UNIVERZITA KARLOVA

Právnická fakulta

Simona Semanová

Úloha práva na přístup k osobním údajům v rámci práva na ochranu osobních údajů

Diplomová práce

Vedoucí diplomové práce: JUDr. Jan Exner

Katedra evropského práva

Datum vypracovaní práce (uzavření rukopisu): 05.02.2021

CHARLES UNIVERSITY

Faculty of Law

Simona Semanová

The role of the right of access to personal data within data protection law

Master's thesis

Master's thesis supervisor: JUDr. Jan Exner

Department of European Union law

Date of manuscript closure: 05.02.2021

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 187 147 znaků včetně mezer.

I hereby declare that I have written this master's thesis on my own and all the sources used have been duly cited and this master's thesis has not been used to obtain any other or the same academic degree.

I further declare that the actual text of this master's thesis, including footnotes and spaces, has 187 147 characters.

Simona Semanová

Table of contents / Obsah

INTRODUCTION

"Nowadays an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers - unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others."[1]

The concept of personal data protection has been at the centre of attention in the European Union for the past few years. It is mainly due to the adoption of the General Data Protection Regulation (hereinafter the "GDPR") by the European Parliament and the Council in 2016. However, data protection law had originated much earlier. The right to personal data protection has evolved from the right to privacy which is according to several human rights acts[2] considered to be an international human right. Later, the right to personal data protection has acquired the level of a fundamental human right itself, as it is acknowledged in Article 8 of the Charter of Fundamental Rights of the European Union. Accordingly, the right to personal data protection has been enacted in the primary[3] as well as in the secondary[4] law of the European Union, both of which are discussed in this master's thesis.

In today's society, full of technological transformations and digitalisation, it is necessary to effectively guarantee the personal data protection of individuals. The existence of the internet, massive surveillance, and a global flow of personal data represent extraordinary challenges for privacy and human dignity. Therefore, it is indispensable to protect the personal information, minimize the risks of misuse and guarantee appropriate rights for individuals.[5] The problem of personal data protection seems to be that individuals are often not aware that their personal data are being processed, who is processing them, or what are the basic aspects and consequences of such processing. Such knowledge is necessary to

[1] Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. *U.S. Department of Health, Education and Welfare* (1973). Page 29

[2] Universal Declaration of Human Rights (1948), European Convention on Human Rights (1950), Charter of Fundamental Rights of the European Union (2000)

[3] Charter of Fundamental Rights of the European Union (2000), Treaty on the Functioning of the European Union (1957)

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[5] Opinion by Artemi Rallo: Privacy and Freedom. *European Data Protection Law Review*. 2018, *4*(2), 150-151.

determine whether the personal data processing is carried out in compliance with data protection law.

The adoption of the GDPR has brought several modernized measures to enhance the personal data protection of individuals. This master's thesis focuses on the rights that the GDPR grants individuals in order to strengthen their position of data subjects and have better control over their personal data than before. These rights are in the field of data protection law known as "data subject rights". One of the most important data subject rights is the right of access to personal data constituted in Article 15 of the GDPR. This right, together with the right to be informed under Articles 13 and 14 of the GDPR, is supposed to ensure that data subjects possess all necessary information on their personal data processing. Based on the mentioned rights, controllers are obliged to provide such information to data subjects.

The aim of this master's thesis is to examine the extent to which the right of access to personal data determines the effectiveness of personal data protection. In other words, how important is the role of the right of access in the standard protection provided by the GDPR and how it arranges data subjects' necessity to be informed of the essential aspects of their personal data processing.

In order to answer these questions, it is at first necessary to define the right to data protection, assess its link to the right to privacy and its development into the standard it represents at present by studying the legal framework thereof (Chapter 1). This is followed by discussing the general aspects of data subject rights, including the determination of principles that need to be adhered to when facilitating data subject rights and that are bound to the whole procedure of personal data processing (Chapter 2). Subsequently, the right to be informed, strongly correlated with the right of access to personal data, is analysed (Chapter 3). Finally, the right of access is scrutinized, namely its development within the legal framework over the years, including the relevant case law of the Court of Justice of the European Union, by examining the key aspects of this right and its exercise in practice (Chapter 4).

The reason why I chose this topic for my master's thesis is that I have found myself interested in data protection law, especially in data subject rights a couple of months ago, during my studies at the University of Copenhagen last academic year. I took there a course on European Data Protection Law, which was the first time I have encountered this important field of law. After completing this course and the semester in Copenhagen, my interest in data

protection law grew stronger. I have been taking my internship at the Consultation Department of The Office For Personal Data Protection of the Czech Republic[6] for a few months now. The knowledge learnt from the course on European Data Protection Law in Copenhagen and the experience gained so far during the internship at The Office For Personal Data Protection have given me many ideas which are used in this master's thesis, including some of the real cases that the Consultation Department of The Office For Personal Data Protection has dealt with. I believe that these remarks will add remarkable value to this thesis and contribute to achieving its aim.

The topic of data subject rights has been tackled by several authors[7] whose literary works have given me the inspiration to work on the topic of this master's thesis. However, the right of access to personal data solely or in connection with the right to be informed has not been subjected to many literary works as far as I am aware of. In addition, I assume that in order to precisely understand the importance of the right of access to personal data, it is not enough to only analyse theoretical works, but some practical surveys need to be conducted as well. Therefore, this master's thesis compares three different empirical studies on the exercise of the right of access and also describes my own experience with the right of access to personal data in practice. For accurate legal comprehension of the issue in question, I have predominantly used in this master's thesis the opinions and guidelines of Article 29 Working Party (hereinafter the "WP29"), the commentary on the GDPR by the Oxford University, recitals to the GDPR, and the judgments of the Court of Justice of the European Union (hereinafter the "CJEU"). Correspondingly, both analytical and empirical methods have been used to achieve the aim of this master's thesis.

The thesis is divided into four chapters that are further subdivided into sections according to the different components that particularly need to be discussed for the purposes of this master's thesis. The first two chapters are rather informative and descriptive, as they should provide the reader with an introduction to the issue of personal data protection and data subject rights. Subsequently, the third and fourth chapter specifically address the right to be informed and the right of access to personal data as the main aspects of the topic of this master's thesis. In these chapters, the focus is not only laid on the theory but also on the practical side of these rights, which is their availability to individuals, their usage, and exercise.

[6] The Supervisory authority of the Czech Republic
[7] Gonzales Fuster, Docksey, Nulíček et al, Pokorná and Dvořáková and others.

1. DEVELOPMENT OF THE RIGHT TO PERSONAL DATA PROTECTION

Personal data protection is an integral part of life in a modern society we belong to. Everyone has a right to such protection and can benefit from it. In fact, it took years to develop the right to personal data protection into the standard it represents today. Since the right to personal data protection has not been classified among the first fundamental rights that were codified in fundamental international human rights documents, it was primarily considered to be an accessory right to the right to privacy. However, over time, it has developed into a separate fundamental right. This chapter discusses the roots of the right to personal data protection and explains some of the essential concepts of data protection law which are necessary to grasp to comprehend this master's thesis.

1.1. A link to the right to privacy

The normative roots of personal data protection are inseparably connected to the phenomenon of privacy. Data protection instruments were primarily introduced to complement the right to privacy, to serve as a subordinate or an accessory part of this right.[8] The right of privacy itself is one of the oldest human rights. One of the first interpretations was formulated by Warren and Brandeis who described the right to privacy as "*the right to be let alone*" by the end of the nineteenth century. They supposed the value of privacy *"is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all*".[9] More than fifty years later, the United Nations General Assembly in 1948 adopted the Universal Declaration of Human Rights (hereinafter the "UDHR"). It was the first international legal act that granted individuals the protection of their privacy. Its Article 12 states that no one shall be subject to arbitrary interference with his or her privacy, family, home, correspondence, honour, and reputation and that everyone has the right to the protection against such interference or attacks. The UDHR is a non-binding declaration. However, it is considered to be a very important act in the international human rights law. The rights codified in it have created the

[8] VAN DER SLOOT, B. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: *Data Protection and Privacy: (In)visibilities and Infrastructures*. Vol. 36. Cham, Switzerland: Springer, 2017, p. 3-30. ISBN 978-3-319-50796-5. DOI 10.1007/978-3-319-50796-5. Page 5.

[9] WARREN S., BRANDEIS L. The Right to Privacy, Harvard Law Review (1890). Page 200.

basis for many posterior legal documents.[10] Another important human rights act concerning privacy is the European Convention on Human Rights (hereinafter the "ECHR") adopted by the Council of Europe in 1950. Unlike the UDHR, the ECHR does not explicitly mention the term of privacy at all. Instead, it uses the term "private life". [11] In its Article 8 it stipulates that "*everyone has the right to respect for his private and family life, his home and his correspondence*." The ECHR is binding for its contracting parties, i.e. 47 Member States of the Council of Europe. Both the UDHR and the ECHR prohibit the interference with the privacy of an individual. The ECHR allows an exception where such interference is in accordance with the law, necessary in a democratic society, pursues legitimate public interests or is necessary for the protection of the rights and freedoms of others. However, the protection of personal data or personal information has not been acknowledged in any of these legal documents. But, they both mention the protection of privacy in correspondence that usually contains private information, which might be the first reference to personal data.

Both the UDHR and the ECHR were adopted before the huge development of the information technology. The right to privacy or private life in those times rather meant the protection of individuals against unlawful interference by a state. However, over time, the need of regulation to protect human rights in the context of new scientific and technological developments started to grow rapidly. The more individuals started to share their personal information publicly, the broader the use of personal data by public authorities as well as private companies to pursue their interests was.[12] Thus, the foundations of the right to personal data protection dwell in the right to privacy since it has served to protect an individual's privacy against unlawful interferences with inter alia his or her personal data.[13]

1.2. The right to personal data protection as a new separate right

The right to personal data protection does not widen the scope of the right to privacy but constitutes the new separate right, as Docksey declares[14]. The right to personal data

[10] *Handbook on European data protection law*: 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Page 21.
[11] GONZALEZ FUSTER, G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU: Issues in Privacy and Data Protection* Law, Governance and Technology Series. Vol 16. Brussels: Springer International Publishing, 2014. ISBN 978-3-319-05023-2. DOI 10.1007/978-3-319-05023-2. Page 38.
[12] Recital 6 to the GDPR.
[13] DOCKSEY, CH. Four Fundamental Rights: Finding the Balance. *International Data Privacy Law*, Vol. 6, Issue no. 3 (2016), pp. 195–209. DOI:10.1093/idpl/ipw014. Page 197.
[14] Ibid. Page 198.

protection started to independently conceive in 1970s in national jurisdictions, but also at regional level under the Council of Europe, the Organisation for Economic Co-operation and Development or the European Union.

1.2.1. The right to personal data protection under the Council of Europe

In the early 1970s, the Council of Europe started to shift their concern from protecting the "private life" to the protection of individuals' personal data.[15] In the following years, the Committee of Ministers adopted the Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector (hereinafter the "Resolution (73)") and the Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector (hereinafter the "Resolution (74)") (hereinafter jointly the "Resolutions"). The Resolutions had recommendatory nature for the governments of the Member States, advising them to comply with the principles set out in the Annexes to the Resolutions[16]. These principles applied to personal information stored in electronic data banks in the private and the public sector[17]. The Annex to Resolution (73) contains roots of the right of access to personal data. The first paragraph of the Principle 9 states that "*access to the information stored should be confined to persons who have a valid reason to know it*."[18] The Explanatory Report specifies that those persons can be either the users of the data banks and their clients or the operators of the electronic data banks.[19]

The Council of Europe did not stop after the adoption of the Regulations but continued to elaborate the complex regulation related to the data protection. In 1981, it adopted the Convention for the protection of individuals with regard to automatic processing of personal data (hereinafter the "Convention 108"). The Convention 108 concerns automatic data processing by both the private and the public sector, as well as data processing by the judiciary and law enforcement authorities. It lays down the key principles of data protection,

[15] GONZALEZ FUSTER, G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU: Issues in Privacy and Data Protection* Law, Governance and Technology Series. Vol 16. Brussels: Springer International Publishing, 2014. ISBN 978-3-319-05023-2. DOI 10.1007/978-3-319-05023-2. Page 84.
[16] Ibid. Pages 85-86.
[17] The Resolutions
[18] The Resolution (73)
[19] Explanatory Report of the Resolution (73) 22 paragraph 36. Access via http://www.legislationline.org/documents/id/6498 Retrieved 29.10.2020.

such as purpose limitation, data minimization, accuracy, and storage limitation.[20] Moreover, it emphasizes the necessity of providing appropriate safeguards on personal data that are being processed. Among other important provisions, the Convention 108 sets forth the right of access to personal data, which is further discussed in Chapter 4. The main purpose of the Convention 108 is to provide individuals with a respect for their fundamental rights, particularly for their right to privacy, with regard to automatic processing of personal data relating to them.[21] At that time, the right to personal data protection started to appear more frequently in case law. Over the years, the European Court of Human Rights (hereinafter the "ECtHR") started to use the Convention 108 as a guide to figure out the extent of the violation of the right to respect for private life granted by Article 8 of the ECHR. The interpretation of this right became broader, encompassing the protection of personal data inward.[22]

The enactment of the Convention 108 represents an important point in data protection law. Since then, the data protection started to be recognised more and became closer to individuals, as the ECtHR has been including it in its decisions. The Convention 108 was revised in 2018. It is binding for those states that have ratified it, which makes it the only international legally binding instrument on personal data protection today.

1.2.2. The right to personal data protection under the Organisation for Economic Cooperation and Development

The OECD had been orientating in the field of new computer and communication technology for a few years before it decided to tackle the problem of the protection of privacy as well. In 1978, the OECD instructed a Group of Experts to work on a development of an international instrument on the protection of privacy, mainly because among the OECD Member States the national legislatures in this field differed.[23] In 1980, the OECD adopted

[20] *Handbook on European data protection law*. 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Pages 24-25.
[21] GONZALEZ FUSTER, G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU: Issues in Privacy and Data Protection* Law, Governance and Technology Series. Vol 16. Brussels: Springer International Publishing, 2014. ISBN 978-3-319-05023-2. DOI 10.1007/978-3-319-05023-2. Page 88.
[22] DOCKSEY, CH. Four Fundamental Rights: Finding the Balance. *International Data Privacy Law*. Vol. 6, Issue no. 3 (2016). pp. 195–209. DOI:10.1093/idpl/ipw014. Page 197.
[23] Annex to the Recommendation of the Council of 23rd September 1980: Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data: Explanatory Memorandum. Available via: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#introduction Retrieved 20.11.2020.

the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[24] (hereinafter the "Guidelines"). The Guidelines set out minimum standards for effective protection of personal data and stipulated the set of eight non-binding principles to apply to manual and electronic processing of personal data in both the public and private sectors. These principles should have been achieved at the national level. What is important in terms of this master's thesis, the Guidelines recognise inter alia the right of access to personal data in paragraph 13. The Explanatory Memorandum explicates that the right of access should be simple to exercise, by which it means that the exercise of this right should not involve any complicated processes or measures, but rather be considered a controller's daily activity. Personal data should be communicated to data subjects within a reasonable time, at no (excessive) charge, in a reasonable manner, and in a readily intelligible form.[25]

1.2.3. The right to personal data protection under the primary law of the EU

Since the foundations of the European Economic Community bore upon economic integration and the establishment of a common market, the original treaties did not refer to the protection of individuals' fundamental rights or freedoms at all.[26] During the virtue of the pillar structure, data protection was divided between the first (European Economic Community, later European Communities) and the third pillar (cooperation between the Member States in the fields of justice and home affairs.).[27] In 2000, the European Union adopted the Charter of Fundamental Rights of the European Union (hereinafter the "Charter"). The Article 8 of the Charter constituted the ultimate protection of personal data in the EU at that time. In the first paragraph, it explicitly awards everyone the right to the protection of personal data. In the second paragraph, it enshrines that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. This paragraph also includes the right of access to personal data and the right to rectification. The third paragraph assigns independent supervisory authorities a duty to control the compliance with the data protection rules.[28] Controllers are

[24] OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)
[25] The Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (OECD). Paragraph 13.
[26] *Handbook on European data protection law*. 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Page 27.
[27] Fact Sheets on the European Union, European Parliament – Personal Data Protection. Available via: https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection Retrieved 1.10.2020.
[28] Article 8 of the Charter

obliged to comply with the stipulated principles and data subjects are entitled to the protection of their personal data both ex ante and ex post of the processing, regardless of whether there has been any interference with their privacy. However, the Charter was primarily a non-binding document, so the right to the data protection under it could not be enforced by individuals. The CJEU had not been even referring to the Charter in its case law.[29]

The Lisbon Treaty signed in 2007 brought a change in many aspects of Union law. The pillar structure was revoked, while the European Parliament was granted new co-legislative powers.[30] The Charter was elevated to the level of a legally binding document within the EU primary law.[31] This all contributed to the development of more precise protection of personal data in the European Union. The Lisbon Treaty incorporated into the Treaty on the functioning of the European Union (hereinafter the "TFEU") a new important provision of Article 16, which not only rewards everyone with the right to the protection of their personal data (paragraph 1), but also provides a legal basis for the European Parliament and the Council to lay down rules relating to the protection of individuals with regard to the processing of personal data, and recalls that compliance with these rules shall be subject to control by independent authorities (paragraph 2).[32]

Article 8 of the Charter provides a fundamental character to the right of data protection and has been legally binding since the adoption of the Lisbon Treaty. Docksey points out that this is a significant division from Article 8 of the ECHR, which "only" grants the right to private life[33]. Although, the Charter also grants the right to private life in its Article 7. During the time of the adoption of the Charter, the right to data protection had already been exempted from the right to private life. Therefore, the two provisions of the Charter are different in their scope and the right to data protection should not be perceived as a part of the right to private life anymore.

