RIGA GRADUATE SCHOOL OF LAW

LAURA GRAVA

PERSONAL DATA PROTECTION IN THE EU – COOPERATION AND COMPETENCES OF EU AND NATIONAL DATA PROTECTION INSTITUTIONS AND BODIES

RGSL RESEARCH PAPER
No. 18

Riga Graduate School of Law

Established in 1998, the Riga Graduate School of Law (RGSL) has emerged as a leading legal education and research institute in the Baltic region. RGSL offers numerous study programmes in the area of International and European Law at bachelor and master's level and cooperates with the University of Copenhagen on a joint doctoral programme. The School benefits from partnerships with numerous leading European universities and cooperates closely with the University of Latvia, the major shareholder. In addition to its growing resident faculty, RGSL also benefits from the involvement of a large number of eminent scholars and practitioners based in the local environment, elsewhere in Europe, and overseas. The School is located in the *Art Nouveau* district of Riga and hosts an outstanding law library.

A primary objective of RGSL is to contribute to the development of Latvia and the wider region by educating new generations of motivated and highly skilled young scholars and professionals capable of contributing to the ongoing process of European integration. Research and education in the area of international and European law are integral to the realisation of this objective.

The present series of Research Papers documents the broad range of innovative scholarly work undertaken by RGSL academic staff, students, guest lecturers and visiting scholars. Scholarly papers published in the series have been peer reviewed.

ISSN 1691-9254

About the author:

Laura Grava graduated the Riga Graduate School of Law with a degree in Law and Business in 2014 and continued her academic studies at RGSL by obtaining an LL.M in International and European law in 2016. Currently working as a lawyer in one of the leading regional law firms, her main areas of interest are corporate law and data protection. This is the publication of the author's distinction-awarded Master's thesis defended at the Riga Graduate School of Law in June 2016.

Abstract:

This article focuses on the institutional aspect of European Union (EU) personal data protection. The aim of the article is to identify current problems in division of competences and in cooperation between national and EU data protection institutions. The author analyses these aspects on two levels. On the vertical level, the author analyses the competences and cooperation between national and EU institutions and on the horizontal level – the division of competences and cooperation between different national data protection authorities.

As of now, each Member State has different data protection rules and procedures. Moreover, as in the EU context data protection is a shared competence, MS are under the obligation to avoid clashes of interests and competences. But due to the particularities of the current legal setup in the area of data protection, national data protection authorities have different levels of competences, involvement and participation in enforcement and protection of personal data. Even though national data protection agencies are obliged by EU law to cooperate, there are no certain ways or tools to ensure that they do so. And, given the recent Court of Justice of the European Union (CJEU) judgments in *Weltimmo*, *Google Spain*, *Schrems* and other cases involving personal data, the competences and required level of cooperation between national and EU institutions have become more unclear than ever.

The author considers that the current legal setup in terms of inter-institutional cooperation is not effective and is prone to creating more problems. As no clear legal mechanism exists, cooperation can become burdensome, complicated, and lengthy, thus failing to ensure uniform application of EU law and assure the legitimate expectations of data subjects or controllers. Moreover, the latest CJEU judgments on the issue of competences of national and EU data protection institutions can cause uncertainties and possible misunderstandings in terms of clear division of powers. It can be expected that in a few years the current problems should be resolved with the implementation of a new EU data protection regulation.

Key words: Personal data protection; EU data protection; national data protection authorities; division of competences; competences; cooperation between institutions.

TABLE OF CONTENTS

1. DATA PROTECTION AS UNDERSTOOD IN EU LAW

The understanding that personal data protection is an area of law that requires special protection has been present since the 1950's. Even if there were no legal instruments addressing specifically personal data, Article 8 of the European Convention on Human Rights (hereinafter – ECHR) provides for protection of personal life, which is understood to include personal data protection. Currently there are many European Union (hereinafter – EU) legal instruments that define data protection and set the main principles and obligations which have to be observed when dealing with personal data. In this chapter the author will, firstly, define the main elements of the concept of personal data as understood in EU law, secondly, analyse the main legal instruments applicable to data protection and, thirdly, address the institutions and bodies at EU and Member State (hereinafter – MS) level, which are competent to deal with data protection.

