codes of conduct, appointment of data protection officers, definitions of controller and processor, new definitions of personal data, processing principles, child's consent, transparency rules, automated decision making, data protection by default and design, certifications, binding corporate rules, transfers or disclosures not authorised by Union law, international cooperation, supervisory authorities, dispute resolution, remedies, liabilities and penalties. All these legislative issues in GDPR are approached by ism of data protection with driven mindset of data activists. GDPR is a regulation for a reason that it should unify the single markets data protection. It is however done with such dogmatism that the drafters themselves apparently did not know how it could be balanced with other rights, freedoms and concepts. Article 85 buries its head on the sand and invites member states to come up with rules that follow the severe policies of the regulation and somehow protects the freedom of expression.

For intermediaries that process third party data the upcoming GDPR will be tricky in terms of balancing freedom of speech with the regulation. General legal basis for the intermediaries to

---

<sup>97</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC

<sup>98</sup> Akturk A. Malcolm J. (2015). Unintended Consequences, European-Style: How the New EU Data Protection Regulation will be Misused to Censor Speech, Electronic Frontier Foundation

<sup>99</sup> Keller D. (2015). Intermediary liability and user content under Europe's new data protection law, Internet Policy review, *Journal of internet Regulation*

process data is that the processing serves legitimate purposes. Again, GDPR does not give clarity and legitimate reasons are undefined but surely, they must contain expression and information rights. Costeja ruling was criticised from lack of clarity on how to assess these colliding interests. A clear unified line of whose interests will be protected in these cases where intermediaries process third party data won't be received from GDPR. Keller rightly argues that it made more sense for data protection rules from the past to lack some detailed provisions concerning freedom of expression since the regulated entities in that era where institutions like banks, big employers, medical offices and like. Today's world with internet of things and intermediaries controlling and processing third party individuals' data content the lack of detailed provisions will probably form extensive problems.<sup>100</sup>

GDPR recitals restate the aim presented by its drafters that this legislation is a regulation so that it will obtain Union wide resemblance in this legislative matter. GDPR recitals promote the balancing of rights and harmonizing of legislation between member states and manages to do neither. It gives strong boundaries for the compliance of data protection and vague contours for the expression. Current data protection legislation directive 95/46/EC also leaves it for the member states to figure out the protection of expression and information. As seen in the past some member states have done basically nothing and others made some poor effort for the protection of those fundamental freedoms while trying to comply with the data protection and the situation is only getting worse with the stricter GDPR.<sup>101</sup>

Since GDPR is expanded to apply to all sorts of online speeches that individuals do by posting information, opinions, ideas, photos et cetera, it should be more detailed in including these forms of speech in balanced protection of data, information and expression. Instead of being more detailed compared to old the Directive it only sets more requirements for data protection but does not mention how to protect the expression. Legal protection of individuals' internet speeches should not be precluded in pursue of restraining the media giants.<sup>102</sup>

GDPR shoves the responsibility of protecting the freedom of expression and information for the member states and intermediaries processing data posted by individuals must act accordingly

---

<sup>100</sup> Keller D. (2015). Intermediary liability and user content under Europe's new data protection law, Core Questions About the GDPR and Intermediary Liability, The Centre for Internet and Society CIS, Stanford Law School

<sup>101</sup> <sup>101</sup> Keller D. (2015). Free expression gaps in the General Data Protection Regulation, Internet Policy review, *Journal of internet Regulation*

<sup>102</sup> Ibid

when asked for right to be forgotten. GDPR does give some obscure guidelines when this kind of requests can be rejected but for the intermediaries it will always just be easier to erase all requests. The fact that GDPR leaves this for the member state laws to figure out means that all the possibilities to reject erasure will vary from country to another and intermediary would need to use lawyer in every single case to estimate how they should act. This administrative burden and fear of sanctions will just lead to wide scale censure.<sup>103</sup> European Commissions has its own evaluation from 2012 analysing the implementation of the data protection Directive in member states. This evaluation already shows that aims of the Directive are implemented very differently in member states. GDPR does not provide unity as it is supposed to for the balancing acts of these freedoms.<sup>104</sup>