[29] DOCKSEY, CH. Four Fundamental Rights: Finding the Balance. *International Data Privacy Law*, vol. 6, no. 3, 2016, pp. 195–209., DOI:10.1093/idpl/ipw014. Page 198.
[30] Fact Sheets on the European Union, European Parliament – Personal Data Protection. Available via: https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection Retrieved 1.10.2020.
[31] *Handbook on European data protection law*. 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Page 27.
[32] Article 16 of the TFEU.
[33] DOCKSEY, CH. Four Fundamental Rights: Finding the Balance. *International Data Privacy Law*, vol. 6, no. 3, 2016, pp. 195–209., DOI:10.1093/idpl/ipw014. Page 198.

1.2.4. The right to personal data protection under the secondary law of the EU

The right to personal data protection appeared in the secondary law for the first time in the mid-1990s. The Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the "Data Protection Directive" or "the DPD") represented a significant legal instrument in the European data protection law until 2018. The aim of its adoption was to harmonise the existing legislation of the Member States on the protection of personal data, to affirm the core principles set out by the Convention 108 and even extend them. [34] Since the directives are not directly applicable, Member States must implement them into their national legislation, while setting out their own means to achieve the goals laid down by the directives. On the one hand, this gives Member States a free hand in mechanisms used to achieve the goals set out by the directives. On the other hand, it might cause differences in the implementation and in the interpretation of the provisions stipulated in the directives among the national legal systems. Likewise, the nature of the DPD caused that Member States implemented its provisions differently, which led to a different level of the protection of personal data among the Member States. It took years to substitute this system with more effective one. In 2016, the European Parliament and the Council adopted the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation). The GDPR was created to update the provisions of the Data Protection Directive and adjust them to the current digital age we live in and which is still developing.[35] One of many highlights of the GDPR is strengthening of the data subject rights, which allows data subjects to have better control over their personal data.[36] Considering that regulations are under Union law directly applicable, the GDPR represents a single set of data protection rules that apply over the EU and finally provides the equal level of protection irrespective of which Member State a data subject is in.[37] The protection granted by the GDPR relates only to natural persons, irrespective of their

[34] *Handbook on European data protection law*. 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Page 29.
[35] Ibid. Page 30.
[36] European Commission Press Corner Questions and Answers: Data Protection Reform. Available via: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_ Retrieved 3.10.2020.
[37] *Handbook on European data protection law*. 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Page 30.

nationality or place of residence.[38] The GDPR does not apply to personal data of deceased persons, nor to the data of legal persons.

1.3. Defining the core terms of data protection law

It is necessary to define the core concepts of data protection law that will be discussed in this master's thesis in order to get the message of the data protection law properly. The definitions mentioned further have been mostly formed by the current legislation of the GDPR.

1.3.1. The processing of personal data

The GDPR applies to the processing of personal data fully or partly by automated means or to the processing other than by automated means when personal data are part of a filing system or are intended to be part of a filing system[39]. This delimitation of the material scope of the GDPR informs us that its provision applies to certain activities that dwell in the processing of personal data. But what actually does the term processing mean? According to the definition from Article 4 (2) of the GDPR, the processing is "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*." This provision provides a demonstrative list of operations performable by controllers or processors seeking to achieve certain goals[40]. In line with that, practically anything can be interpreted as the processing of personal data. It can be a whole group of activities such as collecting personal information, sorting it out, passing it to another party, all in order to e.g., enter into a contract. Or, it can be a single operation as a storage of personal data by a banking company to fulfil its legal obligations of anti-money laundering laws. The term processing is really wide, and it can be applied to any operation with personal data. However, the GDPR only applies to cases where the processing is conducted by automated means or by other means, where personal data are being held in a filing system. In the

[38] Article 1 (2) of the GDPR.
[39] Article 2 (1) of the GDPR.
[40] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 84

territorial scope, the GDPR applies to the processing of personal data in the context of the activities performed by a controller or processor established in the Union, regardless of where the processing takes place, and to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing relates to offering of goods or services to data subjects in the Union, or the monitoring of data subjects' behaviour which takes place within the Union. The GDPR also applies to the processing which takes place outside of the EU, but where Member State law applies by virtue of public international law.[41]

The concept of processing is inseparably linked with the term personal data. Article 4 (1) of the GDPR defines it as "*any information relating to an identified or identifiable natural person*", which is the same definition contained in the Data Protection Directive. The legislator's aim remained unchanged during the creation of the current legislation. This aim has been to provide the broadest definition of personal data as possible[42]. Therefore, personal data might indicate any sort of information relating to an identified or identifiable natural person. The CJEU in the case *Breyer* pointed out that to consider an information to be personal data, it is not necessary for the information itself to identify a data subject[43]. This means that also a piece of information that alone does not tell anything about the data subject can be considered personal data if it is able to identify the data subject when connected with other information. In the case *Breyer* it was a dynamic IP address that the CJEU regarded as the personal data. In addition, according to the WP29 opinion, personal data is any information, regardless of the content of the information, regardless of whether it is true or false and regardless of a form of such information[44].

1.3.2. Data subject, controller, and processor

The definition of personal data in the GDPR also encompasses the definition of a data subject. It is a natural person that can be identified, directly or indirectly, in particular by a reference to an identifier. A bit difficult concept of identifiability of natural persons is explained by the WP29 as the possibility of distinguishing a person from another one, based

[41] Article 3 of the GDPR.

[42] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 77

[43] C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779

[44] Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data. Page 7-8

on some information, i.e. the identifier[45]. These identifiers are demonstratively mentioned in the definition included in the GDPR, such as name, identification number, location data, etc[46].

Whoever determines the means and purposes of the processing of personal data is considered a controller[47]. It can be a natural, legal person or public authority. If there are two or more of them, they are jointly referred to as "joint controllers". Controllers must comply with multiple legal obligations imposed by the GDPR and are responsible for the implementation of appropriate technical and organisational measures to ensure that the processing is performed in accordance with the GDPR and they must be able to prove that[48]. Indeed, controllers have control over the processing of personal data and are responsible and legally liable for that control.[49] The CJEU in *Google Spain*[50] ruled that Google as the operator of the search engine has to be regarded as the controller because it determines the means and purposes of the processing when it temporarily stores personal data, indexes them and makes them available to internet users. Based on that, the controller must ensure, within the framework of its responsibilities, powers, and capabilities that its processing activities are done in compliance with the rules and requirements set forth by the Data Protection Directive so the protection of personal data may have full effect[51].

A processor is a natural or legal person, public authority or any other body which processes personal data on behalf of the controller.[52] The relationship between the controller and the processor must be determined by the Data Processing Agreement which is a contract that stipulates the purposes and duration of the processing, the types of personal data concerned and categories of data subjects, the rights and obligations of the parties, etc.[53] Not having such contract constitutes a breach of the GDPR, especially of the controller's obligation to provide a written documentation of mutual responsibilities. Such a breach may

[45] Ibid. Page 12.
[46] Article 4 (1) of the GDPR.
[47] Article 4 (7) of the GDPR.
[48] Article 24 (1) of the GDPR.
[49] *Handbook on European data protection law*. 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Page 101.
[50] C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. ECLI:EU:C:2014:317.
[51] Ibid. Paragraph 38 of the judgment.
[52] Article 4 (8) of the GDPR.
[53] Article 28 (3) of the GDPR.

eventually lead to imposition of sanctions.[54] The processor must process personal data based on the instructions given by the controller. If the processor exceeds them, and de facto determines means and purposes of the processing, then the processor must be considered the controller. However, the overall responsibility of the processing lies on the controller ensuring that the processing is performed in compliance with the controller's instructions and with Union law.[55]

1.4. Conclusion

The aim of the first chapter of this master's thesis is to introduce the development of the right to personal data protection. From being regarded as an accessory right to the right to privacy, the right to data protection developed into a fundamental human right, established in the Charter and the TFEU. The legal act fully dedicated to personal data protection that is currently in force on the international level is the Convention 108, while on the Union level it is the GDPR. The direct effect of the GDPR ensures the equal level of personal data protection of natural persons among the Member States of the EU. Every processing activity of a controller or processor established in the Union and every processing related to offering of goods or services in the EU or monitoring of the behaviour of data subjects, insofar as their behaviour takes place within the EU, should be carried out in accordance with the GDPR. The final section of this chapter is dedicated to defining the core concepts of personal data protection that are further used in this master's thesis.

[54] *Handbook on European data protection law*. 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Page 109.
[55] Ibid. Pages 108-109.

2. RIGHTS OF DATA SUBJECTS GRANTED BY THE GDPR

Data subject rights compose an intrinsic part of a fundamental right to personal data protection. Some of them have even appeared in Article 8 of the Charter. Under the GDPR, data subjects have been awarded broader list of rights laid down in Articles 15 to 22 than ever. This chapter is devoted to the general comprehension of the importance of data subject rights and principles pertaining thereto.

2.1. Effective protection of personal data

In general, effective legal protection of certain interests depends on the enforcement of individuals' rights. In other words, to make a legal protection effective, it is important to enable the subjects of that protection to exercise and claim their rights. Given that controllers (indeed also processors) dispose of individuals' personal data and so may perform different operations with them, it can be assumed that data subjects are the weaker party of the controller-data subject relationship. Even the diction of a controller in the GDPR states that it determines means and purposes of the processing. Hence, the controller is undoubtedly in the superior position because it has control over the operations with personal data at stake, whereas the data subject cannot affect those operations. In private law, e.g. the employment law or the consumer law, a common practice is to strengthen the position of the weaker party to maintain the principle of equality between the parties. Similarly, if legislators want to mitigate the power inequality between controllers and data subjects, they have to grant data subjects efficient rights and impose duties on controllers (indeed also on processors).[56] Recital 11 to the GDPR confirms this hypothesis by stating that the effective protection of personal data is achieved by strengthening the rights of data subjects and the obligations of controllers and processors, along with monitoring compliance thereof with legal rules and imposing equivalent sanctions for breaching them. The ability of data subjects to effectively exercise the rights granted by Articles 15 - 22 of the GDPR is inherently linked to the fundamental right to effective judicial protection stipulated in Article 47 of the Charter[57]. The CJEU in *Schrems* has concluded that a legislation which does not give individuals any possibility to pursue legal remedies in order to obtain the access to personal data relating to them, or to

[56] *Handbook on European data protection law*. 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4. Page 205.

[57] AUSLOOS, J., VEALE M., MAHIEU R. Getting Data Subject Rights Right: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2019, *10*(3), 283-309. Page 284.

obtain the rectification or erasure of their personal data, "*does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter*"[58].

Some of data subject rights have been guaranteed since the beginning of data protection law, others have been brought along the way of developing information technologies. Second paragraph of Article 8 of the Charter embodies the right of access to personal data and the right to rectification. Equivalently, these rights were also included in the Convention 108 before it was revised[59]. The Data Protection Directive guaranteed some of data subject rights such as the right of access to personal data, the right to rectification of incomplete or inaccurate data and the right to object to processing. However, these rights were not stipulated precisely enough. Consequently, the GDPR has advanced the rights laid down by the Data Protection Directive and added some new ones to the list. For instance, the right to data portability is a brand new right introduced by the GDPR. In such manner, the GDPR nowadays provides a wide scale of data subject rights incorporated in Articles 15 - 22, including the right of access to personal data, the right to rectification, the right to erasure (known also as the right to be forgotten), the right to restriction of processing, the right to data portability, the right to object and the right to not be subject to automated decision making. Sometimes other rights are added to that list. Typically, it is the right to be informed[60], the right to lodge a complaint with a supervisory authority[61], the right to an effective judicial remedy against a supervisory authority[62] and the right to an effective judicial remedy against a controller or a processor[63]. Data subject rights generally work as tools empowering data subjects to control the manner of dealing with their personal data, to modify the flaws of the processing or to claim appropriate compensation for infringements. I personally believe that sufficient awareness of data subjects of these rights is a crucial element of data protection, including their ability to conveniently exercise them and eventually claim them.

[58] C-362/14, Maximillian Schrems v Data Protection Commissioner. ECLI:EU:C:2015:650. Paragraph 95 of the judgment.
[59] The Modernised Convention 108's scope of data subject rights is nowadays similar to the scope of data subject rights of the GDPR.
[60] Articles 11-13 of the GDPR.
[61] Article 77 of the GDPR.
[62] Article 78 of the GDPR.
[63] Article 79 of the GDPR.

2.2. The principles of transparency, fairness, and accountability

Data protection introduces certain procedural rules for controllers to adhere in order to comply with the principle of transparency. The role of the principle of transparency is to facilitate the exercise of the rights of data subjects, ensuring that all of the information provided to them is clear and easy to understand, and to keep controllers and processors responsible for their processing activities being conducted in compliance with data protection rules. This principle is inseparably linked to the principles of fairness and accountability. Generally, the principle of fairness requires the processing to be lawful and fair, while the principle of accountability makes a controller responsible for such lawfulness, fairness, and transparency, and requires them to be able to demonstrate such compliance. These three principles are encompassed throughout the whole GDPR, reflecting the specific data protection rules and requirements, e.g. for the purposes of processing, collection and storage of personal data, information to be provided to data subjects, communication with data subjects, appropriate security of personal data, etc.[64] The WP29 further emphasises that in accordance with the principles of transparency, fairness and accountability, controllers must familiarize data subjects with possible consequences that the processing might have, inform them of the possibility of risks that data subjects should be aware of, notify them of any changes of the information that had been provided to them before, and to provide this information to data subjects in advance before the expiration of stipulated time limits. The principles of transparency, fairness and accountability apply from the beginning of the processing through its whole process.[65]

In relation to data subject rights, the principles of transparency, fairness and accountability are reflected in Article 12 of the GDPR which sets out the common requirements that apply to all of the data subject rights under Articles 15 – 22. They apply irrespective of the legal basis for processing and throughout the whole period of processing.[66] The first paragraph of this provision obliges controllers to take appropriate measures to communicate with data subjects in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. Such requirements must be fulfilled when providing information pursuant to Articles 13 and 14, but also in any other communication with data subjects regarding the rights laid down by Articles 15 – 22. Specific means of communication

[64] Recital 39 of the GDPR.
[65] Article 29 Working Party: Guidelines on transparency under Regulation 2016/679. Pages 4 – 6.
[66] Ibid.

should be used with vulnerable groups of data subjects, such as children, so that the addressee recognises the information and understands it.[67] Article 12 does not order a specific form of communication, but it sets out the principal requirements for it. Under the first paragraph of this provision, the controller's response to the request made by the data subject must be in writing or by other means, which commonly represents electronic means. However, when the data subject wishes to be given some information orally, the controller should comply with that. Thus, in relation to the form of the communication, it is actually the data subject's choice. If he or she files a request in a certain form, the controller must reply and provide necessary information in the same form, if it is possible.[68]

Another requirement resulting from Article 12 of the GDPR is that controllers must deal with requests made by data subjects regarding the exercise of their rights without undue delay. In other words, they must respond as soon as possible, but no later than one month after the request was made. This period may be extended for additional two months if necessary, especially when the controller has to deal with multiple requests.[69] However, Nulíček et al. remark that the reasons for prolonging the period to respond should only relate to the number of requests made by one specific data subject[70]. That is to say, it should not be allowed to prolong the period to respond to a request on the grounds of dealing with large number of requests from multiple data subjects. When the controller has acceptable reasons for extending the response period, the controller still must inform the data subject of such extension within one month from receiving the request, together with specifying the reasons for such delay.[71] The monthly response period continues even in the situation when the controller decides not to take any action towards the data subject's request. In such situations, the controller still bears the information obligation. Therefore, the reasons for not taking any action, the possibility of lodging a complaint with a supervisory authority and the possibility of seeking a judicial remedy must be provided by the controller within a thirty-day period pursuant to Article 12 (4) of the GDPR, even when the controller decides not to deal with the data subject's request.

---

[67] Article 29 Working Party: Guidelines on transparency under Regulation 2016/679. Page 10, paragraph 14.

[68] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 184.

[69] Article 12 (3) of the GDPR, Recital 59 to the GDPR.

[70] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 186.

[71] Article 12 (3) of the GDPR.

Based on the fifth paragraph of the aforementioned provision, data subjects have to be able to exercise their rights free of charge unless their requests would be manifestly unfounded or excessive, particularly because of the repetitive character of the requests.[72] The GDPR uses the term "*manifestly unfounded or excessive*" without any explanation. On the one hand, Polčák suggest interpreting this expression by analogy to the established practice of Member States[73]. On the other hand, Nulíček et al. interpret the manifestly unfounded requests as requests lacking justification where it is necessary and manifestly excessive requests as repetitive ones or as requests of large amounts[74]. Nevertheless, the burden of proof of the manifestly unfounded or excessive character of the request lies on the controller. Therefore, the interpretation of these expressions needs to be analysed on a case-by-case basis according to the circumstances provided by the controller. The problem of manifestly unfounded requests in the matter of the right of access to personal data is further discussed in Section 4.3.1.

Most importantly, controllers are generally supposed to facilitate the exercise of data subject rights.[75] This should involve assisting data subjects in exercising their rights, responding to their requests in stipulated time periods and generally acting in favour of their requests and preventing them from any harm that could disrupt possibilities of exercising the rights granted by the GDPR under Articles 15 – 22.