1.1. Concept of personal data

For the purposes of this research, it is important to define the main concepts of personal data protection in EU law. This chapter will focus on defining such concepts as personal data, data subject, data controller and processor. The interpretation of these concepts will be analysed only through the perspective of EU law as that is the area of focus of this research.

1.1.1. Main terms

Personal data and data subject

The concept of personal data in EU law was first defined in 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 (hereinafter – Data Protection Directive)[1]. Article 2(a) of this Directive sets:

> 'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.2

A similar definition can be found in Article 2(a) of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter – Convention 108)[3], which sets that ""personal data" means any information relating to an identified or identifiable individual ("data subject")"[4]. These definitions also incorporate the definition of data subject – any individual. When

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) *OJ L* 281, 23.11.1995, pp. 31–50.
[2] Data Protection Directive, Art. 2(a).
[3] Council of Europe. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Council of Europe Treaty Series 108 1981.
[4] Convention 108, Art. 2(a).

drafting the Data Protection Directive, the EU lawmaker wished to encompass the elements already present in the definition in Convention 108, in order to "cover all information which may be linked to an individual"[5].

Personal data is any kind of information on an identified or identifiable person, for example, name, identity code, or a photograph. Any information can be considered personal data if it allows identification of a certain individual. The term is thus interpreted very broadly, in order to encompass any kind of information which in certain circumstances or by certain individuals could help to identify a person. To further understand the concept, it can be explained by analysing the components or elements of the definition set in the Data Protection Directive. There are several elements:

- "any information" – this element further emphasizes that any information, objective or subjective, true or false, can be considered to be personal data. For example, a personal description of an individual, the social or economic behaviour of the individual, his appearance, voice, habits, and so on. This has also been confirmed by the Court of Justice of the European Union (hereinafter – CJEU), which has set that "the term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies"[6]. Moreover, the information can be in any form, i.e., it can be alphabetical, numerical, graphical, photographical or acoustic.[7]
- "relating to" – it is considered that information relates to an individual when it is about that individual, even if at first this is not clearly evident.[8] For example, even if the information is about an object, a particular situation or is in combination with other circumstances, the information can relate to a person.
- "an identified or identifiable" – a natural person can be identified when "within a group of persons, he or she is 'distinguished' from all other members of the group"[9], but a person is identifiable, if he or she can be "distinguished". Thus it is irrelevant if the person has already been identified or could possibly be identified at some time in the future. In both circumstances information, which can help to do so can be considered to be personal data. This element is also further explained by the definition in the Data Protection Directive, which sets

  > An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[10]

- "natural person" – it is generally presumed that the Data Protection Directive and personal data protection laws in the EU cover protection of data of natural persons only. Nevertheless, as MS have the discretion to widen the scope of

[5] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. 01248/07/EN
WP 136, p. 4.
[6] CJEU case C-101/01, *Criminal proceedings against Bodil Lindqvist*, EU:C:2003:596, para. 24.
[7] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data, p. 7.
[8] *Ibid*, p. 8.
[9] *Ibid*, p. 12.
[10] Data Protection Directive, Art. 2(a).

application of the Data Protection Directive in certain aspects, MS can set that information on legal persons, deceased persons or unborn children can also be considered personal data. Indeed, the Data Protection Directive does not explicitly prohibit protection of personal data of legal persons, thus some MS, such as Austria, Italy, Luxembourg and, in some aspects, Denmark, provide for personal data protection of legal persons.[11] As the CJEU has expressed:

> Nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof, provided that no other provision of Community law precludes it.[12]

This element also illustrates what is understood as a data subject. Thus, depending on national data protection regulation, a data subject is a natural person, a deceased person, a legal person or an unborn child.