ICC has stated its position for the upcoming regulation about the establishment of data controller and notice of third parties legitimate interest as legal basis for processing data. In this regard ICC notices that the regulation should not set this kind of unbalance by putting the freedoms of data subject in front of freedoms of the controller or the third party. Analytic data processing according to ICC is a vital part of advancement of medicine, social welfare, education, commerce and civil society. Data usually gathered for these uses are not directly from the consent giver but from multiple sources. GDPR is extremely consent oriented and this might make it even impossible to obtain this vital information for the society. GDPR according to ICC does not give controllers real ability to determine the legitimacy of their interest. It is also important to safeguard that freedom of expression is not made inferior by the bureaucratic burdens if not absolutely necessary.<sup>105</sup>

Like mentioned in relation to Facebook, Cambridge Analytica and affecting to the world-wide politics, this approach that GDPR is taking is not the best way to go forward according to the author. The habit of limiting freedom of speech because of information privacy is not a new one but GDPR just takes it up to extreme. These information privacy rules are aimed to give control of personal data back to ourselves and it does sound good at first place, however as this paper has already stated the first expression of these rules can deceive.<sup>106</sup>

---

<sup>103</sup> Ibid

<sup>104</sup> Erdos D. (2014). Fundamentally of Balance: European Union Data Protection Law and Media Expression, NO. 42/2014, University of Cambridge, p. 2

<sup>105</sup> ICC commission on the Digital Economy, (2015) ICC Position on Legitimate Interest

<sup>106</sup> Volokh E. (2000). Freedom of Speech and Information Privacy: The Troubling Implication of a Right to Stop People from Speaking About You, Stanford Law Review, Vol 52, No. 5, 1049

The author sees limiting freedom of speech because of information privacy as a step back for humanity. Like stated in this Facebook, Cambridge Analytica case the new increased use of personal data does create issues for the democracy and rights of individuals. Strict information privacy rules that tries to cure these Legislative issues by hiding data and limiting its collection is not far reaching solution, it is like putting a bandage on an open wound that needs stitching and time to recover. Limiting and hiding personal information as default and design can lead to catastrophic outcomes for the democracy and free society.

One does not have to look far back in history to notice that ordinary people can make better decisions based on conclusions they can make themselves based on free information, compared to a situation where society is limiting the information strongly. While free information has been compounded with advanced education in a society the end result has always been supreme. Our new era of information technology has certainly presented us with an obstacle where individuals have to learn to navigate, this time through extensive information amounts and may struggle with it. But as this paper has argued the solution of hiding and limiting data like GDPR does is not the only way and the author wants to present an optional solution also. Sometimes it is good for society to look back when thinking ahead and not try to figure out the wheel again sort of said. Yes, we have a problem with excess amount of information and usage of personal data, but the solution is not to bury our heads in the sand and start protecting every piece of personal information like government secrets but to look back and learn. Free information is good for the society, has always been and continues to do so. Educating the population and giving them resources to make enlightened conclusions and decisions is still the way ahead. Financial cost, trouble and time used to this legislation could be targeted other ways.

### **3.2. Case Law: C-131/12 Google Spain v Mario Costeja González**

In 2010, Spanish national named Costeja Gonzalez brought a complaint before his country's data protection agency. Complaint was against newspaper La Vanguardia and Google Spain and Google Incorporated. He wanted a newspaper to remove or modify information related to his 1998 record so that the information would be removed from a webpage and would no longer

appear in a search engine.<sup>107</sup> Data Protection Agency dismissed the complaint against the newspaper but upheld it against Google and importantly found that internet search engines are also subjected to data protection laws and must protect personal information.<sup>108</sup>

National High Court of Spain processed the appeal and presented questions to the European Court of Justice (CJEU). Here the Important finding of the ICJ was to apply the EU Directive 95/46 and founded that internet search engines must be regarded as controller with respect to processing of personal data with acts of indexing, locating, storing and disseminating information. Here the ruling set spark to the upcoming GDPR stating that for guarantee of personal data protection search engines can be ordered to remove personal information published by third party websites.<sup>109</sup> In authors opinion, balance with the free expression and right to information started to fade away since that moment.