Summing up, the GDPR clearly imposes an important role to the rules laid down in Article 12 in order to improve the conditions under which controllers deal with data subjects and process their personal data. Article 12 reflects that the practical requirements on the quality, accessibility and comprehensibility of the information is as important as the actual content of the information necessary to be provided to data subjects.[76]

[72] Article 12 (5) of the GDPR.
[73] The EU General Data Protection Regulation (GDPR). *A Commentary.* Edited by KUNER, CH., BYGRAVE, L. A., DOCKSEY, CH. Oxford University Press, 2020. ISBN 978-0-19-882649-1. Pages 408-409 (Polčák).
[74] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 187-188.
[75] Article 12 (2) of the GDPR.
[76] Article 29 Working Party: Guidelines on transparency under Regulation 2016/679. Page 5.

2.3. Restrictions of data subject rights

In spite of the fact that data subject rights are very important, it must be noted that they are not absolute, thus can be limited. According to Article 52 (1) of the Charter, limitations of the rights must be provided for by law and they must respect the essence of the rights. They may be made only if necessary, while meeting objectives of general interest. The GDPR lays down specific regime for limitations of data subject rights. Its Article 23 allows the Union or Member States to adopt a legislative measure to restrict the scope of the obligations and rights stipulated in Articles 12 – 22, Article 34 and Article 5 of the GDPR.[77] Nulíček et al. consider Article 23 as one of the most important provisions of the GDPR when it comes to individual modifications made on the national level since the provision affords Member States the possibility of adopting restrictions of the rights and duties imposed by the GDPR[78]. Nonetheless, such restrictions must be necessary for the public interest and other rights of individuals, while the balance with the right to data protection must be preserved[79]. Based on Recital 73 to the GDPR, the restrictions should also comply with the provisions of the Charter and the ECHR. The restrictions of the data subject rights shall be imposed only for the purposes exhaustively enumerated in Article 23 which requires such restrictions to be necessary and proportionate measure to safeguard national security, defence, public security, prevention, investigation, the detection or prosecution of criminal offences or the execution of criminal penalties, including the prevention of threats to public security, any other important objectives of general public interest, in particular an important economic or financial interest of the Union or of a Member State, the protection of judicial independence and judicial proceedings, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, monitoring or inspection connected to the exercise of official authority, protection of the data subject or the rights and freedoms of others, and the enforcement of civil law claims[80]. Thus, the GDPR requires restrictions of data subject rights to be "the necessary and proportional measure", but does not define what is meant by this expression. According to Pokorná and Dvořáková, "the proportional measure" mentioned in Article 23 signifies a measure that limits the restriction of data subject rights to a minimum

[77] To the extent that Article 5 corresponds to the rights and obligations in Articles 12 to 22.

[78] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 241.

[79] POKORNÁ, A., DVOŘÁKOVÁ H. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020. ISBN 978-80-7598-309-1. Page 216.

[80] Article 23 (1) of the GDPR.

that is necessary for the purposes set out in paragraph 1 of that article. The expression "the necessary measure" then signifies a provision needed because there is no other measure to achieve the purposes set out in the aforementioned article.[81]

When the Union or Member States decide to impose the restrictions, they must also bear in mind the condition mentioned in Article 23 (2). This paragraph sets out requirements for the content of the legislative measure, based on which data subject rights would be restricted. Such legislative measure must contain particular information on the purposes or categories of processing, the categories of personal data, the scope of the restrictions, the safeguards to prevent abuse or unlawful access or transfer, the specification of the controller or categories of controllers, the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing, the risks to the rights and freedoms of data subjects, and the right of data subjects to be informed of the restriction, unless informing them is prejudicial to the purpose of the restriction. The condition of providing such information to data subjects is a reflection of the principle of transparency. In line with that, data subjects would not be surprised of a restriction of a particular right when they later attempt to exercise it against the controller.[82] If a legislative measure that is purported to restrict data subject rights does not contain specific provisions pursuant to Article 23 (2), it will lead to a refusal of adoption of such measure on the grounds of non-compliance with the GDPR. Scrutinizing the compliance of such legislative measures with Article 23 is left to national courts that have to take into account the circumstances of individual cases and the case law of the CJEU, particularly in the interpretation of the concept of proportionality and necessity of such measure.[83]

Besides the general restrictions of the data subject rights permitted under the conditions laid down by Article 23, the GDPR also contains some specific ones. Pursuant to Article 6 (2), Member States may maintain or introduce more specific provisions in relation to the processing based on the compliance with a legal obligation to which a controller is subject, or on the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller,[84] by determining specific requirements for the

[81] POKORNÁ, A., DVOŘÁKOVÁ H. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020. ISBN 978-80-7598-309-1. Page 217.
[82] WP29: Guidelines on transparency. Page 34.
[83] POKORNÁ, A., DVOŘÁKOVÁ H. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020. ISBN 978-80-7598-309-1. Page 218.
[84] Article 6 (2) c), e) of the GDPR.

processing and other measures to ensure lawfulness and fairness of such processing. Another example are Articles 85 – 91 which allow Member States to adopt specific restrictions for various situations, such as collision of the personal data processing and the freedom of expression, processing of the national identification number, processing in the context of employment, etc.[85] Furthermore, restrictions of the right to be informed can be found in Article 14 (3), which is further discussed in Chapter 3 of this master's thesis.

The importance of data subject rights is undoubtful, as was already discussed. They serve data subjects to maintain some sort of control over the processing of their personal data and support the fundamental right of personal data protection. Nevertheless, as many other rights, these are also not absolute, as they might be restricted by the Union or Member States. Having in mind the importance of data subject rights and to preserve the fundamental right to data protection, it is necessary that these restrictions are made in the light of the principle of proportionality, transparency and only to the necessary extent.

2.4. Relevant Case law

2.4.1. C-486/12, X[86]

In the case of X, the CJEU has examined the legality of the principles of charging fees for exercising the right of access to personal data. Article 12 a) of the Data Protection Directive stipulated that every data subject had the right to obtain from the controller *"without constraint at reasonable intervals and without excessive delay or expense*" the confirmation whether there were his or her personal data undergoing processing and some information regarding such processing. The CJEU had to examine the interpretation of the expression *"without excessive delay or expense*". The question was whether this expression should be interpreted as "without expense" or "without excessive expense". The CJEU held it meant the latter, i.e. the provision should be interpreted in the manner that charging fees is generally possible, unless such fees are excessive, meaning they exceed the cost of communicating relevant personal data to the data subject. The CJEU proclaimed that Member States should have ensured a fair balance in levying fees, minding on the one hand, the interests of data

[85] POKORNÁ, A., DVOŘÁKOVÁ H. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020. ISBN 978-80-7598-309-1. Page 219.
[86] C-486/12. Request for a preliminary ruling under Article 267 TFEU from the Gerechtshof te 's-Hertogenbosch (Netherlands), made by decision of 26 October 2012, received at the Court on 31 October 2012, in the proceedings brought by X. ECLI:EU:C:2013:836.

subjects in protecting their privacy, and, on the other, the burden which the obligation to communicate such data represents for controllers.

Back then, these conclusions could have also been applied to the requests concerning other rights of data subjects. However, nowadays, the GDPR instructs controllers to provide information to data subjects ideally for free. Therefore, the conclusions of this case can apply only to the extent of manifestly unfounded or excessive request referred to in Article 12 (5) a) of the GDPR, where the controller can charge a reasonable fee, or in the situation where the data subject requests more than one copy of personal data according to Article 15 (3) of the GDPR.[87]

2.4.2. C-293/12, Digital Rights Ireland[88]

In this case, the CJEU has examined the validity of the Data Retention Directive[89] which aimed to harmonise national provisions for retaining citizens' personal data, generated, or processed by publicly available electronic communication services or networks in order to transmit them to competent authorities to fight serious crime such as terrorism. The Data Retention Directive allowed Member States to use citizens' data collected by electronic communication service providers. The CJEU found retained personal data of citizens to allow public authorities to have a precise picture of the private lives of those persons, such as the habits of everyday life, places of residence, daily movements and activities, social relationships, etc. The CJEU has held that the obligations imposed by the Data Retention Directive constituted an interference with the right to privacy and with the right to data protection. After that, the CJEU must have assessed whether such interference could be justified, while having taken into account Article 52 (1) of the Charter. The CJEU has pointed out that limitations to fundamental rights should only apply, insofar as it is strictly necessary, and that Union law must lay down clear and precise rules governing the scope of limitations and the safeguards for individuals[90]. It has held that the Data Retention Directive did not set

[87] POKORNÁ, A., DVOŘÁKOVÁ H. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020. ISBN 978-80-7598-309-1. Page 210.
[88] C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General. ECLI:EU:C:2014:238.
[89] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive).
[90] C-293/12, Digital Rights Ireland Ltd. Paragraphs 52-54 of the judgment.

out clear and precise rules governing the extent of the interference nor the clear safeguards for the protection of the retained data. On these grounds, the Data Retention Directive was held as invalid even though it pursued a legitimate aim.

This case demonstrates how a legislative measure that pursues a legitimate aim may interfere with the right to data protection. Every such interference needs to fulfil certain conditions to be justified. Here, the CJEU recalled Article 52 (1) of the Charter that requires any limitation of rights to undergo a test whether the essence of the rights is respected, whether it meets the objective of general interest and whether it meets the principle of proportionality. Similarly, the restrictions of data subject rights are only lawful if they respect the essence of the fundamental rights and freedoms and compose a necessary and proportionate measure in a democratic society to safeguard an important interest stipulated in Article 23 (1) of the GDPR.

2.5. Conclusion

Chapter 2 is dedicated to the general notion of data subject rights. Some of them have been a part of data protection since its origins while others have been introduced later with adoptions of new legislations that adapt to current level of technological and informational developments. However, they all are equally important instruments in enforcing the protection of individual's personal data. Section 2.2. discusses how the principles of fairness, transparency and accountability contribute to the effective use of data subject rights, as they require controllers to follow certain rules. These are stipulated in Article 12 of the GDPR and include inter alia the way of communication with data subjects, response time for their requests or fees that controllers may levy on data subjects. Controllers are generally compelled to facilitate the exercise of data subject rights. However, data subject rights are not absolute, since they may be restricted by the legislative measures enacted by Union or Member State law, where it is necessary and proportionate, aiming to safeguard an important interest. This chapter aspires to provide an introduction to data subject rights and related requirements for controllers, which I believe is necessary in order to proceed further in examining the role of the right of access to personal data.

3. THE RIGHT TO BE INFORMED

The awareness of the existence of data subject rights and of the possibility to exercise them is a key point for individuals in terms of protection of their personal data. Data subjects undeniably have a right to know by whom their personal data are processed or to whom their personal data are disclosed. They have the right to be informed of the important elements of the processing and of the possibilities of how they can enforce the protection of their personal data. For these reasons and due to the principle of transparency, there are certain aspects data subjects must be informed of by controllers. Such information should either come prior to the intended processing, or as soon as possible, in a situation where personal data are obtained from a third party and not from the data subject. This information obligation applies to all processing activities for all legal grounds for processing. Authors of the Oxford Commentary to the GDPR refer to it as "data protection notice" or "privacy notice".[91]

3.1. Legal background of the right to be informed

The Convention 108 did not explicitly mention the principle of transparency as a foundation of the right to be informed.[92] Nonetheless, its Article 8 a) stipulates that individuals shall be enabled to know the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or place of business of the controller. Clearly, this provision corresponds with the notion of the right to be informed as we know today, yet it is not that precise. Similar standard that appeared in the Convention 108 was encompassed in the OECD Guidelines from 1980. It was the paragraph 12, titled as "Openness Principle", which aimed to ensure availability of information on the existence and nature of personal data, the main purposes of their use, as well as the identity and residence of the data controller. The principle reckons the existence of a general policy of openness about developments, practices, and policies with respect to personal data. The paragraph 12 of the OECD Guidelines remained unchanged after the revision of the Guidelines in 2013.[93]

The legislation of the EU has gradually contributed to advancing the right to be informed. The Data Protection Directive in its Articles 10 and 11 obliged controllers to provide a certain minimum of information about processing to data subjects. When data were

[91] The EU GDPR: *A Commentary*. Page 415.
[92] On the contrary, Modernised Convention 108 imposes the principle of transparency into its Article 8.
[93] The EU GDPR: *A Commentary*. Page 421.

collected from the data subject, the controller had to provide two types of information: the controller's identity (possibly also the identity of its representatives) and the purposes of the processing. Any further information needed to be provided when it was necessary for connection with the specific circumstances under which personal data were processed, to guarantee fair processing towards the data subject.[94] The examples of such further information were stated in the Data Protection Directive as the recipients of the personal data, an obligatory or a voluntary character of replies to the questions, consequences of failure to reply and the existence of the right of access and the right to rectify personal data unless the data subject had already had that information. Similarly, when personal data were not obtained from the data subject, it was also necessary to provide the information on the identity of the controller or its representatives and on the purposes of the processing, perhaps also further information as in the previously mentioned situation. When personal data were obtained from a source other than the data subject, the necessary information had to be provided to the data subject at the time of undertaking the recording of the personal data or no later than when the first disclosure of the personal data to a third party took place[95]. However, this was not necessary when the data subject had been aware of those facts before, or, where the processing was carried out for statistical purposes or for the purposes of historical or scientific research, or where communicating such information was impossible or would take disproportionate effort or if the processing was expressly laid down by law. Nonetheless, in these cases, the ensuring of appropriate safeguards was needed to be implemented.[96]

3.2. The right to be informed under the GDPR

The GDPR incorporates the right to be informed in its Articles 13 and 14. Comparing with the previous EU legislation[97], the scope of the controller's information obligation towards data subjects has been extended. The division on the basis of a source of personal data, however, preserved. While Article 13 tackles the situation where personal data are collected from the data subject, Article 14 the situation where personal data have been obtained from a source other than the data subject. Both articles also make a distinction between the information that must always be provided to the data subject[98] and the further

[94] Article 10 (1) of the DPD.
[95] Article 11 (1) of the DPD.
[96] Article 11 (2) of the DPD.
[97] The Data Protection Directive.
[98] Article 13 (1), Article 14 (1) of the GDPR.

information which is necessary to ensure fair and transparent processing[99]. According to the Oxford Commentary, this distinction does not have any practical importance, but the wording of the second paragraphs indicates that this information is devoted to guarantee fair and transparent processing. Therefore, the second paragraph of both articles should be interpreted in the light of the principles of fairness and transparency. Articles 13 and 14 certainly impose on controllers a positive obligation to act.[100] By fulfilling this obligation controllers contribute to keep the processing transparent, as data subjects are aware of the fundamental aspects of the processing of their personal data and know who is processing them, to whom they are disclosed or how long they will be kept by a particular controller. All the information that must be communicated to data subjects pursuant to Articles 13 and 14 is of equal importance.[101] Since the GDPR does not prescribe the specific format of the data protection notice, a common practice is to provide the necessary information in the privacy policy of the controller. The United Kingdom's Supervisory Authority the Information Commissioner's Office (hereinafter the "ICO") informs that there are many appropriate techniques to provide the information to data subjects, e.g. via short notices, mobile and smart device functionalities, icons, etc. The ICO suggests using the same medium which was used to collect personal data, if it is possible.[102] Nonetheless, controllers must adhere to the principle of transparency and comply with the rules of communication set out in Article 12, along with taking into account all of the circumstances of the processing.[103] The form and the manner in which the information is provided to data subjects is important as much as the content of the data protection notice. The ICO also discusses that it might be challenging to encourage data subjects to read privacy information, as they are often unwilling to read detailed explanations and long terms and conditions. This should not arouse in controllers a feeling that providing information on the processing is just a formality. On the contrary, they should provide that information precisely and effectively so that data subjects understand it and maybe use that information in exercising their other rights.[104]

---

[99] Article 13 (2), Article 14 (2) of the GDPR.

[100] The EU GDPR: *A Commentary*. Page 427-428.

[101] WP29: Guidelines on transparency. Page 14.

[102] For organisations/Guide to Data Protection/Guide to the General Data Protection Regulation (GDPR)/Individual rights/Right to be informed. Available via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/#top Retrieved 29.11.2020

[103] WP29: Guidelines on transparency. Page 14.

[104] For organisations/Guide to Data Protection/Guide to the General Data Protection Regulation (GDPR)/The right to be informed/How should we draft our privacy information? Available via: https://ico.org.uk/for-

3.2.1. The right to be informed under Article 13 of the GDPR

Article 13 applies to situations where a controller obtains personal data from a data subject. According to WP29, this can occur in two situations: 1. when the data subject consciously provides his or her personal data to the controller (e.g. orally, via online forms, etc.) and 2. when the controller collects personal data from the data subject by observation (e.g. using cameras, voice recorders, wi-fi tracking devices, etc.).[105] A data protection notice in these cases should be provided at the time when the personal data are obtained.

The information that must be included in the data protection notice according to Article 13 (1) consist of: the identity and contact details of the controller (possibly of the controller's representative); the contact details of the data protection officer, if it is applicable; the purposes of the processing and the legal basis for the processing; the legitimate interests of the controller or of a third party if the processing is based on this ground; the recipients or categories of recipients of the personal data; the fact that the controller intends to transfer personal data to a third country or to an international organisation and appropriate information on what grounds[106] the transfer is to be made.

To ensure fair and transparent processing according to Article 13 (2), the controller must inform the data subject of the period for which the personal data relating to this data subject will be stored. If that is not possible, the controller must provide at least the criteria used to determine that period. However, WP29 emphasizes that it is not sufficient to declare that the personal data will be kept for as long as necessary for the legitimate purposes of the processing.[107] Thus, the controller must provide either exact time period or an explanation of how the period is determined so data subjects can at least expect for how long their data will be retained.[108] The controller then has to inform the data subject of the existence of the rights awarded to data subjects by the GDPR, particularly the right of access to personal data, the right to rectification or erasure of personal data, the right to restriction of processing or to object to processing, the right to data portability, and the right to lodge a complaint with a supervisory authority. According to the Oxford Commentary on the GDPR, this should also include a brief explanation of how data subjects can exercise these rights. Where the

organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/how-should-we-draft-our-privacy-information/#id1 Retrieved 29.11.2020

[105] WP29: Guidelines on transparency. Page 15.