The definition of personal data may also vary in the national data protection legislation of each MS. As mentioned, MS have a discretion to widen the scope of the definition. Thus it is possible that the concept of personal data will include different elements in each MS. To illustrate, the definition of personal data in the Personal Data Protection Law of Latvia is very similar to that in the Data Protection Directive and that of Convention 108, setting that personal data is "any information related to an identified or identifiable natural person"[13]. A similar definition can be found in Danish personal data legislation ("'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject')"[14]) and the German personal data law (""Personal data" means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)"[15]). But the Personal Data Act of Sweden gives a different definition to personal data, stating that personal data is "all kinds of information that directly or indirectly may be referable to a natural person who is alive"[16]. Thus, in Sweden, the concept of personal data does not include data on legal entities, deceased persons or unborn children.[17]

Data controller

Personal data is usually obtained and processed by a data controller. The Data Protection Directive defines a data controller as:

---

[11] C. Kuner. *European data protection law: corporate compliance and regulation.* 2nd edition. Oxford; New York: Oxford University Press, 2007, p. 77.
[12] CJEU case C-101/01, *Criminal proceedings against Bodil Lindqvist*, para. 98.
[13] Parliament of the Republic of Latvia. Personal Data Protection Law of Latvia (23.03.2000), Art. 2(3).
[14] Danish Parliament. Act on Processing of Personal Data. Act No. 429 of 31 May 2000, Art. 3(1). Available at: https://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/ Last visited on 10 March 2017.
[15] German Bundestag. Federal Data Protection Act, Art. 3(1). Available at: http://www.gesetze-im-internet.de/englisch_bdsg/ Last visited on 10 March 2017.
[16] Swedish Parliament. Personal Data Act of Sweden (1998:204), issued 29 April 1998, Section 3.
[17] E.W. Hager, A. Niden. "Sweden" in *Data Protection & Privacy. Jurisdictional comparisons.* 2nd edition. London: Thomson Reuters, 2014, p. 770.

> Natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.[18]

This definition has three main points, which describe what a controller is.

First, it is set that a controller is a "natural or legal person or any public authority, agency or any other body"[19]. Thus, a controller can be a private or public figure and does not need any official nomination or declaration to be considered one. But in order to ensure the data subject a greater possibility to refer to a stable entity, a legal person will most likely be considered a controller (for example, if data is processed within a company, that company will be the controller, rather than the employee who carried out the processing).[20] Thus, in case of a breach, the natural person in charge of processing will most likely not be liable and the company will bear the risks. Nevertheless, if a natural person, i.e. an employee of a company, were to commence processing data outside the tasks given by the company and for his/her own needs, that employee would be considered to be a controller. Thus, in order to assess who is the data controller and who bears the liability in case of any breaches, it is important to analyse the specific situation and parties involved.

Second, the definition sets that a controller acts "alone or jointly with others"[21], meaning it is possible that more than one controller is responsible for processing certain data. In situations involving more than one actor who determines processing of personal data, all actors should be considered to be data controllers and thus subject to the requirements set in the Data Protection Directive and MS national data protection laws. As explained by the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (hereinafter – Article 29 Working Party or Working Party), ""jointly" must be interpreted as meaning "together with" or "not alone" in different forms and combinations"[22].

Third, a data controller is one who "determines the purposes and means of the processing of personal data"[23]. Thus, the controller is one who makes the decision on which data to collect and for what purposes it will be processed. Indeed, the controller is the one who sets all the rules according to which data will be processed. The possibility to determine the purposes may arise out of various legal or contractual competences. Legal provisions can "imply a certain responsibility"[24] to collect and process personal data. For example, an employer is usually legally required to acquire some information on its employees, thus becoming a data controller. Similarly, a contract can also stipulate that one of the contracting parties will process the personal data of the other, thus becoming a controller. If there are

---

[18] Data Protection Directive, Art. 2(d).
[19] *Ibid*.
[20] Article 29 Data Protection Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". 00264/10/EN WP 169.
[21] Data Protection Directive, Art. 2(d).
[22] *Supra* note 20.
[23] Data Protection Directive, Art. 2(d).
[24] *Supra* note 20.

no legal, contractual or factual circumstances for determining how and for what purposes personal data will be processed, there is no data controller.