This decision of European Court of Justice was revolutionary in the field of data protection versus free expression and it has become famous or infamous depending on the view even in mainstream media and as far as its legal significance goes it is definitely considered as a landmark case<sup>110</sup> that gave GDPR its final confirmation. This decision has been cited already in over 30 cases and more will come, but there are lots of opposite concerns also arguing that it has not found balance between data protection and free expression.<sup>111</sup> As has been seen earlier in this thesis, it is the opinion of the author that European Court of Justice with this decision has not struck balance between these competing freedoms and the balance will twist even more now that the GDPR uses its opportunity to relay on it.

In Costeja ruling CJEU did not identify the publisher's expression rights as balancing factor in relation to what should and should not be removed. GDPR does not clarify this or correct this

---

<sup>107</sup> Court Decision, 13.5.2014 Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. C-131/12.

<sup>108</sup> Global Freedom of Expression, Columbia University, case law, Google Spain SL v. Agencia Espanola de Protection de Datos, New York, accessible: <https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/>, 21.03.2018

<sup>109</sup> Ibid

<sup>110</sup> Court Decision, 13.5.2014 Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. C-131/12.

<sup>111</sup> Global Freedom of Expression, Columbia University, case law, Google Spain SL v. Agencia Espanola de Protection de Datos, New York, accessible: <https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/>, 21.03.201

and the data protection seems to be over ruling and the exceptions are concerning the legitimate aim of the controller and possibly third parties but not so much the publishing individual.<sup>112</sup>

Costeja case created questionable movement with the world's biggest search engine Google. Google created an online form so that European citizens can request removals of webpages that contain personal data related to them. If Google denies a request, a person can make an appeal through the data protection agency DPA that has jurisdiction to enforce it. However, there is no appeal process provided by Google or by any appointed free speech agency for the person harmed by the granted request to protect their free speech or right to information. GDPR crafters have made the playfield one sided and there is nothing for individuals to do but to wonder and adapt.<sup>113</sup>

### **3.3. First Amendment of the United States Constitution**

Robert A. Sedler has written in his Essay on Freedom of Speech: The United States versus the Rest of the World about his presentations on constitutional protection of freedom of speech. The significant factor in his presentations relates to different reception between U.S. audience and other audiences. For those different audiences he has compared the strong constitutional protection of freedom of speech in U.S. and the lesser protection in EU and other countries. Sedler has pointed out the extreme where U.S. goes in free speech protection even allowing hate speech to far greater extent than other countries.<sup>114</sup> The author identifies with that approach and point out its own observation of golden middle ground between U.S. system and GDPR.

In these presentations Sedler asked philosophical questions from the different crowds and noted that consensus was formed. This consensus among very different crowds was that the strong constitutional protection of freedom of speech in U.S. was indeed manifestation of an American humanistic value. That value is based on the history, experiences and culture of the American

---

112 Global Freedom of Expression, Columbia University, case law, Google Spain Sl v. Agencia Espanola de Protection de Datos, New York, accessible: <https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/>, 21.03.2018

113 Weston M. (2017). The Right to Be Forgotten: Analyzing Conflicts Between Free Expression and Privacy Rights, Brigham Yang University, 27

114 Sedler, R. (2006). An Essay on Freedom of Speech: The United States versus the Rest of the World, Michigan State Law Review, 377-378

people.<sup>115</sup> The author expresses its opinion that EU will have hard time forcing the GDPR for U.S. processors and controllers due to its lack of protection of expression.