[106] Articles 45-47 of the GDPR (the adequacy decision by the Commission, appropriate safeguards)

[107] Cited in: The EU GDPR: *A Commentary*. Page 428.

[108] The EU GDPR: *A Commentary*. Page 428.

processing is based on the data subject's consent, the existence of the right to withdraw the consent at any time needs to be communicated too. Afterwards, the controller must inform the data subject whether he or she must provide the personal data on the grounds of a statutory or contractual requirement, or whether it is necessary to enter into a contract, including possible consequences if the data subject fails to provide such data. Lastly, if there is automated decision making involved in the processing of personal data, including profiling, the controller must reveal its existence and information about the logic used in it. Also, the controller must provide the information about the significance and consequences of automated decision making for the data subject and about Article 22 of the GDPR which is devoted to the right not to be subject to a decision based solely on automated processing, which produces legal effects or similarly significantly affects the data subject.[109]

Article 13 (3) is dedicated to the situation where the controller intends to further process the personal data for a purpose other than that for which the personal data were initially collected. In such case, a new information obligation arises, by virtue of which the controller must inform the data subject of the new purposes of the processing. By all means, it must be done prior to the new further processing. Also, if any relevant information about the new processing referred to in Article 13 (2) does not cohere with the information provided for the former processing, it will need to be updated.[110]

Article 13 (4) represents an exemption from the data protection notice in the situation where the data subject already has the information from the aforementioned paragraphs of Article 13. For instance, it might occur when data subjects sign an amendment to the existing contract where the processing of personal data remains unchanged. The controller must always make sure that the data subject really possesses all the relevant information, and that the controller is able to prove so when needed. However, the fact that this information is enumerated in the GDPR does not deprive the controller of the information obligation. Even if the data subject can learn such information by reading the text of the GDPR, the controller still must provide all the necessary information.[111] In other words, the principle of *ignorantia legis non excusat* does not apply to data subjects because they have to be informed of all relevant facts by a specific controller who processes their personal data.

---

[109] Article 13 (2) of the GDPR.
[110] The EU GDPR: *A Commentary*. Page 430.
[111] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 195.

3.2.2. The right to be informed under Article 14 of the GDPR

Article 14 is applicable when the controller obtains personal data from a source other than the data subject. That is when the controller obtains personal data from another controller, whether it is a private or a public entity, or when the controller obtains personal data without any action of another controller or the data subject, e.g. in the investigation of a loss event.[112] The set of information that needs to be provided to the data subject pursuant to this provision partially overlaps with the information that needs to be provided according to Article 13. That includes the facts about the identity of the controller and its representative, the purposes of the processing, the existence of data subject rights, etc. The only exception is the information on a statutory or contractual requirement for the provision of personal data, or whether the data subject is obliged to provide personal data, which applies only if the personal data were obtained right from the data subject.[113] Article 14 (2) is devoted to ensuring fairness and transparency throughout the processing. Similarly to Article 13 (2), it concerns the period of data retention, the existence of data subject rights, the legitimate interests pursued by the controller or by a third party, if the processing is based on this ground, the right to withdraw a consent at any time, if the processing is based on the consent, the existence of automated decision making involved in the processing including profiling. In addition to the information required by Article 13, Article 14 also expects controllers to provide the categories of personal data concerned and the source of personal data since the data subject has not provided his or her personal data to the controller and thus cannot know what types of personal data are being processed and from whom the controller obtained them. Therefore, to comply with the principles of fairness and transparency, the controller must provide such information to the data subject too.[114] Awareness of all categories of data undergoing the processing as well as of their source is a necessary element for data subjects since without it they would not be able to exercise their data protection rights. Although the GDPR separates the information that has to be provided to data subjects into two paragraphs, all of it is equally important.[115]

Time periods for the delivery of the data protection notice under Article 14 are slightly more complicated than those in Article 13. Article 14 (3) a) formulates a general rule that the controller shall provide the data protection notice within a reasonable period after obtaining

[112] Ibid. Page 197.
[113] The EU GDPR: *A Commentary*. Page 444.
[114] Ibid.
[115] Ibid. Page 445.

the personal data, but at the latest within one month, having regard to the specific circumstances under which the personal data are processed. Thus, the controller is more flexible here, as it may need some time to identify and reach the data subject. The controller yet needs to make sure it never exceeds the one-month period.[116] The point b) of this provision indicates that if the personal data are to be used for communication with the data subject, the controller must provide the data protection notice at the latest at the time of the first communication with the data subject. The WP29 points out that if the first communication happens within a month from obtaining the personal data, then the information must be provided no later than at the time of the first communication with the data subject regardless of whether the one-month period from the point of obtaining the personal data has expired or not. If the first communication with the data subject occurs later than one month from obtaining the personal data, then Article 14 (3) a) applies. Pursuant to that, the data protection notice must be delivered to the data subject within one month after the personal data were obtained, i.e. before the planned communication. Finally, Article 14 (3) c) recalls the situation where the data are being disclosed to another recipient. In such a case, the information must be provided no later than at the time of the first disclosure to the recipient. Then, if the disclosure takes place within a month from obtaining the personal data, the information must be provided exactly at the time of that first disclosure, regardless of whether the one-month limit from obtaining the data has expired or not. On the contrary, if the disclosure of the personal data occurs later than one month after obtaining the personal data, then general one-month period again continues to apply, and so the data protection notice must be provided to the data subject at the latest within one month after it was obtained.[117] To sum up, in any case, the maximum time limit within which the controller must provide information pursuant to Article 14 is one month.

Equivalently to Article 13 (3), if the controller intends to further process the personal data, the controller must inform the data subject of this fact and provide other relevant information pursuant to Article 14 (2), all prior to the start of the further processing.

Finally, Article 14 (4) remembers situations when the controller does not have to provide the information stipulated in paragraphs 1 and 2 to data subjects. WP29 points out that these exemptions should be interpreted rather strictly to ensure the coherence with the

[116] Ibid. Page 445.
[117] WP29: Guidelines on transparency. Pages 15-16.

principle of transparency.[118] Similarly to the exemption under the Article 13 (4), the Article 14 (5) a) composes the exemption of providing the information where the data subject already possess it. This covers a situation where the controller that collects the personal data from the data subject provides him or her with the necessary information and then transfers the personal data to another controller. If the information provided by the first controller suffices to fully cover the information obligation of the second controller, the second controller does not have to provide the same information to the data subject. In this case, the second controller has to be able to prove that all the necessary information pursuant to Article 14 had already been provided to the data subject.[119] Another situation where the controller can avoid the information obligation is if the provision of such information is impossible or would involve a disproportionate effort. This is particularly in the case when the processing is being conducted for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. WP29 suggests that the controller carries out the balancing test between the effort that is involved to provide the information to the data subject and the potential impact on the data subject if he or she would not be given the necessary information. Anyway, the controller has to take appropriate measures to protect the data subject's rights, freedoms, and legitimate interests, including making the information publicly available.[120] The controller is also not obliged to provide the data protection notice where obtaining or disclosure of personal data is expressly laid down by Union or Member State law to which the controller is subject, under the condition that the law in question provides appropriate measures to protect the data subject's legitimate interests. This means that Union or Member State law directly addresses the controller, and the obtaining or disclosure of the personal data is mandatory upon the controller. Thereon, the controller must be able to demonstrate the fact that the law in question requires the controller to obtain or disclose the personal data concerned. At the same time, Union or Member State law has to require the adoption of appropriate measures to protect the data subject's legitimate interests, and the controller should ensure compliance with those requirements.[121] According to Nulíček et al., this exception may be used for the purposes of state administration information systems[122]. Finally, the last exemption from the information obligation regards the personal data which

[118] Ibid. Page 28.
[119] The EU GDPR: *A Commentary*. Page 446.
[120] WP29: Guidelines on transparency. Page 31.
[121] Ibid. Page 32.
[122] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 201.

must remain confidential due to an obligation of professional secrecy regulated by Union or Member State law. The controller must prove that this exemption applies to each specific case.[123]

3.3. Relevant case law

3.3.1. C-201/14, Bara[124]

The Romanian court of appeal requested the CJEU to interpret the Data Protection Directive in the matter of information obligation under its Articles 10, 11 and 13. In the original dispute, S. Bara and others brought the action against the Romanian tax authority ("ANAF") and national health insurance authority ("CNAS") in which they challenged the legality of transferring the personal data relating to their tax incomes from ANAF to CNAS because they did not give any consent to it nor were they informed of the same.

The CJEU examined the exemptions to the right to be informed laid down by Article 13 of the DPD. The CJEU noted that the fact that national legislature obliges national public authorities (including ANAF) to transfer the personal data necessary for insurance purposes to health insurance authorities does not exempt them, as the controllers, from their information obligation under the Article 10. Therefore, ANAF was obliged to inform the data subjects of its identity, purposes of the processing and all of the further information necessary to maintain legitimate processing of the personal data, including the information on the recipients or the categories of recipients as well as on the existence of data subject rights. Therefore, the transfer of personal data from ANAF to CNAS was not in accordance with Article 10 of the Data Protection Directive. None of the exemptions laid down by Article 13 were appliable to this situation. The Data Protection Directive states in Article 13 (2) that Member States may restrict the right to be informed by a legislative measure. In this case, the definition of information and conditions for the transfer of personal data were not laid down in a legislative measure, but in the Protocol agreed between ANAF and CNAS which was not set out in an official publication.

Additionally, CNAS was also obliged to provide necessary information to data subjects according to Article 11, mainly on the purposes of processing, categories of personal

[123] WP29: Guidelines on transparency. Page 33.

[124] C-201/14, Smaranda Bara and others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF), ECLI:EU:C:2015:638.

data concerned and the existence of data subject rights. This obligation was not fulfilled either. The exemption in Article 11 (2) was not applicable nor were the general exemptions under Article 13.

For specified reasons, the CJEU held it was necessary to interpret the provisions in question as precluding national provisions which allowed national public authorities to transfer personal data to another national public authorities and their subsequent processing without data subjects having been informed of that transfer and subsequent processing.

3.3.2. C-473/12, IPI[125]

In the case IPI, the CJEU dealt with interpretation of the right to be informed in relation to the investigation by the private detectives working for a professional association of real estate agents ("IPI"). One of IPI's responsibilities was to ensure the proper practice of the profession of estate agents. To perform this duty, IPI was authorised to use the services of private detectives. IPI challenged the work of two estate agents before a national court, claiming that they acted contrary to the rules regulating this profession, and asked the court to order them to cease various estate agency activities. The two estate agents claimed that the evidence on which IPI based its legal action was not obtained lawfully, as they were not informed of the monitoring of their activities.

The national court requested the CJEU to provide a preliminary ruling to interpret Article 13 (1) g) of the Data Protection Directive. The CJEU was specifically asked to answer the question whether that provision allowed Member States to choose whether or not to provide for an exception to the information obligation under Article 11 (1), whether it would be necessary in order to protect the rights and freedoms of others. By the second question, the national court asked whether the professional activities of private detectives authorised to report to the judicial authorities any infringement of the provisions protecting a professional title and organising a profession belong within the exemption under Article 13 (1) (d) and (g) of the Data Protection Directive.

[125] C-473/12, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte, intervening parties: Union professionnelle nationale des détectives privés de Belgique (UPNDP), Association professionnelle des inspecteurs et experts d'assurances ASBL (APIEA), Conseil des ministres. ECLI:EU:C:2013:715.

The CJEU found out that both Articles 10 and 11 were applicable to this case because private detectives may collect personal data either directly from data subjects or from third parties. The CJEU remarked that Article 13 (1) allowed Member States to adopt legislative measures to restrict the scope of the information obligation where such a measure would be necessary for the purposes set out in Article 13 (1) (a) to (g). This, however, was not mandatory, but only an option. Thereon, if a Member State chose to implement the exemption provided for in Article 13 (1) (d), then the professional body concerned and the private detectives performing activities on behalf of that body were not subject to the obligation to inform the data subject provided for in Articles 10 and 11. On the other hand, if the Member State did not provide that exemption, data subjects, in this case the estate agents, must have been informed of the processing of their personal data according to these provisions.

3.3.3. C-40/17, Fashion ID[126]

In this case, the German consumer protection organization (Verbraucherzentrale NRW) filed a lawsuit against Fashion ID, an online fashion shop, in which it challenged the placement of a Facebook "Like" button on the shop's website. Placing the "Like" button on the website of Fashion ID caused that the personal data of the visitor of the website were transmitted to the company Facebook Ireland as a result of that website including such button. This transmission occurred without the visitor being aware of it and regardless of whether he or she was a user of Facebook or has clicked on the "Like" button.

Firstly, the CJEU concluded that Fashion ID is a joint controller together with Facebook Ireland. Then, the CJEU assessed the allocation of the information obligation between these joint controllers. Regarding the definition of a controller, along with the opinion of Advocate General[127], the responsibility of Fashion ID was limited to the operations for which it determined the means and purposes of the processing of the personal data. Thus, Fashion ID was responsible for the collection and transmission of the personal data, however, not for the subsequent processing carried out solely by Facebook.

The CJEU finally ruled that in a situation where there are separate phases of the processing carried out by two joint controllers the duty to inform data subjects of some

[126] C-40/17. Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV. ECLI:EU:C:2019:629
[127] OPINION OF ADVOCATE GENERAL BOBEK, delivered on 19 December 2018, Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

aspects of the processing laid down in Article 10 of the DPD is incumbent on both controllers, but the content of the information that must be provided to the data subject relates only to the operation or the set of operations in respect of which one of the joint controllers actually determines the purposes and means of the processing.

3.4. Conclusion

The right to be informed is a significant data subject right that has been involved in some of the early legal documents dedicated to data protection. Since then, it evolved into the rule ensuring that data subjects are informed of the processing of their personal data by a particular controller and of the key aspects of such processing, most importantly of the identity of the controller, the purposes of the processing, the retention period, the rights of data subjects, etc. The Data Protection Directive as well as the GDPR have divided the right to be informed into two provisions. One applies to a situation where personal data were obtained from the data subject, while the other applies to a situation where personal data were obtained from another source. It was discussed that the right to be informed relates to the principles of fairness and transparency which are an inherent part of the data protection. It is the controller's positive obligation to provide the necessary information in the data protection notice in a clear and concise manner and in an appropriate form to be accessible and understandable by all data subjects. The controller must always be able to prove that the data subject was provided with the necessary information. The affirmative approach of the CJEU that commonly ruled in favour of providing information to data subjects, when it was disputed, contributes to the importance of the role of the right to be informed. By obtaining such information, the data subject is aware of the fact that some of his or her personal data are being processed by the particular controller, including other aspects of the processing, which allows data subjects to observe whether such information seems valid, unconcealed, and true. By obtaining the knowledge of data subject rights, data subject can get familiar with their purposes and may find them beneficial for future use. From my perspective, the right to be informed is an essential element of data protection and can be very practical in finding out any flaws of the processing and in exercising data subject rights.

4. THE RIGHT OF ACCESS TO PERSONAL DATA

The right of access to personal data has been part of data protection since its early beginnings. In a general sense, this right enables an individual to submit a request to a controller, upon which he or she is then able to obtain a confirmation that his or her personal data are being processed by this controller and (or) to obtain several facts about the processing, if the controller satisfies the request. The right of access seems to be powerful in giving data subjects knowledge of the processing of their personal data which can subsequently be used to enforce the protection of these data. However, despite its long existence in data protection law, exercising the right of access in practice might face many difficulties from not being aware of such right through not being able to identify the controller, to unjustifiable refusal the access request. In fact, the percentage of successfully obtained accesses to personal data is still not high enough to proclaim that the right of access represents an instrument largely contributing to the effective protection of personal data. In order to get closer to adequate level of protection of personal data by virtue of the right of access, there are certain components that must work properly. In addition, the aim of this chapter is to scrutinize the development of the right of access including its essence and analyse the remarks from the empirical studies conducted on the exercise of the right of access in practice.