Data processor

When a data controller has obtained data, it can choose to designate a data processor, which will process the data according to the requirements of the controller. As Article 2(e) of the Data Protection Directive sets, a data processor is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"[25]. This definition is very broad, in order to cover any natural or legal persons who would process personal data as required by the controller and would be subject to the Data Protection Directive. A controller can decide to appoint a data processor, if it wishes to, as there are no preconditions for when this can be done. If the data processor goes beyond what is required by the controller (i.e. processes more data or for other purposes than required), it is no longer considered a processer, but rather a joint controller.[26] A data processor has to observe the requirements under the Data Protection Directive as to the security of data processing and observance of the mandate set by the data controller.

1.1.2. Data protection and right to privacy as different concepts

In addition to defining personal data, it is important to distinguish this concept from that of privacy. Even though the CJEU or European Court of Human Rights (hereinafter – ECtHR) has not set a clear distinction between the two concepts, it can be argued that they are not one and the same and involve different levels of rights protected. It is argued that personal data is a much broader concept than privacy as it also relates to other freedoms and rights, and protects data regardless of the relationship with privacy.[27] Indeed, where privacy could be considered as "the right to be left alone"[28], data protection encompasses a broader view of possible and permissible actions with one's data. The right to privacy can also be defined as a "right which prevents public authorities from measures which are privacy invasive, unless certain conditions have been met"[29]. But data protection strives to "establish conditions under which it is legitimate and lawful to process personal data"[30]. So the two concepts are not one and the same.

Nevertheless, the two concepts are very often interlinked and sometimes used as synonyms. Moreover, the link is strengthened by Article 8 of the ECHR, which protects the right to private and family life. Indeed, very often the ECtHR has

[25] Data Protection Directive, Art. 2(e).
[26] *Supra* note 20.
[27] H. Hijmans. "The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU" (PhD diss. Faculty of Law at the University of Amsterdam and Faculty Law and Criminology at the Vrije Universiteit Brussel, 2016), p. 67. (Hijmans, 2016)
[28] J.S. Peers, T. Hervey, J. Kenner, A. Ward. *The EU Charter of Fundamental Rights: a commentary.* Oxford; Hart Publishing, 2014, p. 228.
[29] European Data Protection Supervisor. Legislation. Available at: https://secure.edps.europa.eu/EDPSWEB/edps/cache/offonce/EDPS/Dataprotection/Legislation Last visited on 10 March 2017.
[30] *Ibid*.

also interpreted this right to cover the right to data protection.[31] The ECtHR has in multiple cases applied Article 8 in order to ascertain whether the right to personal data protection has been breached, thus clearly indicating that it considers data protection as one of the rights protected by the wording of Article 8 of the ECHR.[32] Similarly, the CJEU has often used the concept of data protection and privacy as one and the same right, referring to Article 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union[33] (hereinafter – Charter) simultaneously. For example, in *Volker und Markus Schecke* the Court set:

> it must be considered that the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual [...] and the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention.[34]

It stated similarly in *Michael Schwarz v Stadt Bochum*, indicating that it considers both articles in a "joint reading"[35]. But the CJEU is not consistent in referring to both Articles. In *Deutsche Telekom AG v Bundesrepublik Deutschland* it referred only to Article 8 in order to analyse lawful processing of personal data.[36] But in *Ryneš*, when looking at the legitimacy of processing personal data, the CJEU referred only to Article 7 of the Charter.[37] Thus, the CJEU has refrained from clearly distinguishing the two rights.