United States Court of Appeals, Second Circuit, Docket No. 13-3315 January 28, 2015, “Lorraine Martin” case is a good example of U.S.’ strong advocacy of the freedom of speech protected by the first amendment of the United States Constitution. Lorraine Martin was arrested in 2010 with drug charges. Various newspapers published the arrest in their internet news forums stipulating suspected drug ring. Connecticut State did not pursue charges and case was dismissed and for that reason she claimed that the story was false and defamatory. Martin asked for erasure of the internet publications on the basis of local erasure status. When the newspapers refused she filed actions on libel and privacy invasion. District court ruled in favour of press freedom whether the charges were dropped or not and the court of appeal stick by that decision. This is just one of many cases showing that U.S. prizes the free expression and right to information over the privacy.<sup>116</sup>

GDPR is drafted in a way that seeks to have as far reaching scope as it can. It is drafted to have an effect on the third country undertakings that have any connection to EU or its citizens. If third country undertaking advertises, offers any goods or services or monitors data subject behaviour inside the EU or for the EU citizens the GDPR comes into effect for them.<sup>117</sup> If GDPR doesn’t have enough problems in EU dealing with the issue of it ramming down on free speech the U.S will be even harder. Free speech is protected in United States Constitution’s First Amendment with freedom of religion and in U.S people value their free speech ”religiously”.

This wide scope of the GDPR reaching its fingers to hopefully cover the whole planet with data protection of its citizens is going to step on the toes of sovereignty of third countries. GDPR wants EU citizens to be able to object, have right to erasure and data portability worldwide, meaning to delete data from global public and have one-sided censorship. The founder of Wikipedia obviously has his own narrative on the subject calling the GDPR insane, but it does

---

<sup>115</sup> Sedler, R. (2006). An Essay on Freedom of Speech: The United States versus the Rest of the World, Michigan State Law Review, 377-379

<sup>116</sup> Weston M. (2017). The Right to Be Forgotten: Analyzing Conflicts Between Free Expression and Privacy Rights, Brigham Yang University, 7-8

<sup>117</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC, Article 3

not mean it has truth in it. He pointed out that there should be no defence for the existence of right to censor what people say in internet or to prevent the publication of truthful information.<sup>118</sup>

In her thesis Mindy Weston states that European citizens support the hard core data rights of GDPR like right to be forgotten. She also states that Europeans favour privacy over free speech unlike Americans.<sup>119</sup> It is the opinion of the author that this is not correct. GDPR is done pretty far away from the people of EU. One could say that the Britain's exit from EU (Brexit) for example is the will of the Britain's people since just over 50% majority voted for it. GDPR however is not a result of referendum of EU citizens, far from it.

No matter if GDPR is the will of the European people or not, the violations for free speech and information won't be easily tolerated in U.S, not by its people and not by its courts. U.S also recognizes privacy rights when the speech contains obscenity, defamation, hatred or violence, racism et cetera.<sup>120</sup> The author of this thesis is all for those data privacy rights and so is many other people, but GDPR goes way beyond those and that is where it will find resistance from the U.S. courts.<sup>121</sup> Costeja case would probably not had ended in same way if it would have been ruled by the United States Court, and that's something to think about for the drafters of GDPR.

U.S. caselaw shows that it's courts have recognised privacy rights in many different cases. However, they all have one thing in common, privacy rights tend to be recognised when they support other fundamental rights like freedom of speech, freedom to personal liberty and minority rights, not the other way around like GDPR.<sup>122</sup>

Long shot of hope would be integration of GDPR rules to U.S. through possibly fourth coming trade deal. If Privacy Shield<sup>123</sup> holds, its synthesis with EU's trade deal would be truly a step

---

<sup>118</sup> Weston M. (2017). The Right to Be Forgotten: Analyzing Conflicts Between Free Expression and Privacy Rights, Brigham Yang University, 23

<sup>119</sup> Weston M. (2017). The Right to Be Forgotten: Analyzing Conflicts Between Free Expression and Privacy Rights, Brigham Yang University, 23-24

<sup>120</sup> JUSTIA, (2018) Constitutional law, Privacy Rights and Personal Autonomy. Accessible: <https://www.justia.com/constitutional-law/docs/privacy-rights/>. 8.5.2018

<sup>121</sup> Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC, Official Journal of the European Union

<sup>122</sup> Cornell Law School, Legal Information Institute, Privacy. Accessible: <https://www.law.cornell.edu/wex/privacy>. 8.5.2018

<sup>123</sup> The International trade administration ITA, Department of Commerce. Privacy Shield Framework. Accessible: <https://www.privacyshield.gov/welcome>. 7.5.2018

forward. That deal will be complex and full of compromises either way, so why won't throw one GDPR in the mix. U.S. would be a great partner to participate in GDPR but it might be a long shot. However, other large markets like Canada or India might be in EU's radar if U.S. constitution's First Amendment won't bow.