4.1. Legal background of the right of access to personal data

The right of access to personal data is one of the oldest rights that have ever been granted for data subjects. In 1981, The Council of Europe acknowledged the roots of this right in Article 8 b) of the Convention 108 by stating that everyone is allowed to obtain at reasonable intervals and without excessive delay or expense confirmation whether their personal data are being processed as well as communication of personal data in an intelligible form. There were also some references to the right of access in The Council of Europe's Resolutions even before the adoption of the Convention 108. Similarly, the Guidelines adopted by the OECD contained the reference to the right of access, as was already mentioned in Section 1.2 of this thesis. These legal acts, however, did not regulate the right of access to the extent that it could be regarded as an effective tool of protection of personal data, as the current notion of the right of access might be. For example, Article 8 b) of the Convention 108 only allowed data subject to get to know whether his or her personal data are processed

and if so, what are the categories of these personal data[128]. Paragraph 13 of the Guidelines by the OECD encompassed the right of access in the same manner even though it also added the possibility of being given reasons, if the access request was denied, and of being able to challenge such denial. The last sentence of that paragraph also included the possibility to challenge the personal data that were being processed and afterwards to have those data erased, rectified, completed, or amended. This formulation of the right of access is still narrow even though it encompasses some additional features. Interestingly, the Guidelines included the possibility to obtain reasons for denial of the request to obtain information whether there are personal data being processed. The Explanatory Memorandum adds that if it was interpreted broadly, the right to obtain such reasons could be used also for other adverse decisions with the intention to alert the data subject about it and inform him or her of their rights in this matter[129]. Paragraph 13 c) and d) include the right to challenge. According to the Explanatory Memorandum, this right applies to challenges in first instances to data controllers as well as to challenges before courts or other competent public authorities. However, data subjects cannot choose the form of a remedy that they could seek in such challenges. The OECD left this decision upon national laws to determine what kinds of remedies would be available for violations of the rules stipulated by the Guidelines.[130]

Under Union law, the first legal instrument fully dedicated to personal data protection, the Data Protection Directive, incorporated the right of access into its Article 12 (a). According to it, every data subject was guaranteed to obtain from the controller three types of information: (i) a confirmation whether personal data relating to the data subject were being processed, and further details about the processing, including the purposes of the processing, the categories of personal data concerned, the recipients of personal data and categories of recipients of personal data; (ii) a communication of the personal data undergoing processing in an intelligible form and information about the source of such data; and (iii) information about the logic involved in any automatic processing of personal data concerning the data subject at least in the case of the automated decisions[131]. The Data Protection Directive set

[128] However, the Article 8 of the Modernised Convention 108 now represents similar standard of the right of access to personal data as the GDPR.
[129] Annex to the Recommendation of the Council of 23rd September 1980: Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data: Explanatory Memorandum. Available via: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#introduction Retrieved 20.11.2020.
[130] Ibid.
[131] The EU GDPR: *A Commentary*. Page 453.

forth that the right of access could be exercised via usual communication channels, using an intelligible form for communicating the information so it would be understandable by all individuals, and to provide that information without an excessive delay[132]. The problem of the DPD was that it did not prescribe any specific form of the access request, any authentication requirements for data subjects nor the exact time period within which the access request must have been handled by the controller. Not specifying these important aspects of the right of access caused considerable discrepancy in transposition of this provision among the Member States. Such differences may have induced a contradistinctive level of the protection of personal data, letting the exercise of the right of access be more accessible in some Member States than in the others.[133] Article 12 of the Data Protection Directive have been titled "Right of Access". However, the points b) and c) of this article encompassed the right to rectification, erasure or blocking of personal data which could be used by the data subject if the processing did not comply with the provisions of the Data Protection Directive, particularly because the personal data were incomplete or inaccurate. Ausloos and Dewitte suggest that positioning of the right of access together with the right to rectification, erasure or blocking of personal data within the Data Protection Directive is connected to the purpose of the right of access, which is to enable data subjects to feasibly exercise other data subject rights[134].

4.2. The scope of the right of access under Article 15 of the GDPR

The scope of the obligatory information to be provided in order to satisfy the access request has expanded with the adoption of the GDPR. Besides that, the practical application of this right improved as well, since the GDPR includes more precise instruments to ensure a feasible procedure of submitting the access request by a data subject and of responding to the request by a controller.

[132] BIER, CH., KÖMPF, S., BEYERER J. A Study on Corporate Compliance with Transparency Requirements of Data Protection Law. Published in: *Data Protection and Privacy: (In)visibilities and Infrastructures*. Vol. 36. Cham: Springer, 2017, pp. 271-292 ISBN 978-3-319-50796-5. DOI 10.1007/978-3-319-50796-5. Page 285.
[133] The EU GDPR: *A Commentary*. Page 453.
[134] AUSLOOS, J., DEWITTE P. Shattering one-way mirrors - data subject access rights in practice. *International Data Privacy Law*. 2018, *8*(1), 4-28. Page 7.

4.2.1. Confirmation of the processing of personal data

The first component of Article 15 of the GDPR is similar to provisions contained in the previously mentioned legal acts relating to data protection. It is a confirmation whether personal data of a particular data subject are being processed by a particular controller or not. To comply with this requirement, the controller should provide a simple confirmation or a denial of the processing of personal data to the requester.[135] Although it may sound trivial, obtaining the confirmation of whether the processing takes place has a meaningful significance in data protection law. The first step to exercise any of the data subject rights is to have the knowledge of the processing of personal data by the particular controller or processor. Without this knowledge, it is practically impossible for data subjects to exercise these rights and thus enjoy the personal data protection. Thus, the confirmation of the processing can trigger the data subject to exercise his or her other rights or to challenge the legality of the processing before the competent authorities.

4.2.2. Details about the processing and comparison to the right to be informed

If a controller confirms that the processing of personal data is being carried out, then it should also provide some additional details about it. These details demonstrate elemental features of the processing, including the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipients to whom the personal data are disclosed and the period for which the controller intends to store the personal data, or at least the criteria used to determine that period. The controller also has to inform the data subject of the existence of data subject rights, such as the right to rectify or to erase the personal data, the right to restrict the processing, including the right to lodge a complaint with a supervisory authority. If the personal data were not collected from the data subject, the controller has to inform the data subject of their source. In the case of automated decisions, the logic involved in any automated processing of data needs to be provided to the data subject too. In addition, when the personal data are transferred to a third country or to an international organisation, the controller has to inform the data subject of such fact, including the appropriate safeguards adopted because of the transfer.[136]

[135] The EU GDPR: *A Commentary*. Page 462.
[136] The Article 15 (1), (2) of the GDPR.

Seemingly, there is an overlap with the information that must be given to data subjects in the data protection notice pursuant to Articles 13 and 14 of the GDPR, which was discussed in Chapter 3. The right to be informed is based on providing information on the controller and on the processing to the data subject before the processing, at its beginning, or within a month before the beginning of the processing. It might seem pointless to seek the same information through the right of access after that information had already been provided. However, the right to be informed and the right of access slightly differ in their purpose. As explained in the Oxford Commentary, the information related to the right of access has to be "*more precise and granular*", accommodating the specific aspects of the particular data subject who requests the access, and the aspects regarding the personal data relating to him or her. On the contrary, information under Articles 13 and 14 usually covers processing of personal data relating to multiple data subjects and so serves as a general information. Also, the data protection notice is compulsory for the controller to provide, while the information pursuant to Article 15 must be provided only as a reaction to the request made by the controller. In other words, to ensure the right to be informed is accommodated, the controller must proactively inform data subjects of the existence and details of the processing, whereas to ensure the right of access is accommodated, it is the data subject who must actively exercise that right.[137] In my opinion, these two separate rights correlate to the extent that they both ensure that data subjects have essential information about the processing of their data. Although they pertain to different stages of the processing, a certain interaction between these two rights can be seen in analysing whether the processing is being done in compliance with data protection rules. Firstly, the data subject must be informed that there is some processing being conducted by the particular controller and after being informed of such fact, he or she may exercise the right of access to personal data, for example in order to compare whether the information on the controller or on the specific aspects of the processing is still accurate and up to date. Summing up, both the right to be informed and the right of access to personal data secure the provision of important details about the processing and so they both play a significant role in data protection.

[137] The EU GDPR: *A Commentary*. Page 462.

4.2.3. Copy of personal data

Article 15 (3) of the GDPR introduced the possibility to obtain a copy of the personal data that are being processed. This has created a significant shift in the field of data protection since the access to personal data is now not limited to a provision of a simple summary of the personal data, but it means that data subjects can obtain a more sophisticated ensemble of their personal data.[138] Although it is a very advantageous novelty in data protection law, it could be defined more precisely. The GDPR does not define the term "copy" or give any guidance on how to interpret it, neither there are any instructions for controllers on how to meet the requirement for providing the copy of personal data. This might induce considerable inconvenience in practice, as different entities might interpret it diversely. The term itself might evoke an assumption that controllers have to disclose copies of their original documents, where some of personal data of a particular data subject appear. On the other hand, it might mean that controllers can only provide copies of those parts of documents, where personal data appear. Perhaps, controllers may try to avoid this ambiguity caused by not giving any guidance on the interpretation of the term "copy" by continuing to provide only a summary of personal data as it was before the adoption of the GDPR. Article 15 (4) states that obtaining the copy of personal data shall not affect the rights and freedoms of others in a negative way. Recital 63 states that paragraph 4 mainly refers to trade secrets, intellectual property rights, in particular the copyright protecting the software. Similar protection should be accorded to personal data of third persons. This collision typically appears in the case of providing a recording from the CCTV cameras. Nevertheless, such restrictions should be interpreted rather strictly to avoid a refusal to provide all information to the data subject.[139]

In the case *Nowak*[140], the CJEU examined a situation where a trainee accountant Mr. Nowak wanted to access his exam script of the second level examinations set by the Institute of Chartered Accountants of Ireland by using the right of access to personal data under Article 12 a) of the Data Protection Directive. His request was declined as was the subsequent complaint he made to the Data Protection Commissioner. After the proceedings on the national level, the case was brought to the CJEU with the question whether the written

[138] The EU GDPR: *A Commentary*. Page 464.
[139] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 205-206.
[140] C-434/16 Peter Nowak v Data Protection Commissioner. ECLI:EU:C:2017:994

answers submitted by a candidate at a professional examination and examiner's comments to the candidate's answers constitute personal data–within the meaning of Article 2 a) of the DPD. The CJEU considered that the exam scripts normally include the name of the candidate or his or her identification number and that the written answers which are part of the examination reflect the candidate's knowledge in a given field, his intellect, thought processes and handwriting. Thus, the CJEU has ruled that "*written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data*" within the meaning of Article 2 a) of the DPD. The controller then has to comply with the principles and safeguards that must be observed in the area of personal data protection, and with the rights of access, rectification and objection of personal data relating to a particular data subject. Upon that, the CJEU has ruled that the rights of access and rectification may also be exercised towards the written answers submitted by the candidate at the professional examination and to any comments made by the examiner with respect to those answers[141]. The CJEU also emphasized that the right of access is necessary to enable the data subject to acquire the rectification, erasure or blocking of his or her personal data by the data controller[142].

The Data Protection Directive did not impose the obligation of providing the copy of personal data to data subjects as the GDPR does. The CJEU referred to Article 15 (4) of the GDPR in the judgment, however, it did not explicitly mention the form of the copy which should have been provided to the data subject. On the grounds of this judgment, I assume that in this case the data subject should have been able to obtain the copy of the original exam script together with the copy of the examiner's evaluation. Any other means of providing him with the written answers and the evaluation would not be as effective as providing him with the copy of the original exam script. If it was likewise performed in the case of Mr Nowak, it would then mean that the "copy" that is referred to in Article 15 (3), (4) of the GDPR may have different forms and it is not limited to a simple summary of personal data, but that it is rather seen as an original document that includes personal data as exam scripts do.

In another case, the Consultation Department of the Office for Personal Data Protection of the Czech Republic (hereinafter "the Office") dealt with the question whether an employer as a controller is obliged to provide all of the employment contracts and their amendments to a former employee who has asked for copies of them in the submitted access

[141] Ibid. Paragraph 51 of the judgment.
[142] Ibid. Paragraph 57 of the judgment.

request. The employer was not willing to provide them, arguing that the contracts also included provisions where the personal data of the former employee were not mentioned. The Office tackled the question whether controllers must on the grounds of an access request provide copies of the original documents containing the personal data of the data subject, or only the copies of those parts where the personal data are explicitly mentioned. The Office found that the contracts were part of a filing system kept on employees by the employer. Whereas the GDPR applies to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, the Office held an opinion that all the provisions in the employment contracts which are part of a filing system might relate to the particular data subject and therefore all of these provisions must be accessible by virtue of the right of access. Thus, the data subject had the right to obtain from the employer the copies of the employment contracts and their amendments in their entirety. Nevertheless, assuming that the employee was probably given his or her duplicate of the employment contract at the beginning of the employment, the employer might have charged a reasonable fee for administrative costs according to Article 15 (3) of the GDPR.[143]

On the other hand, Pokorná and Dvořáková assess that the approach that a provision of the copy of personal data under Article 15 (3) should be interpreted as provision of an original document composed of personal data may lead to problems in practice, e.g. when data are processed by informative systems.[144] I personally lean toward the opinion of the Office because a document like a contract should be considered in its entirety, as all of its provisions compose a whole unit and cannot be divided into single provisions. Also, it is in conformity with the principle of transparency that the controller should provide the copy of the whole document. The data subject may then make sure what parts of the document include his or her personal data. The argument that the provision of the copy of an original document composed of personal data can be problematic in practice is indeed right when controllers process a large amount of personal data in numerous documents. However, controllers should attempt to fully satisfy the access requests of data subjects and facilitate their right of access to personal data. Anyway, in the case of manifestly unfounded and excessive requests, the controller may either charge fees for administrative costs or refuse to act as was already mentioned in Section

[143] Personal consultation with the head of the Consultation Department of the Office for Personal Data Protection, Mgr. Ladislav Hejlík, on 26.10.2020.

[144] POKORNÁ, A., DVOŘÁKOVÁ H. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020. ISBN 978-80-7598-309-1. Page 181.

2.2. Such refusal, however, should be considered on a case-by-case basis and not abused only because of a massive processing of personal data.

What is more, the Oxford Commentary triggers the issue, whether providing the copy is necessary in responding to every access request since Article 15 does not explicitly require that. The authors of the commentary suggest that in order to make sure that the data subject obtains the copy of his or her personal data, it is better to expressly request it, otherwise it may be left on the controller to decide what form of access to personal data would be used.[145]

4.3. Exercising the right of access to personal data under the GDPR

4.3.1. Satisfying the access request

Whenever a controller receives a request the subject of which is to access one's personal data, the controller is required to respond within one month of receipt of the request according to Article 12 (3) of the GDPR. In the event of receiving complex requests or a large number of requests, the controller may extend this period by two additional months. This decision must always be communicated to the data subject. Similarly, when the controller decides not to satisfy the access request, it should not be left without any action. It is necessary to inform the data subject of the intention not to satisfy the request and to provide specific reasons for it. Additionally, even when the controller decides not to take any action towards the access request, the controller is required to inform the data subject of the possibility of logging a complaint with a supervisory authority and seeking a judicial remedy. Pursuant to Article 12 (4) of the GDPR this action must also be taken within one month.

If the controller processes an enormous amount of personal data relating to the requesting data subject, the controller is allowed to ask the data subject to specify the access request to personal data he or she specifically needs.[146] This although does not mean to ask the data subject to narrow the request. If the data subject does not specify the personal data he or she particularly wants to obtain, the controller must provide the corresponding data in a full scope, i.e. every relevant type of information stipulated in Article 15 of the GDPR. It is

[145] The EU GDPR: *A Commentary*. Page 464.
[146] Recital 63 of the GDPR.

unacceptable to deny or restrict the right of access just because the controller processes large amounts of personal data of the data subject.[147]

The Consultation Department of the Office has also dealt with a question from the controller who had received an access request. The requesting data subject requested the access to all personal data relating to her that the controller possessed and demanded a copy of such data. The controller asked the Office whether it was necessary to provide a copy of every document which contained the name of the data subject, pointing out that some information on that data subject might have appeared in thousands of files and in a numerous e-mail correspondence. The Office has based its opinion on the Recital 63 which emphasises that it is not allowed to deny or restrict the right of access for the reason of processing large amounts of personal data of the requesting data subject. The Office has also noted that if the data subject does not specify the request, the controller must provide all of the personal data relating to that data subject that have been processed. However, the Office has stated that mentioning only a name of a natural person in an e-mail correspondence or other similar communication channel, when that natural person is not the sender nor the addressee, does not fall within the material scope of the GDPR set out in Article 2 (1) and so the controller does not necessarily have to provide the access to such information. On the contrary, the Office has referred to Article 12 (5) b) of the GDOR and has held that requesting the access to the information which the data subject is undoubtedly familiar with, e.g. regarding the performance of his or her employment duties, may constitute a manifestly unfounded request that may lead to the refusal of the request to the extent of the familiar information. With regard to the context of this specific access request, the Office has found a possibility that there might have been a malicious intention of the data subject behind it. However, the Office is not competent to assess the nature of intentions, but if the malicious intention of the data subject was proven, it would lead to the rejection of the access request on the grounds of Article 12 (5) b) of the GDPR, if the request was regarded as manifestly unfounded.[148]

Similar opinion on the interpretation of "manifestly unfounded request" has been held by the ICO by stating that a request could be manifestly unfounded if it was made to harass and cause disruption to the controller, for instance by consisting of unsubstantiated accusations against the controller or its employees. In addition, the ICO considers the request

[147] Ibid.

[148] Personal consultation with the head of the Consultation Department of the Office for Personal Data Protection, Mgr. Ladislav Hejlík, on 26.10.2020.

manifestly unfounded also in the situation where the individual clearly has no intention to exercise the right of access to personal data because he or she is willing to withdraw the request in return for some form of benefit from the controller. Although, the ICO has noted that the use of aggressive or inappropriate language does not solely constitute a manifestly unfounded request.[149] Since there is no exact guidance on what falls under the term of "manifestly unfounded", every request has to be considered individually, in its own context.

4.3.2. Identity verification

While evaluating a request for the access to personal data by a controller, an uncertainty about the identity of the requester may occur, particularly in the context of online services and online identifiers.[150] In this event, the controller may demand an additional information from the data subject to verify his or her identity in accordance with Article 12 (6) of the GDPR before revealing the personal data to the requester.[151] Obviously, the controller may request only information that is necessary to confirm whether the requester and the data subject whose personal data are processed by the particular controller is the same person. For verification of the identity, many controllers require a copy of an identification document or a guaranteed electronic signature[152]. As a substitute, controllers may ask the requester certain questions on the basis of which they may decide whether the requester is the data subject. Until the controller receives the additional information, the one-month period for responding to the access request is stopped and begins again after the controller is able to verify the identity of the requester.[153] The identity verification serves as a protection against revelation of personal data to an unauthorised person. Making personal data available to a person other than the data subject may constitute *"an unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*, defined in Article 4 (12) of the

[149] Guide to the General Data Protection Regulation (GDPR)/Right of access/When can we refuse to comply with a request? Available via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/when-can-we-refuse-to-comply-with-a-request/ Retrieved 02.11.2020.

[150] Recital 64 to the GDPR.