## CONCLUSION

The author uses this thesis to go deeper in the fundamentals of the European General Data Protection Regulation (GDPR), to see and analyze how it fits into our society, economical aim, fundamental rights and values. In this pursuit the author has identified three legislative issues in the regulation: GDPR does not support the legal aim of a single market and protects data unnecessarily against the principle of proportionality. Legislative drafting of the GDPR is poorly made and it makes it uncertain and fragmented. GDPR undermines the freedom of expression and information, provided by ECHR, UDHR, THE CHARTER and U.S. First Amendment. Relevant legislations and their relations towards these identified legislative issues are in the centre of this paper. Landmark cases of data protection are analysed for the support of creation of comprehensive portrait of the GDPR's success and fails. The author distances this thesis from the ones that explain what the regulation means for different instances and how they should prepare for it and concentrates on fundamentals that will have far reaching effects.

EU did not want to regulate privacy over freedom of speech in analogue times before internet. Internet has been and still is a vital stepping stone for benefit of the human kind providing it with unseen possibilities to share and to receive information freely all over the world. The author presents share economies as a good example of how twenty-first century economy is free and data driven. Uber cars are popular around the globe where average people share their information and invite people to ride in their cars. Airbnb is superseding conventional hotels world-wide. Its users share their names, locations, interests, household pictures and then invites strangers to live in their apartments. The author wants to point out that these shared economies are replacing the old conventional businesses and interests and what is central in them is that people willingly share their information, lifestyle and property with the world-wide economical network. Tremendous popularity of these social share economies begs the question whether GDPR supports the fundamental aim of the single market and does it regulate inside the boundaries of

principle of proportionality. It is concluded that CJEU and Commission should note this in their future decisions.

Aims behind the European General Data Protection regulation GDPR are valid and a successfully drafted data protection law would be a great mile stone and advantage for all but in author's opinion GDPR is nothing like that. Delegated acts are designed to amend or supplement non-essential elements in EU legislative acts. The author is raising questions about the throwbacks of delegative acts granted for Commission in central legal issues of the GDPR.

One of the GDPRs legislative issues is widely asked question, does old controller-processor standard contractual clauses apply when GDPR starts to apply in 25<sup>th</sup> of May 2018. Many variable opinions to that question are introduced, demonstrating the uncertainty in this essential part of the legislation. Other kind of legally binding and enforceable instrument can be created between governments for data transfer. An example of that is EU-US Privacy Shield but at this point of time when the so called Schrems II case is waiting to happen, a long-lasting solution to rely on Privacy Shield is fragile. The author points out the unsettling fact that governments of different member states are giving different guidelines for the usage of standard contractual clauses. As an example, data protection agencies of member states like UK, Estonia, Netherlands and Sweden are recommending that companies continue using old standard contractual clauses hinting that they are not going to rush evaluate complaints before clear replacements are given. In contrast, France for example is already investigating complaints related to these.

In author's opinion the major will and need for GDPR comes from the need and desire to control media giants. The author has stated that one-stop-shop kind of unified for all resolution would be nice, but GDPR fails delivering it. The author points out that it is not a functional resolution to make one massive piece of legislation to govern all opposite instances like profit-seeking corporations and small-town administrations.

Freedom of expression and the right to information is rooted deep in civilized world. It is protected in United Nations Universal Declaration of Human Rights, in Charter of Fundamental Rights of the European Union, European Convention on Human Rights and United States bill of rights First Amendment. Throughout the ages the freedom of speech has been protected by the importance of open discussion and discovery of truth. The author thinks that after GDPR starts to apply in 25<sup>th</sup> of May 2018, less can be expected to be protected by the freedom of speech or the

freedom to information. GDPR crafters have been so excited in their mission to be the best at data protection that they forgot the rest of the international values people hold.

GDPR has enough problems in the EU but it will have a mountain to climb with U.S. if it continues ramming down on free speech. Free speech is protected in United States Constitution's First Amendment with freedom of religion and in U.S people value their free speech "religiously". GDPR's violations for free speech and information won't be easily tolerated in the U.S, not by its people and not by its courts.

The author has concluded that this regulation will kill innovation and entrepreneurship and move business away from EU. The author suggests that the regulation should better identify the ways for data controllers to process individual's data lawfully by establishing legitimate interest. The author sees that GDPR should be amended with sight that it is more important in default for the masses to have this information available than for an individual to hide it. The author concludes that giving comprehensive data protection for individuals does not mean hundred percent coverage and GDPR should not go beyond what is in accordance with the principle of proportionality. The author has demonstrated in relation to Facebook data breach that people don't care about protecting virtually all of their personal data and so GDPR should not aim to protect it data if it is violating the proportionality principle.

Prosperous data driven economy is built on education, personal skills and experience. In author's opinion it is important to educate people and give them an access to free information and give necessary tools to evaluate the information that they receive. By this way people can make educated decisions and society doesn't have to take a step back by starting to hide data.

The author has pointed out multiple issues rising from the power of delegated acts given for the Commission in relevant places of the regulation. Commission needs to give these delegated acts soon to give clarity for the member states. Additional guidelines and approved codes of conduct and certifications need to be presented fast for GDPR to redeem itself.

To sort out the vast issue of data transfer for the sake of the single market CJEU needs to find a right, balanced answer to Schrems II case and do it with a speeded process. Author has demonstrated that EU model contracts like Privacy Shield and standard contractual clauses are way too important for the single market to be in this kind of crippled state.

GDPR aims to be unifying legislation, so called one-stop-shop for the single market and for that reason is chosen to be done as a regulation. The author has pointed out issues related to that and suggested a compromise where EU would have same sets of rules in every member states but different sets for different entities like undertakings and state administration. This kind of approach is familiar from U.S. legislation, it just needed to be more demanding.

The author has identified the problems that GDPR will have with U.S, its companies and its courts. The author has presented a solution to finding a middle ground between harsh interpretation of GDPR and a strong constitutional protection of freedom of speech in the U.S. The author has suggested to find that middle ground and that way trying to attach it to EU's trade deals. This way values important for the GDPR would be easier to internalize and they would be easier to spread.

## LIST OF REFERENCES

### Scientific Books

- Alhadeff J. (2016). Foreword from the Chair of the ICC Commission on the Digital Economy, Paris
- Barendt E. (2005). Freedom of Speech, Oxford University Press, 526-529
- Craig P., De Burca G. (2011). EU Law Text, Cases and Materials. 5<sup>th</sup> ed. New York: Oxford university press, 133-138
- Hornung G. A. (2012). General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft, 9 SCRIPT ed. 64
- Koops B.J. (2014). The trouble with European data protection law, International data privacy law, 2
- Makiyama H. L. (2012). Digital Trade in the U.S. and Global Economies', ECIPE
- Sotto L. J., Hydak C. D. (2016). EU-US Privacy Shield: A Path Forward, Risks Benefits and the Future of the Agreement, Hunton & Williams, Corporate Compliance Insight, 6
- Tétrault M. (2017). Here We Go Again: Schrems 2 Puts the Model Clauses for Transfer of EU Personal Data in Doubt Lexology, London UK, Accessible: <https://www.lexology.com/library/detail.aspx?g=2b8e2ad4-1964-431f-9c3d-845a8278a96d>. 6.5.2018
- Wallsten S. (2015). The Competitive Effects of the Sharing Economy: How is Uber Changing Taxis? Technology Policy Institute, Washington, DC