[151] Applies to all requests regarding the rights of data subjects under the GDPR.

[152] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 185.

[153] ICO UK Guide to the General Data Protection Regulation / Right of access. Available via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ Retrieved 23.10.2020

GDPR as the "personal data breach". Such disclosure may lead to negative consequences for both the data subject and the controller. Therefore, I presume that verifying the identity of the person who seeks the access to personal data should be considered the controller's duty to preserve an adequate level of protection of personal data that the controller processes. Also, it should be regarded as one of appropriate technical and organisational measures that the controller is obliged to implement pursuant to Article 24 (1) of the GDPR. Finally, if the controller is unable to identify the data subject even after obtaining the additional information for the purposes of verification of his or her identity, the controller must inform the requester of this fact and deny the access to personal data.[154]

Recital 64 further emphasises to pay a special attention to online services and online identifiers. Regularly, when a person visits a webpage, the provider of this webpage might collect the visitor's IP address. If the visitor, i.e. the data subject, then submits the access request, the controller may struggle to verify his or her identity if the IP address is the only or one of a few pieces of information that the controller has about the data subject. The Office for Personal Data Protection has dealt with the similar case where the controller (a website provider) knew only the IP address and the telephone number of the data subject. When the requester submitted the access request through the e-mail, the controller could not be sure if the requester was the data subject. The Office advised the controller to ask the requester to provide the same information that the controller has already had. After that, the controller should have compared whether the information that the requester provided corresponded to the personal data of the data subject that the controller was processing.[155] Therefore, to verify the identity of the requester should not always mean to demand additional personal information. When possible, it is better to compare the accuracy of the information that the data subject can provide with the information that the controller already has. This would preserve the principle of data minimisation which is stipulated by Article 5 (1) c) of the GDPR because the controller would not obtain any other unnecessary information. In addition, verification of the identity does not mean the controller may collect personal data solely for the purpose of being able to react to potential access requests[156].

[154] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 186.
[155] Author's own experience acquired during the internship at The Office for Personal Data Protection.
[156] Recital 64 to the GDPR.

Recital 63 provides a good example of a measure that would ensure that personal data are only disclosed to the data subject they relate to. According to it, the controller should be able to provide a remote access to a secure system which gives the data subject a direct access to his or her personal data. This secure system lies on the idea of providing personal data only relating to the specific data subject. Alongside, the data subject is allowed to correct his or her personal data that are being processed. Using such system should not affect the rights or freedoms of others, including trade secrets or intellectual property rights. Since recitals are not obligatory part of the GDPR, this should be considered only a recommendation for controllers if they want to adopt a useful instrument for satisfying access requests.[157]

4.4. Relevant Case law

4.4.1. C-553/07 - Rijkeboer[158]

In the original case, Mr. Rijkeboer requested the College van burgemeester en wethouders van Rotterdam (hereinafter the "Dutch local authority") to provide him with the access to his personal data, in particular the information on the disclosure of his personal data to third parties during the previous two years. By submitting the access request, he was mainly seeking the identity of the third parties and the content of information that was disclosed to them. The request was satisfied only partially, as the Dutch local authority provided the information that related only to the period of one year before the request was made. In the following legal dispute, the Dutch court asked the CJEU a preliminary question whether the right of access to information on the recipients or categories of recipient of personal data regarding the data subject and on the content of the personal data communicated under Article 12 (a) of the Data Protection Directive may be limited to a period of one year preceding the request to access those personal data.

The Data Protection Directive did not set any time limits for the exercise of the right of access to personal data nor for the time period of the data that should be provided by the controller upon the access request. In order to assess the scope of the right of access, the CJEU divided the personal data in question into two categories. The first category concerned

[157] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3. Page 203.

[158] C-556/07, College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer, ECLI:EU:C:2009:293

the personal data kept by the local authority relating to the particular data subject, such as name and address. Such data could be labelled as the basic data and were stored for a long time. However, the second category of personal data in question concerned the information on the recipients or categories of recipient to whom the basic data were disclosed and information on the content of the basic data. In accordance with the Dutch legislation, such information could be stored for only one year. None of the provisions of the Data Protection Directive specified the storage period of the personal data of the second category and therefore Member States had a certain range of autonomy in this field. The CJEU although stressed that such autonomy did not give Member States an unlimited independence. In the light of that, it was possible to set an exact time limit for the exercise of the right of access to information on the recipients or categories of recipient of personal data and on the content of such personal data, but while doing so, it was necessary to take into account the purpose of the right of access to personal data, i.e. to enable data subjects to exercise the other rights. By those other rights, the CJEU mainly meant the right to object to the processing, the right to rectify or to erase the personal data and the right to file an action when the data subject suffers damage.[159]

The CJEU finally held that for the purposes of exercising the other data subject rights, the right of access had to relate to the past. According to the CJEU, it was a responsibility of a Member State to ensure a fair balance between the data subject's interest in the data protection and the protection of privacy on the one hand, and on the other, the burden which the obligation to store the information on recipients or categories of recipient of personal data and on the content of personal data disclosed to those recipients, represents for the controller.[160]

While the Data Protection Directive was in force, Member States had more independence in defining their data protection rules. Netherlands did not act contrary to the DPD when it set out the storage period for some categories of personal data. However, it was done without considering the purpose of the right of access. Consequently, such limitation caused an interference with the data subject rights because after the expiration of the stipulated storage period it was impossible to exercise them. This issue is now resolved, as the GDPR is directly applicable in Member States and so there is no space for Member States to set out their own rules.

[159] Ibid. Paragraphs 42-52 of the judgment.
[160] Ibid. Paragraph 70 of the judgment.

4.4.2. C-141/12, C-372/12 – YS and others[161]

In these joined cases, the CJEU dealt with the preliminary question relating to Article 12 (a) of the Data Protection Directive, submitted by the Dutch court in context of two national disputes between the Ministry for Immigration, Integration and Asylum and asylum or residence permit seekers.

The asylum or residence permit seekers requested an access to the documents, executed by the Ministry for Immigration, Integration and Asylum before the final decision on the asylum or residence permit requests was made. The purpose of those documents was to explain the reasons for a draft decision made by a case officer which was given to a reviser to sign. Such documents contained a legal analysis of the cases and represented a part of the preparatory process, but not of the final decisions on the asylum or residence permit. The requests for access to the aforementioned documents were refused.

The CJEU confronted a problem whether a data subject is entitled to access the information concerning him or her included in the aforementioned documents, and if so, whether satisfying such access request requires the provision of a copy of those documents, or whether a complete and intelligible summary of the information contained in the documents would be sufficient. The CJEU recalled the purpose of the Data Protection Directive, which is to protect the fundamental rights and freedoms of individuals, particularly their privacy in relation to the protection of their personal data. Data protection law in general presumes that the data subject is entitled to scrutinize the accuracy of his or her personal data stored by the controller and the legality of the processing. For such scrutiny, it is necessary to first exercise the right of access to personal data, so the data subject knows what sorts of information the controller possesses. The CJEU distinguished the right of access to personal data from the right to access the information, noting that the former could be used for obtaining the information concerning the data subject's asylum or residence permit request, however, not for obtaining the legal analysis, as it did not constitute the personal data, despite both being part of the same document. The latter then could mean the access to the documents as such.[162]

In the matter of obtaining a copy, the CJEU has held that it is up to Member States to determine the specific tangible form the response to the access request should have. In these

[161] Cases C-141/12, C-372/12. YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel (C-372/12) v M, S. ECLI:EU:C:2014:2081

[162] Ibid. Paragraph 48 of the judgment.

particular cases, the CJEU allowed two forms of access to personal data. Either a copy or an original document in which information other than the data subject's personal data were erased. Alternatively, a full summary of personal data in an intelligible form which allows the data subject to check the accuracy of those data and whether the processing is in compliance with the Data Protection Directive.[163]

Obtaining the copy of personal data was also discussed in Section 4.2.3. of this master's thesis. In the case YS and others, the CJEU has held an opinion that a copy of an original document where parts that do not include the personal data of the requesting data subject were erased would be an appropriate option of how to provide the personal data upon the access request. As was mentioned in Section 4.2.3., The Office of Personal Data Protection has held an opinion that the data subject can access a document in its entirety. However, it is important to mention that the Office has dealt with the case of the employment contract where the data subject had probably received a copy of such contract before he or she submitted the access request. Therefore, none of the confidential information would be disclosed to him or her in that case. On the contrary, in the cases like YS and others, some parts of the document that contained personal data cannot be disclosed to individuals because of their confidentiality or protection of other important interests. Therefore, in some situations, data subjects might obtain a copy of the whole document in which their personal data appear, while in other cases they have to accept the disclosure of only those parts of the document where their personal data are explicitly mentioned. Not being able to verify whether the parts that were not disclosed contain any other information concerning the data subject can be considered detrimental to the data subject. However, it is necessary to analyse every access request as an independent case and carefully decide what personal data should or should not be disclosed while striving to fully satisfy the access request.

4.5. Analysis of the right of access to personal data and its exercise in practice

For the purposes of discovering how important the role of the right of access is within data protection law, the usage of this right must by analysed. Firstly, it is important to scrutinize the theoretical aspects of the usage of the right of access, especially to what extent this right is accessible to natural persons. Secondly, it needs to be discussed what impact the

[163] Ibid. Paragraphs 58–60 of the judgment.

exercise of the right of access might have on the protection of personal data of individuals, including its advantages and disadvantages. To successfully analyse the role of the right of access, the observation of its practical aspects cannot be omitted. For this reason, the aim of this chapter is to examine different studies conducted to determine how much the right of access is used by data subjects and satisfied by controllers, including any possible issues that might occur in exercising such right. After analysing the mentioned aspects, it should be possible to evaluate the involvement of the right of access to personal data within data protection law.

4.5.1. The availability of the right of access

The wording of the first sentence of Article 15 (1) of the GDPR suggests that every data subject can exercise the right of access to personal data. Then, on the contrary, no one else can exercise this right but the data subject. This is also proven by the fact that revealing personal data to an incorrect person might constitute an infringement of the personal data protection rules as was already mentioned before. However, a controller may find out that it does not process any no personal data of that requester, and so the response to the access request would be negative in such case. This leads to a conclusion that if the requester could not be identified by the controller, he or she would not fulfil a definition of the data subject under Article 4 (1) of the GDPR. This is, however, ascertained after the controller's evaluation of the request, verification of the requester's identity and other operations necessary for determining whether the personal data of the requester are being processed by the controller. In this sense, every natural person who has a reasonable belief that his or her personal data are being processed by a particular controller may submit an access request to the controller on the grounds of Article 15.

The GDPR applies to the processing of personal data by a controller or a processor established in the Union, regardless of whether the processing takes place in the Union or not and on the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing relates to the offering of goods or services to data subjects in the Union or the monitoring of data subjects' behaviour which takes place within the Union. As a result, the exercise of the right of access to personal data is available to everyone who believes his or her personal data are undergoing processing under these conditions.

The GDPR does not set any specific conditions for the exercise of the right of access to personal data. Based on general requirements for the exercise of data subject rights under Article 12 (5), submitting the access request must be free of charge. As was discussed before, the controller may charge a reasonable fee where requests from the data subject are manifestly unfounded or excessive. There is no specific form to submit the request required by the GDPR. The Oxford Commentary suggests that the data subject can exercise the right of access by submitting a request or by asking for the access to his or her personal data[164]. The data subject may submit the access request by e-mail or by regular mail, ask for his or her personal data via phone call or even in-person. These ways of exercising the right of access are further discussed in Section 4.5.3. of this thesis. Anyway, in order to exercise the right of access, data subjects should not be facing any difficulties. As the Recital 63 states, data subjects should be able to exercise this right *"easily and at reasonable intervals".* This probably means the controller's obligation to facilitate the data subject rights and to respond to requests made by data subjects within a monthly period after obtaining the request[165].

Summing up, it appears to be feasible for natural persons to submit the access request upon which they seek the information whether the processing of their personal data is being conducted by the particular controller and (or) some details about the processing. If the situation fulfils the material and territorial scope of the GDPR, the controller must deal with the request and act towards satisfying it. The controller who receives the access request should make sure whether the requester is the data subject and if so, provide him or her with the desired information if possible free of charge and within one month after obtaining such request.

4.5.2. The effect of the right of access to personal data

By receiving a response to the access request from a controller, a data subject obtains a confirmation whether his or her personal data are being processed, including other important information concerning the processing. Based on this response, the data subject can find out what information concerning him or her is held by the controller. For instance, when Maximilan Schrems[166] filed the access request to Facebook, he received an enormous PDF file full of information on his Facebook user account. The file contained massive amount of

[164] The EU GDPR: *A Commentary*. Page 462
[165] Article 12 (2), (3) of the GDPR
[166] C-362/14 Maximillian Schrems v Data Protection Commissioner. ECLI:EU:C:2015:650

different information concerning Shrems' friends on Facebook, the people he unfriended, every event he responded to, his private messages including some sensitive information, and even the data that had been erased.[167] Thanks to this disclosure, Schrems was then able to file a complaint with the Data Protection Commissioner because he was aware of which of his personal data Facebook possessed and how it fulfilled their obligations resulting from the principle of transparency. As a result of the mentioned complaint, Schrems challenged transfers of personal data to the United States on the grounds of revelations made by Edward Snowden.[168] It eventually resulted in the proceedings before the CJEU and became one of the most medialized cases where Facebook has been involved. The first step in this procedure where Schrems fights against mass surveillance carried out by Facebook and against transfers of personal data to a country where the level of protection of personal data is lower than in the EU was actually the access request. Obtaining the information on the purposes of the processing, the categories of personal data that are being processed, the recipients of personal data, the storage period, etc. might be helpful in finding out that some conditions under which the processing is being conducted are not in accordance with data protection law. It might be, for example, inaccuracy of the personal data, unlawful disclosure to recipients, or too long storage period. In such cases, there are other data subject rights that can be exercised in order to correct such errors of the processing, such as the right to rectify the inaccurate data, complain about unlawful disclosure before a Supervisory Authority, or demand erasure of the personal data that are no longer necessary to be stored by the controller. Accordingly, the right of access to personal data composes the first necessary step towards the exercise of other data subject rights. It almost seems impossible to achieve the erasure or rectification of personal data, or to object to the processing without the exact knowledge of essential information about the processing of personal data conducted by the controller or processor. In this sense, the right of access is sometimes referred to as a precondition for the exercise of

[167] For instance: Max Schrems: The Austrian Thorn In Facebook's Side, available via: https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/?sh=3eb66e3e7b0b; or Max Schrems: the man who took on Facebook – and won, available via: https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544. Both retrieved 6.11.2020.

[168] Edward Snowden, a former Central Intelligence Agency (CIA) employee in June 2013 revealed documents about numerous global surveillance programs run by the United States' National Security Agency (NSA) to several journalists and press. In the context of these revelations, he has been charged with several felonies as well as sued in civil proceedings. He has been staying in Russia since 2013.

other data subject rights.[169] The CJEU has confirmed this role of the right of access in the cases *Nowak*[170] and *Rijkeboer*[171].

In addition, WP29 has acknowledged the link between the right of access to personal data and the right of data portability by stating that "*data portability complements the right of access*". This is explained as the right to data portability which enables the data subject to receive his or her personal data that are being processed and to store them for further personal use. It does not necessarily require transferring the data to another data controller as it may seem.[172] In this regard, obtaining the access to data is a part of the exercise of the right to data portability which, however, has a different purpose than the right of access does.

Returning to Schrems case, it is appropriate to highlight that by obtaining the access to his personal data, he did not only discover the enormous amount of information that Facebook has held on him. He was also able to review how Facebook has complied with the European data protection standards. His findings became a trigger for the following complaint and further proceedings before the CJEU. From this point of view, the right of access does not only act as the first step towards or prerequisite for the exercise of other data subject rights, but it also serves to assess the controller's compliance with data protection rules.[173] Ausloos et al. state that it can complement the monitoring of the compliance with the GDPR carried out by Supervisory Authorities[174]. In connection with that, the right of access is also a useful tool for monitoring conformity with the general principles governing the processing of personal data set out in Article 5 of the GDPR, as well as assessing whether the processing is lawful according to Article 6 of the GDPR and its other provisions. According to the Recital 63 every data subject should be able to exercise the right of access so that he or she could be aware of, and verify, the lawfulness of the processing.

The conformity with the rules stipulated in the GDPR is a reflection of the principles of transparency, fairness, and accountability that were discussed in Section 2.2. of this thesis.

---

[169] AUSLOOS, J., DEWITTE P. Shattering one-way mirrors - data subject access rights in practice. *International Data Privacy Law*. 2018, *8*(1), 4-28. Page 7.
[170] C-434/16, Nowak. Paragraph 57 of the judgment.
[171] C-553/07, Rijkeboer. Paragraphs 51-52 of the judgment.
[172] Article 29 Working Party: Guidelines on the right to data portability. Page 4-5.
[173] AUSLOOS, J., DEWITTE P. Shattering one-way mirrors - data subject access rights in practice. *International Data Privacy Law*. 2018, *8*(1), 4-28. Page 8.
[174] AUSLOOS, J., VEALE M., MAHIEU R. Getting Data Subject Rights Right: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2019, *10*(3), 283-309. Page 285.

Based on what was already mentioned, the right of access may be considered the way of checking the compliance with those principles since it gives the data subject a picture of the details of the processing. The response to the access request shows how the controller communicates with the data subject, i.e. how easy it might be to understand the information, whether the response is done by using clear and plain language or it is not likely to be understood by an average data subject at all. The form of the response should be accessible and not difficult for data subjects to navigate, as analysed by Ausloos et al. They point out that many controllers provide a copy of personal data in screenshots and PDF formats, which might not be convenient for the average data subject to orientate in.[175] The response to the access request may reflect whether there was any important information concealed at the beginning of the processing when the controller has the information obligation under Articles 13 and 14 of the GDPR. According to the Oxford Commentary, such response composes a deeper and more precise layer of information than what the controller discloses in the data protection notice[176]. In addition, the data subject may find useful to compare the information from the data protection notice which he or she presumably obtained at the beginning of the processing with the information he or she obtained as the response to the access request. For instance, the data subject can check if the recipients of personal data remained unchanged or whether the controller uses the data for the same purposes that they were collected for. The data subject may also control whether the storage period is adequate for the purposes of the processing of personal data. The accuracy of such information indicates how the controller complies with data protection rules since an integral part of the data protection is that the processing is conducted in the light of the principles of fairness, transparency, and accountability and every change in the conditions of the processing should be communicated to the data subject. Overall, it is undisputable that the quality of the protection of personal data increases with the possibility of verifying the adherence of such principles and of data protection rules in general.

Summing up, the role of the right of access to personal data is mainly, but not exclusively, to serve as a precondition for the exercise of other data subject rights, to check how the controller adheres to its obligations imposed by data protection law and to observe the compliance with the principles of fairness, transparency, and accountability in the

[175] Ibid. Page 286-288.
[176] The EU GDPR: *A Commentary*. Page 452.

procedure of the processing of personal data. By all of these useful features, the right of access contributes to the effective protection of personal data.

By all means, data subjects may exercise the right of access solely for the purposes of ascertaining whether there is a processing taking place. Or just because they want to learn other information listed in Article 15, e.g. the length of the storage period, the recipients of personal data, etc. Nevertheless, if the data subject aims to proceed with enforcing his or her data protection rights, he or she may file a request for rectification of the personal data if they are not accurate or up to date[177], or to ask for the erasure of their data if any of the reasons specified in Article 17 (1) of the GDPR apply. Another option is to object to the processing when it is based on point (e) or (f) of Article 6 (1) of the GDPR or when personal data are processed for direct marketing purposes.[178] In the event of violation of rights or obligations laid down by the GDPR, the data subject might exercise the right to lodge a complaint with a supervisory authority[179], possibly also the right to seek an effective judicial remedy.[180] In *Rijkeboer*, the CJEU has correspondingly concluded that the right of access is necessary in a situation where the processing does not comply with the provisions of the Data Protection Directive to enable the data subject to request the controller to rectify or erase the processed data, to object to the processing or to initiate legal proceedings and obtain compensation for the damage suffered.[181]

4.5.3. The exercise of the right of access in practice

Despite its effective potential to enhance the protection of personal data, the right of access seems to be underused in practice. Such underuse presumptively results from the lack of awareness of this right and generally of data protection laws both on the controllers' and data subjects' side. In order to scrutinise the usage of the right of access in practice, this master's thesis examines three empirical studies conducted on the usage of the right of access and describes my own experience with filing the access request.

[177] Article 16 of the GDPR.
[178] Article 21 of the GDPR.
[179] Article 77 of the GDPR.
[180] Articles 78, 79 of the GDPR.
[181] C-553/07, Rijkeboer. Paragraphs 51- 54 of the judgment.

The Ausloos's and Dewitte's empirical study[182] tackled the accommodation of the right of access to personal data by approaching 66 service providers from various sectors across the EU to whom the access requests were submitted.

Firstly, the study attempted to identify and locate each of the service providers, i.e. controllers, and examine their privacy policies. The outcome showed that the vast majority of these controllers could be identified easily, by visiting their websites, where the controllers alongside disclosed their privacy policies. However, in 31% of the cases it was found difficult to identify the controller and to detect its privacy policy, mostly because of the unsatisfactory or problematical website design. It is important to mention that only a half of the detected privacy policies were considered satisfying. Those were the ones that were intelligibly enumerating the categories of personal data that were to be processed by the particular controller, their source, purposes of the processing, lawful grounds of the processing and third parties to whom personal data were to be disclosed.[183] Moreover, Ausloos and Dewitte note that almost all of the detected privacy policies were lacking some of the required information that has to be provided to data subjects prior to or at the beginning of the processing as the data protection notice. They also emphasize that adequate location and reading of privacy policy is necessary in "*data subjects' informational empowerment.*"[184] In other words, data subjects should be able to reach the controller's privacy policy easily and understand its provisions correctly, without any doubts in its meaning.

Secondly, the study assessed the ability of data subjects to exercise the right of access to personal data. The researchers ascertained that only 66% of the investigated controllers included clear instructions on how to exercise this right in their privacy policies.[185] A certain number of the controllers completely ignored the requests, which is why they were contacted multiple times. Unfortunately, several controllers did not even understand what the subject of the access request was, as they were not aware of the right of access at all. Thus, in those cases, the additional explanation of the context of the request was necessary. The researchers found only 22% of the responses to the access requests satisfactory. In the rest of the cases, the controllers lacked the awareness of the right of access, were reluctant to provide the requested information or took long time to answer, while 26% of the requests were not

[182] AUSLOOS, J., DEWITTE P. Shattering one-way mirrors - data subject access rights in practice. *International Data Privacy Law*. 2018, *8*(1), 4-28. Page 9.
[183] Ibid. Page 10.
[184] Ibid. Page 11.
[185] Ibid. Page 12.

answered at all. Many of the controllers also lacked proper organization, which is essential to provide the requested personal data.[186] In some instances, the researchers were encountered with unpleasant reactions to the access request such as suspicion, irritation, or bad faith.[187] The overall results from this empirical study confirm the assumptions that the right of access is generally underused and not adequately accommodated. It is mainly because of a poor understanding of data protection law and data subject rights, the reluctance to satisfy the access requests or insufficient organization measures to provide the requested personal data.[188]

The second empirical study[189] on the exercise of the right of access was conducted across ten European countries, selected to represent a good geographical and cultural variety. Equivalently to the first study, this one also consisted of two parts. The first part was dedicated to locating data controllers and assessing their privacy policy, and the second one to submitting the access request to them.[190]

In order to locate the controllers, researchers' main method was to do so by visiting their online websites. In some cases, they also tried to locate the controllers by a phone call or in-person, by asking the controllers´ representatives questions relating to the controllers and their processing activities. The average success rate in locating the controllers was 80%, whereas the worst way to do so appeared to be the in-person way since the representatives of the controllers who were approached by the researchers seemed to have a low level of expertise in data protection law and were in many cases unable to answer the questions they were asked. In around a half of the analysed privacy policies, the information about what types of personal data are processed was absent, which simply shows poor coherence with the principle of transparency.[191]

In the second part, where the access requests were filed, the researchers especially demanded the information about sharing personal data with third parties and about automated decision making processes. It was found that in more than a half of all cases, controllers did not provide adequate answers about sharing the personal data with third parties. What is even

[186] Ibid. Page 16.
[187] Ibid. Page 14.
[188] Ibid. Page 18.
[189] NORRIS, C. et al. The Unaccountable State of Surveillance: Exercising Access Rights in Europe. Vol. 34, Springer International Publishing AG, 2017. Pages 45-463.
[190] Ibid. Page 9.
[191] Ibid. Page 405 – 411.

worse, 71% of the controllers did not provide appropriate information about the automated decision making processes. Generally, only in 57% of instances, the adequate access to personal data was actually provided. Other responses were either incomplete or denied, while one in five requests was denied without a substantiation of a valid reason. Geographically, the researchers were able to obtain the access in most cases in the United Kingdom, Germany, and Slovakia.[192] This study also proved how difficult for data subjects it can be to exercise the right of access to personal data. It is partly because of the insufficient knowledge of data subject rights, at other times because of the poor administrative and bureaucratic organization, or violations of legal obligations.[193]

Both studies had been conducted before the GDPR entered into force, i.e. under the Data Protection Directive. One of the conclusions of both of the studies was the call for better implementation of Union law in the data protection field, as the interpretations of several data protection provisions varied among the Member States. The adoption of the GDPR seems to have solved this difficulty since the character of the regulation shifts the force of this act above the force of national laws. In contrast to the directives that require implementation, the GDPR is directly applicable, which ensures that equal data protection provisions now apply to all of the Member States. The authors of the studies recommended the involvement of the national Data Protection Authorities (hereinafter the "DPAs") and even the European Data Protection Board (hereinafter the "EDPB") in raising awareness about the existence of data subject rights and obligations of controllers[194]. Ausloos and Dewitte additionally highlight the role of the Data Protection Officer (hereinafter "the DPO"). While under the Data Protection Directive it was left up to the Member States to set forth the conditions of the appointment of the DPO, the GDPR counts with some situations where the controller must designate the DPO and also provide the possibility to designate one when it is not required. If the controller has appointed the DPO who inter alia deals with the access requests, it is more likely that the data subject obtains more professional response to the access request than in the cases where the requests are answered by persons without necessary expertise. Also, the contact details of the DPO must be published so the data subject can easily find the contact where he or she can direct the access request[195]. I must agree with the advice of strengthening the role of the

[192] Ibid. Page 416 – 422.
[193] Ibid. Page 453 – 454.
[194] AUSLOOS, J., DEWITTE P. Shattering one-way mirrors - data subject access rights in practice. *International Data Privacy Law*. 2018, *8*(1), 4-28. Page 27.
[195] Ibid. Pages 25-26.

DPAs, EDPB and the DPOs, assuming that the knowledge of data subject rights is sine qua non of appropriate accommodation of the right of access to personal data. Data subjects simply cannot benefit from the right of access if they do not have proper information about how to do so. Similarly, if controllers are not at all aware of the right of access nor of data subject rights, it is almost impossible for data subjects to exercise them, as controllers hinder data subjects in doing so. Such unawareness of data subject rights dwells likely in complete unfamiliarity with data protection law. Therefore, I assume that the role of national DPAs and EDPB should be strengthened in order to disseminate the information about the purposes of data protection, principles and important provisions among data subjects, controllers, and processors. The more they understand the merit of data protection law, the better results will be in exercising data subject rights, including the comprehensive compliance with data protection provisions.

The third study[196] was carried out at the time when the GDPR has already been in force. Here, researchers targeted 334 of the most popular websites according to the ranking made by Alexa, an American web traffic analysis company. It is necessary to mention that many of the websites that were subject to the study are located outside the European Economic Area (EEA) where Union law does not apply. However, they offer their services also in the EEA, which makes them obliged to comply with the provisions of the GDPR.

The researchers firstly examined to what extent the websites facilitate submission of the access request. In most cases, they found the description of the procedure in privacy policies, sometimes also the respective form to file the access request was available to download. When there was no such information nor the form, it was necessary to contact competent DPOs, mostly by an e-mail. In some instances, though, the only way to submit the access request was to send it via regular mail or to make a phone call, so the researchers decided to leave these cases out of their study.[197] After submitting the access request, they examined the identity verification carried out by the controllers. It was found that the websites that provided the access request form for a signed-in user did not perform further identification of the requester. Others usually asked for additional information on the requester, a sworn declaration or they made a phone call to verify the requester's identity.[198]

[196] BUFALIERI L., LA MORGIA, M., MEI, A., STEFA, J.*: GDPR: When the Right to Access Personal Data Becomes a Threat*. Sapienza University of Rome, 2020.
[197] Ibid. Chapter III, Section B
[198] Ibid. Chapter III, Section C

Some of the controllers required a copy of the ID card to verify the identity. It is a remarkable fact that they usually wanted to send the copy via e-mail, without using any security measures. What is more, there was barely any information on how the copy of the ID card is stored or whether it is deleted after the authentication phase.[199] When the access request was sent from the e-mail address that matched the e-mail address of the user account in the respective website, controllers usually did not require any further verification. Even when the researchers used a fake e-mail address that was very similar to one that was used for the user account, i.e. the e-mail address that was known to the controller, no steps to verify the validity of such address were taken by the controller. According to the authors of this study, such behaviour might lead to "*spoofing attacks*".[200]

The main result of this study is that around 36% of the targeted websites failed to provide the personal data requested.[201] It was either for technical problems that restrained the researchers from submitting the access request successfully, or because of refusing to provide the personal data or for failing to answer within the 30-day period set out by the GDPR. Some of the controllers even argued that they were not affected by the GDPR.[202] In some of the successful cases where personal data were eventually obtained, the researchers found risky that the controllers provided personal data via e-mail without any encryption or similar safeguards. When the controller provided a password to view the document with the personal data, it was often sent in the same e-mail where the data were attached. At other times, a password to encrypt the personal data was based on the information on the requester, and so it could have been easily revealed.[203]

The third study shows that the ability to exercise the right of access might have improved since the adoption of the GDPR. It is proven by the fact that 88% of the responses to the access request were received within the 30-day period, while the average time to respond was 16,4 days.[204] On the other hand, some of the procedures conducted by controllers could jeopardize the personal data at stake. It was mainly the matter of the identity verification which was either completely omitted or based on unsecured disclosure of an ID. Also, the provision of personal data without bearing their confidentiality might put them in

[199] Ibid. Chapter IV, Section B.
[200] Ibid. Chapter IV, Section C.
[201] Ibid. Chapter VII.
[202] Ibid. Chapter III, Section D.
[203] Ibid. Chapter IV, Section A.
[204] Ibid. Chapter VII.

jeopardy. Such conduct is against the purposes and principles of the data protection and needs to be improved in order to ensure the security of personal data. In addition, the controllers located outside of the EEA need to understand the GDPR and to know that they are obliged to comply with it when they offer their services in the EEA in accordance with Article 3 (2) a) of the GDPR. Their inappropriate approach towards the exercise of the right of access, rationalized by saying the GDPR does not apply to them, is completely unacceptable.

In order to properly understand the notion of the right of access to personal data and to experience how its exercise is achieved in practice, I decided to describe my own experience with filing the access request with a company called Revolut Ltd (hereinafter "the Company" or "the Controller"). The Company offers financial services such as transfers and exchange of money worldwide, while being established in the United Kingdom. I have been a regular user of the services that the Company offers via the mobile application for a couple of years now.

I submitted the access request by sending an e-mail to the address of the Company's DPO, specifically proposing the types of personal data that Revolut Ltd as the Controller collects, i.e. how the company meets its obligation of transparency relating to the collection and use of such data and to what third parties my personal data are disclosed and on what legal grounds it is done so. Right after sending my e-mail, I received an immediate automatic reply stating that the Company aimed to respond within one calendar month. Interestingly, the Company did not require any identity verification. After four days, I received the e-mail response to my request signed by the Data Protection Manager. At first, the Company provided a list of categories of personal data that have been processed. The second information was the data retention period lasting 6 years, which was shortly explained by referring to anti-money laundering, terrorist financing and transfer of funds laws. This was followed by the information concerning the protection of confidentiality and security of personal data that lies in using secure third-party servers protected by firewalls with restricted access and encryption. The response contained a list of third parties to whom personal data have been disclosed, including fraud prevention agencies, cloud storage providers, banks and other financial services partners, card manufacturing and delivery companies and companies from the Revolut group. Finally, the Company provided information concerning the right to lodge a complaint with the ICO and the right to challenge the Company's decision through the English courts. At the end, there was a reference to the Revolut's privacy policy to find more information. The attachment to the e-mail contained my personal contact details, details of my Revolut user account with payment card details, including information about the device on

which the mobile application has been used. I presume that this attachment should have represented a copy of the personal data pursuant to Article 15 (3) of the GDPR. To view the attachment, it was necessary to type the security password. The password was not explicitly mentioned in the e-mail, but the clue to it, which consisted of my personal information, was.

Overall, I would rate this experience as decent. The pros are that the response was received on the fourth day after submitting the access request, which I consider a quick reaction, while the whole response was reasonably understandable since it was written in clear and plain language. These aspects were in compliance with Article 12 (1) and (3) of the GDPR. Securing the copy of the personal data with the password is also favourable. However, the password itself could be easily detected by someone who has read the e-mail and has known some basic personal information about me. Using a password to secure the personal data has already been discussed in the third empirical study in this section, where the passwords to view the personal data were sent in the same e-mail together with the personal data. Such conduct was regarded as inappropriate because it could jeopardize the security and confidentiality of the personal data. For this reason, I consider the measure of securing the copy of the personal data to be a positive remark, however its realisation undoubtedly requires using higher security.

The cons are that the copy of the personal data did not cover all categories of personal data that the Company processes which were included in the e-mail as the information that the company collects. Also, the purposes of the processing were not enumerated in the response nor was the information concerning the automated decision making, which is contrary to Article 15 (1) of the GDPR. However, these facts could be found in the privacy policy which was referred to in the response to the access request. The fact that the identity verification was absent in this case appears to be a little bit alarming even though the fact that the same e-mail address used for filing the access request has also been used for the Revolut user account could be considered a proof that the person filing the request is the user of the account. Anyway, in my opinion, this is not a good practice, considering that the Company offers financial services. Therefore, some of the information they collect and process should require even higher level of security than other, more common operations with personal data. The identity verification is a meaningful step in dealing with access requests and it definitely should not be omitted. Other aspects of the response to my access requests were reasonable, as Revolut Ltd offers financial services, and so there are further legal obligations it must meet. These include particularly obligations imposed by the anti-money laundering, terrorist

financing and transfer of funds laws. Therefore, there are some aspects of the processing that need to be adjusted to comply with such laws, for example the storage period of personal data which might seem to be too long, or number or categories of third parties to whom the personal data are disclosed.

The overall outcome of this experience was nevertheless instructive, and I would consider it positive rather than negative. It is obvious that Revolut Ltd intends to comply with the GDPR and to favour data subject rights. However, there were some worrisome remarks on securing the personal data which should definitely be improved. These include strengthening of the personal data security by implementing measures that would safely provide the password to view the copy of the personal data, including carrying out identity verification of the requester-to make sure that the personal data are not disclosed to unauthorised persons.