## Scientific Articles

- Akturk A., Malcolm J. (2015). Unintended Consequences, European-Style: How the New EU Data Protection Regulation will be Misused to Censor Speech, Electronic Frontier Foundation
- Bartl M., Irion K. (2017). The Japan EU Economic Partnership Agreement-. Flows of Personal Data to the Land of the Rising Sun, University of Amsterdam, CSECL, 1
- Bertermann N. ed (2016). EU General Data Protection Regulation, A First Introduction describing the major changes compared to today's German law, Practice Group IT & Digital Business
- Bräutigam T., Miettinen S. ed. (2016). The Land of Confusion: International Data Transfers between Schrems and the GDPR, University of Helsinki Faculty of Law
- Cornell Law School, Legal Information Institute, Privacy. Accessible: <https://www.law.cornell.edu/wex/privacy>. 8.5.2018
- Chirica S. (2017). The Main Novelties and Implications of the New General Data Protection Regulation, Perspectives - *Business Law Journals*, Vol 6, Issue 1
- Docksey C. (2016). Four fundamental rights: finding the balance, *International Data Privacy Law* Vol6 No 3, 2-3
- Erdos D. (2014). Fundamentally of Balance: European Union Data Protection Law and Media Expression, NO. 42/2014, University of Cambridge, 2
- Grafl H. (2016). Unconditional Right to Object to the Inclusion of Data in a Publicly Available Data Application Violates Art 10 ECHR- *ICL Journal*, Vol 10, 1/2016, 2-3
- Keller D. (2015). Intermediary liability and user content under Europe's new data protection law, Core Questions About the GDPR and Intermediary Liability, The Centre for Internet and Society CIS, Stanford Law School
- Kuner C. (2012). The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, *Bloomberg BNA Privacy and Security Law Report*, 23
- Sedler, R. (2006). An Essay on Freedom of Speech: The United States versus the Rest of the World, *Michigan State Law Review*, 377-378
- ICC commission on the Digital Economy, (2015). ICC Position on Legitimate Interest
- Keller D. (2015). Free expression gaps in the General Data Protection Regulation, *Internet Policy review- Journal of internet Regulation*
- Nolan K. (2015). GDPR: Harmonization or Fragmentation? Applicable law problems in EU Data Protection Law- *Berkley Technology Law Journal*, University of California, Berkley

- Volokh E. (2000). Freedom of Speech and Information Privacy: The Troubling Implication of a Right to Stop People from Speaking About You, *Stanford Law Review*, Vol 52, No. 5, 1049
- Voss G., W. (2012). Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments, *Business Law Today*, Accessible: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/busiltom2012&div=96&id=&page=>. 10.5.2018
- Weiss M. A., Archick K. (2016). U.S.-EU Data Privacy: From Safe Harbour to Privacy Shield, Congressional Research Service, 15
- Weston M. (2017). The Right to Be Forgotten: Analysing Conflicts Between Free Expression and Privacy Rights, *Brigham Yang University*, 27-33
- Yokovleva S., (2017). Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"? Cambridge University Press
- Zervas G. Proserpio D., Byers J.W. (2017). The Rise of the Sharing Economy: Estimating the Impact of Airbnb on the Hotel Industry- *Journal of marketing research*, Vol54, No. 5, 687-705

## **EU and International Legislation**

- Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSGVO 2000) Accessible: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>. 15.4.2018
- Consolidated Version of the Treaty on the Functioning of the European Union, Art 16(1), Art 290
- EU Commission, The European Single Market, Accessible: [https://ec.europa.eu/growth/single-market\\_en](https://ec.europa.eu/growth/single-market_en). 7.5.2018
- EUR-LEX, Access to European Union Law, proportionality principle, Accessible: <https://eur-lex.europa.eu/summary/glossary/proportionality.html>. 7.5.2017
- European Court of Human Rights Council of Europe, European Convention on Human Rights, Article 10, Strasbourg
- European Commission, Data transfer outside the EU, decision 2010/87/EU, Accessible: [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en). 5.5.2018
- Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC, Official Journal of the European Union

The International trade administration ITA, Department of Commerce. Privacy Shield Framework. Accessible: <https://www.privacyshield.gov/welcome>. 7.5.2018

United Nations General Assembly, Universal Declaration of Human Rights, 10 December 1948 Paris, Art10, 19

United States Constitution. First amendment. FREEDOM OF RELIGION, SPEECH, PRESS, ASSEMBLY, AND PETITION. Passed by Congress September 25, 1789, Ratified December 15, 1791. The First 10 Amendments from the Bill of Rights. Accessible: <https://constitutioncenter.org/interactive-constitution/amendments/amendment-i>. 7.5.2018

### **Other Court Decisions**

Court Decision, 6.10.2015, Maximilian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650

Court Decision, 13.5.2014 Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. C-131/12.

Verfassungsgerichtshof Österreich, G 264/2015, 08.10.2015

### **Other Sources**

Boucher T. (2017) Balancing right under GDPR, Medium, Accessible: <https://medium.com/@timboucher/balancing-rights-under-gdpr-458fb025de5b>. 03.03.2018

Clark R. (2017). What Europeans Really Think of the EU, The Spectator, Accessible: <https://www.spectator.co.uk/2017/07/what-europeans-really-think-of-the-eu/>. 7.5.2018

David Berredy. (2017). Click to agree with what? No one reads terms of service, studies confirm, The Guardian. Accessible: <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>. 5.5.2018

Eurostat Statistic Explained, (2018). International Trade in Goods, accessible: [http://ec.europa.eu/eurostat/statisticsexplained/index.php/International\\_trade\\_in\\_goods/fi](http://ec.europa.eu/eurostat/statisticsexplained/index.php/International_trade_in_goods/fi). 1.5.2018

GDPR requirements, deadlines and facts, February 16 2018, CSO, Accessible: <https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html>. February 18 2018

- Global Freedom of Expression, Columbia University, case law, Google Spain Sl v. Agencia Espanola de Protection de Datos, New York, accessible: <https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/>. 21.03.2018
- Ingram D., Vengattil M. (2018). UPDATE 3-Facebook's rise in profits, users show's resilience after scandal, CNBC, Reuters, accessible: <https://www.cnbc.com/2018/04/25/reuters-america-update-3-facebooks-rise-in-profits-users-shows-resilience-after-scandals.html>. 5.5.2018
- Internet World Stats, (2017). World Internet Users and 2018 Population Stats, Accessible: <https://www.internetworldstats.com/stats.htm>. 7.5.2018
- JUSTIA, (2018) Constitutional law, Privacy Rights and Personal Autonomy. Accessible: <https://www.justia.com/constitutional-law/docs/privacy-rights/>. 8.5.2018
- Macrae A. (2016). GDPR-the good, the bad and the ugly, tripwire, Accessible: <https://www.tripwire.com/state-of-security/security-awareness/gdpr-the-good-the-bad-and-the-ugly/>. 28.2.2018
- Myers A. (2016). Top 10 operational impacts of the GDPR: Part 4- Cross-border data transfer, The International Association of Privacy Professionals (IAPP), Accessible: <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/>. 5.5.2018
- Nasdaq, Facebook Inc Class A Common Stock 3month. Accessibl: <https://www.nasdaq.com/symbol/fb>. 10.5.2018
- Rosenberg M., Frenkel S. (2018). Facebook's Role in Data Misuse Sets Off Storms on Two Continents, The New York Times, Accessible: <https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html>. 21.3.2018
- Statista. Number of monthly active Facebook users worldwide as of 4<sup>th</sup> quarter 2017 (in millions) (2018) Accessible: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>. 7.5.2018
- The Eu General Data Protection Regulation (GDPR), it governance, Accessible: <https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation> , 19 March, 2018 Nadeau M., General Data Protection Regulation
- Zetony D. (2018). GDPR: The Most Frequently Asked Questions: Are the Standard Contractual Clauses Enough? accessible: <https://www.bryancave.com/en/thought-leadership/gdpr-the-most-frequently-asked-questions-are-the-standard.html>. 5.5.2018