4.6. Conclusion

Chapter 4 is the longest and probably the most informative chapter of this thesis. It is also the chapter that mainly contributes to answering the research question of the role of the right of access. The beginning of this chapter tries to present a brief view of the development of the right of access to personal data from the early beginnings of the data protection. It is followed by the description of the right of access in accordance with the paragraphs of Article 15 of the GDPR. The overlapping of the right of access with the right to be informed and the difference between these two rights are discussed, leading to the conclusion that the right to be informed provides the fundamental information on a controller and processing which has to be always provided because of the controller's obligation. In contrast, the right of access provides information on the controller and the processing relating to the particular data subject and is executed when the data subject files the access request. Afterwards, the important aspects of the right of access, such as the verification of the requester's identity and the possibility of obtaining a copy of personal data are examined. The analysis of the right of access includes the assessment of its availability to data subjects from which it has been deduced that every natural person is able to submit the access request pursuant to Article 15 if the material and territorial scope of the GDPR is fulfilled. The most important finding of this chapter is that the right of access serves as the first step that is necessary for the data subject to take in order to exercise the other data subject rights. Besides that, it can indicate how the controller meets its obligations and handles its responsibilities in the data protection area. At

the end of this chapter, three empirical studies are discussed. They all have shown that the right of access is underused and not facilitated enough by controllers. The reason for it evidently derives mostly from the poor awareness of the data protection provisions. In some cases, also the reluctance from controllers or inadequate organisational measures to exercise the right of access have been found. Chapter 4 ends with the description of my own experience with submitting the access request and its outcome. My findings have confirmed that controllers do not always perform identity verification of the requester, which is a very important step in dealing with the access requests, and they have also demonstrated that the security and confidentiality of the personal data might be easily jeopardised if the provision of such data in the response to the access request is not safeguarded sufficiently.

CONCLUSION

Data subjects' awareness of the fact that their personal data are undergoing processing by a particular controller and of other important aspects of such processing can have a significant impact on the protection of their personal data and thus their privacy. Without this knowledge, the data subject might be exposed to unlawful storage, usage, or transfers of his or her personal data to third parties without being aware of it. Such unlawful usage might lead to wrongful profiling or even surveillance of the data subject. Without the knowledge of data subject rights, the data subject cannot have his or her data rectified if they are inaccurate, erase the data if they are stored longer than is appropriate for the purposes of the processing, or challenge a breach of the data protection law. It is obvious that the importance of being informed of the processing of personal data is considerably huge.

The right to be informed under Articles 13 and 14 and the right of access to personal data under Article 15 of the GDPR were designed to ensure that data subjects receive necessary information relating to the processing. While the right to be informed pertains to the positive obligation of the controller to provide the enumerated information to the data subject at the beginning of the processing or no later than one month after obtaining the personal data, the right of access lies in submitting the access request by the data subject to the controller who is obliged to respond within one month whether some of the data subject's personal data are being processed, and if so, to provide other necessary information relating to that processing. These two rights overlap in the scope of the information that is to be provided, but they slightly differ in the purpose of that information. The information provided in the data protection notice pursuant to Articles 13 and 14 concerns the general aspects relating to the processing of personal data by the particular controller and can be same for multiple data subjects. The information provided in the response to the access request relates to the particular data subject and his or her personal data. Both of these rights contribute to the awareness of important aspects of the processing which is necessary for ensuring the adequate level of personal data protection.

However, the right of access to personal data was found to have also other indispensable purposes. It is often regarded as the first step or precondition for the exercise of other data subject rights, such as the right to rectification or erasure, the right to object to the processing, or the right to lodge a complaint with a supervisory authority. Without the information provided upon the access request, the data subject would be normally unable to

exercise these rights. Such conclusion was also expressed by the CJEU in the respective case law[205]. The right of access can also serve as a useful tool for monitoring how controllers and processors comply with the obligations imposed upon them and with other provisions enacted in the GDPR, most importantly with the principles of transparency, fairness, and accountability.

The empirical studies that were compared in Chapter 4 have revealed that the right of access is underused by data subjects and often not accommodated enough by controllers. The main reason for such findings is indisputably the lack of awareness of the right of access, both by data subjects and controllers. As was already mentioned, the lack of awareness of the right of access indicates that data subjects and controllers are often not familiar with the whole data protection law. That is where the right to be informed and corresponding data protection notices are necessary. Controllers must be familiar with the provisions of the GDPR due to their responsibility for the processing of personal data in the course of their activities. They are also responsible for proving that the processing is in compliance with the GDPR. However, the right of access was in some cases also found to be ignored or unsatisfied without a substantial or a valid reason. This was regarded as an inappropriate conduct and it might need the involvement of national DPAs and EDPB to disseminate how to adequately handle access requests. These institutions could also assist in spreading the knowledge of data subject rights and their usage to data subjects.

The right of access may contribute to uncovering the flaws of personal data processing or unlawfulness thereof. Then, the role of the right of access is essential in checking how controllers operate with personal data of data subjects and in allowing them to exercise their other data subject rights. I presume that the aim of this master's thesis was fulfilled, as based on relevant literary works, case law and empirical studies it has been concluded that the right of access has an important place in the protection of personal data.

Although the protection of personal data seems to be strengthened increasingly, there are still some aspects that should be improved as it was shown in the practical remarks of this master's thesis. Personal data are a sensitive object that should possess adequate protection regardless of the country where the processing is being carried out or of the controller's origin. The reason for such protection is that the misuse of personal data can have a considerable impact on our privacy which I believe is a very valuable commodity in today's

[205] C-434/16, Nowak. Paragraph 57 of the judgment, C-553/07, Rijkeboer. Paragraphs 51-52 of the judgment.

society full of profiling, surveillance, and other technological instruments. Therefore, we all should attempt to spread the awareness of data subject rights because, at the end of the day, we all are data subjects.

LIST OF ABBREVIATIONS / SEZNAM ZKRATEK

CJEU	Court of Justice of the European Union
EU	European Union
TFEU	Treaty o the functioning of the European Union
Charter	Charter of Fundamental Rights of the European Union
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
UDHR	Universal Declaration of Human Rights
Member States	Member States of the European Union
Union law / EU law	The law of the European Union
OECD	Organisation for Economic Co-operation and Development
GDPR	General Data Protection Regulation
DPD	Data Protection Directive
WP29	Article 29 Working Party
DPO	Data Protection Officer
EDPB	European Data Protection Board
DPAs	Data Protection Authorities

LIST OF SOURCES / SEZNAM ZDROJŮ

Legal documents:

Universal Declaration of Human Rights (1948)

European Convention on Human Rights (1950)

Charter of Fundamental Rights of the European Union (2000)

Treaty on the Functioning of the European Union (1957)

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

The Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector

The Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector

The Convention for the protection of individuals with regard to automatic processing of personal data

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Annex to the Recommendation of the Council of 23rd September 1980: Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data: Explanatory Memorandum.

Article 29 Working Party: Guidelines on transparency under Regulation 2016/679

Article 29 Working Party: Guidelines on the right to data portability

Bibliography:

Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education and Welfare (1973)

WARREN S., BRANDEIS L. The Right to Privacy, Harvard Law Review

Handbook on European data protection law: 2018 edition. Luxembourg: Imprimerie Centrale in Luxembourg, 2018. ISBN 978-92-9491-901-4

GONZALEZ FUSTER, G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU: Issues in Privacy and Data Protection* [online]. Vol 16. Brussels: Springer International Publishing, 2014. ISBN 978-3-319-05023-2. DOI 10.1007/978-3-319-05023-2

The EU General Data Protection Regulation (GDPR). *A Commentary.* Edited by CH. KUNER, L. A. BYGRAVE, CH. DOCKSEY. Oxford University Press, 2020. ISBN 9780198826491.

NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů: Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3.

POKORNÁ, A., DVOŘÁKOVÁ H. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020. ISBN 978-80-7598-309-1

NORRIS, C. et al. The Unaccountable State of Surveillance: *Exercising Access Rights in Europe*. Vol. 34, Springer International Publishing AG, 2017.

BIER, CH., KÖMPF, S., BEYERER J. A Study on Corporate Compliance with Transparency Requirements of Data Protection Law. Published in: *Data Protection and Privacy: (In)visibilities and Infrastructures*. Vol. 36. Cham: Springer, 2017, pp. 271-292 ISBN 978-3-319-50796-5. DOI 10.1007/978-3-319-50796-5.

Articles:

Opinion by Artemi Rallo: Privacy and Freedom. European Data Protection Law Review. 2018, 4(2)

DOCKSEY, CH. Four Fundamental Rights: Finding the Balance. International Data Privacy Law, vol. 6, no. 3, 2016, pp. 195–209., DOI:10.1093/idpl/ipw014.

VAN DER SLOOT, B. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: *Data Protection and Privacy: (In)visibilities and Infrastructures* [online]. Vol. 36. Cham, Switzerland: Springer, 2017, p. 3-30. ISBN 978-3-319-50796-5. DOI 10.1007/978-3-319-50796-5

AUSLOOS, J., VEALE M., MAHIEU R. Getting Data Subject Rights Right: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2019, *10*(3), 283-309.

AUSLOOS, J., DEWITTE P. Shattering one-way mirrors - data subject access rights in practice. *International Data Privacy Law*. 2018, *8*(1), 4-28

BUFALIERI L., LA MORGIA, M., MEI, A., STEFA, J.: GDPR: When the Right to Access Personal Data Becomes a Threat. Sapienza University of Rome, 2020.

Case law:

C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779

C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. ECLI:EU:C:2014:317

C-362/14, Maximillian Schrems v Data Protection Commissioner. ECLI:EU:C:2015:650

C-486/12. Request for a preliminary ruling under Article 267 TFEU from the Gerechtshof te ’s-Hertogenbosch (Netherlands), made by decision of 26 October 2012, received at the Court on 31 October 2012, in the proceedings brought by X. ECLI:EU:C:2013:836

C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General. ECLI:EU:C:2014:238

C-201/14, Smaranda Bara and others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF), ECLI:EU:C:2015:638

C-473/12, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte, intervening parties: Union professionnelle nationale des détectives privés de Belgique (UPNDP), Association professionnelle des inspecteurs et experts d’assurances ASBL (APIEA), Conseil des ministres. ECLI:EU:C:2013:715

C-40/17. Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV. ECLI:EU:C:2019:629

OPINION OF ADVOCATE GENERAL BOBEK, delivered on 19 December 2018, Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

C-434/16 Peter Nowak v Data Protection Commissioner. ECLI:EU:C:2017:994

C-556/07, College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer, ECLI:EU:C:2009:293

C-141/12, C-372/12. YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel (C-372/12) v M, S. ECLI:EU:C:2014:2081

Other sources:

Fact Sheets on the European Union, European Parliament – Personal Data Protection. Available via: https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection Retrieved 1.10.2020

European Commission Press Corner Questions and Answers: Data Protection Reform. Available via: https://ec.europa.eu/commission/presscorner/detail/en/MEMO Retrieved 3.10.2020[206]

For organisations/Guide to Data Protection/Guide to the General Data Protection Regulation (GDPR)/Individual rights/Right to be informed. Available via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/#top Retrieved 29.11.2020

For organisations/Guide to Data Protection/Guide to the General Data Protection Regulation (GDPR)/The right to be informed/How should we draft our privacy information? Available via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/how-should-we-draft-our-privacy-information/#id1 Retrieved 29.11.2020

Guide to the General Data Protection Regulation (GDPR)/Right of access/When can we refuse to comply with a request? Available via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/when-can-we-refuse-to-comply-with-a-request/ Retrieved 02.11.2020.

ICO UK Guide to the General Data Protection Regulation / Right of access. Available via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ Retrieved 23.10.2020

Personal consultation with the head of the Consultation department of the Office for Personal Data Protection, Mgr. Ladislav Hejlík, on 26.10.2020.

Max Schrems: The Austrian Thorn In Facebook's Side, available via: https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/?sh=3eb66e3e7b0b Retrieved 6.11.2020.

Max Schrems: the man who took on Facebook – and won, available via: https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544 Retrieved 6.11.2020.

[206] During the revision of the thesis on 10.12.2020, it was found that this link is no longer up to date.

ABSTRACT

Nowadays, when the world is full of technological transformations and digitalisation, surveillance, and a global flow of personal data, it is necessary to have the possibility of adequate protection of personal data. Such protection is more effective when data subjects are aware of the rights granted to them under data protection law and thus are able to effectively exercise them. In order to do so, they have to be informed of certain aspects of their personal data processing that is carried out by a particular controller. The right to be informed and the right of access to personal data were designed to ensure that data subjects have that necessary information.

This thesis focuses on the right of access to personal data and raises the question about the extent to which this right determines the effectiveness of the protection of personal data. In order to answer this question, the author firstly deals with the right to data protection in general to explain its basic concepts, which is necessary to grasp the aim of this thesis. This is followed by discussing the general aspects of data subject rights, including the determination of principles that need to be adhered to under data protection law. Subsequently, the right to be informed, strongly correlated with the right of access to personal data, is analysed. Finally, by examining the legal background of the right of access, scrutinizing its key aspects, and analysing its exercise in practice, the author concludes the importance of the right of access to personal data.

It is shown that the right of access is often referred to as the first step or a precondition for the exercise of other data subject rights, such as the right to rectification or to erasure, the right to object to the processing, or the right to lodge a complaint with a supervisory authority. The right of access is also able to uncover flaws of the processing of personal data since it enables data subjects to check how a controller complies with data protection law and the core principles thereof.

Nevertheless, the empirical part of this thesis reveals that the right of access is not exercised adequately in practice. The author scrutinizes three different empirical studies on the exercise of the right of access, the results of which show the need of better knowledge of the existence of the right of access to personal data and its deeper comprehension. The studies found a considerable number of controllers who did not satisfy the data subjects' access requests or satisfied them only partly, often without a lawful reason to do so. The author also describes her own experience with submitting the access request. Overall findings of this

empirical part of the thesis are that the individuals, i.e. both data subjects and controllers, need to be aware of the data protection more than they are. In order to achieve that, the author suggests that national DPAs and EDPB should be engaged in spreading such awareness among data subjects and controllers. The author believes that when the adequate knowledge and comprehension of data protection rights are achieved, the access requests will be handled in a better manner.

KEY WORDS

right of access
personal data
processing
information

ABSTRAKT

V současnosti je společnost, ve které žijeme výrazně ovlivněna technologickými transformacemi, digitalizací, dohledem a globálním tokem osobních údajů. Je proto nevyhnutné, aby jednotlivci měli zabezpečenou tomu odpovídající ochranu jejich osobních údajů. Taková ochrana je účinnější, pokud subjekty údajů znají svá práva, která jsou jim v rámci práva na ochranu osobních údajů přiznána a pokud jsou schopny tyto práva účinně uplatňovat. Za tímto účelem musí být subjekty údajů informovány o zpracování jejich osobních údajů, a o všech skutečnostech s tím souvisejících. Toto zajišťuje zejména právo být informován a právo na přístup k osobním údajům.

Tato diplomová práce se zabývá právem na přístup k osobním údajům a pokládá si otázku, do jaké míry je toto právo schopno ovlivnit účinnost ochrany osobních údajů. Za účelem odpovědi na tuto otázku se autorka nejprve věnuje právu na ochranu osobních údajů obecně, aby vysvětlila jeho základní pojmy, které jsou nutné k uchopení cíle této práce. Poté se autorka věnuje obecným aspektům práv subjektů údajů jako takových a zásadám, kterých je v rámci ochrany osobních údajů nutno dodržovat. Dále je analyzováno právo být informován, které s právem na přístup k osobním údajům neodmyslitelně souvisí. Nakonec autorka dospívá k závěru o úloze práva na přístup k osobním údajům, a to zkoumáním jeho vývoje, klíčových aspektů a pozorováním jeho uplatňování v praxi.

Tato diplomová práce prokazuje, že právo na přístup je často označováno jako první krok nebo předpoklad k výkonu dalších práv subjektu údajů jako např. práva na opravu nebo výmaz osobních údajů, práva vznést námitku proti zpracování nebo práva podat stížnost u dozorového úřadu. Právo na přístup k osobním údajům může také odhalit nedostatky zpracování osobních údajů, protože umožňuje subjektům údajů kontrolovat, jak správce dodržuje právní předpisy a základní zásady práva na ochranu osobních údajů.

V empirické části této práce je nicméně zjištěno, že právo na přístup není v praxi dostatečně uplatňováno. Autorka analyzuje a porovnává tři různé praktické studie o výkonu práva na přístup k osobním údajům v praxi, jejichž výsledky naznačují potřebu většího povědomí jednotlivců o existenci tohoto práva a jeho hlubšího porozumění. Dané studie navíc ukázaly, že existuje značný počet správců, kteří žádostem subjektů údajů o přístup k osobním údajům vůbec nevyhověli nebo jim vyhověli jen částečně, a to často bez relevantního důvodu. Autorka navíc popisuje svou osobní zkušenost s podáním žádosti o přístup k osobním údajům. Celkovým zjištěním této empirické části práce je, že jednotlivci, jakožto subjekty údajů i

správci, by měli mít větší povědomí o ochraně osobních údajů. Za tímto účelem autorka navrhuje, aby národní dozorové úřady a Evropský sbor pro ochranu osobních údajů byly i v této oblasti více činné a šířily informace o ochraně osobních údajů mezi subjekty údajů a správce. Autorka se domnívá, že s dosažením kvalitních znalostí o ochraně osobních údajů a porozuměním této ochrany budou i žádosti o přístup k osobním údajům vyřizovány adekvátněji.

KLÍČOVÁ SLOVA

právo na přístup
osobní údaje
zpracování
informace