But, when discussing EU law, some authors consider that data protection and privacy are not synonyms. It is argued that the concept of privacy involves the notion of informational self-determination, meaning a person's right to determine for himself when, how and to what extent information about him is communicated to others.[38] This notion is not in accordance with what EU law understands as data protection. Indeed, self-determination or consent to data processing is only one of the grounds for legitimate data processing under EU law. Nevertheless, the secondary law of the EU also provides for other grounds for processing, by evaluating the legitimate interests of the data subject and the data controller and thus ensuring lawful processing without personal consent.[39] Thus, even though

---

[31] ECtHR. *Amann v. Switzerland*. Case No. 27798/95, 16 February 2000; ECtHR. *Taylor-Sabori v. the United Kingdom*. Case No. 47114/99, 22 October 2002; ECtHR*. M.S. v. Sweden*. Case No. 74/1996/693/885, 27 August 1997.

[32] European Union Agency for Fundamental Rights. "Handbook on European data protection law", p. 37. Available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf Last visited on 10 March 2017.

[33] Charter of Fundamental Rights of the European Union (Charter), *OJ C* 326, 26.10.2012, pp. 391–407.

[34] CJEU joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, EU:C:2010:662, para. 52.

[35] CJEU case C-291/12, *Michael Schwarz v Stadt Bochum*, EU:C:2013:670, para. 25.

[36] CJEU case C-543/09, *Deutsche Telekom AG v Bundesrepublik Deutschland,* EU:C:2011:279, para. 49.-53.

[37] CJEU case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, EU:C:2014:2428, para. 29.

[38] *Supra* note 28, p. 229.

[39] *Ibid*.

privacy and data protection are closely interlinked, data protection goes beyond the right to privacy and should be considered as a separate right.

1.2. Applicable legal norms

As this research focuses on EU law, it is important to analyse the legal norms which govern data protection in the EU. Data protection provisions are present in the Treaty of the Functioning of the European Union (hereinafter – TFEU)[40] and the Charter, as well as other more specific legal norms, such as directives and regulations on various data protection matters. Currently, the main legal instrument for personal data protection in the EU is the Data Protection Directive. It should be stressed that this research aims to analyse the correlation and relationship with national and EU institutions in terms of data protection. Thus, EU legal norms regulating data protection within EU institutions and bodies will not be analysed in detail, and a more detailed analysis will be aimed at other legal norms which govern the above mentioned relationship. Other EU legal norms in the area of personal data protection include, firstly, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (Regulation 45/2001)[41], which applies only to data protection and processing rules within the EU institutions and does not concern cooperation with MS institutions. This document will be briefly analysed in Chapter 1.3.4, when analysing the European Data Protection Supervisor – the official data protection authority in the EU. Secondly, the author will also not analyse in detail Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter – e-Privacy Directive)[42] (as amended in 2009 by EU Directive 2009/136/EC[43]). The e-Privacy Directive does not refer to the competences or obligations of national or EU institutions and should be considered as complementing and particularizing the Data Protection Directive[44] in the electronic communications sector.

Additionally, it must be stressed that at the moment of this research Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April

---

[40] Consolidated version of the Treaty of the Functioning of the European Union (TFEU). *OJ C* 326, 26.10.2012, pp. 47–390.

[41] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (Regulation 45/2001), *OJ L* 8/1, 12.1.2011.

[42] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive), *OJ L* 201, 31/07/2002, pp. 0037-0047.

[43] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *OJ L* 337, 18.12.2009, pp. 11–36.

[44] E-Privacy Directive, Art. 1(2).

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 (hereinafter – General Data Protection Regulation)[45] has just been adopted, so the author will also address this legal instrument. Moreover, it is important to briefly analyse the different national data protection laws of MS in terms of the competences of national data protection agencies (hereinafter – DPAs), as they may illustrate the different approaches and levels of competences attributed to national and EU institutions and bodies.

1.2.1. Treaty of the Functioning of the European Union

Article 16 of the TFEU prescribes the general right to personal data protection to everyone and it reads as follows:

> 1. Everyone has the right to the protection of personal data concerning them.
>
> 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.[46]

This Article illustrates that the EU has recognized personal data protection as a fundamental right and coincides with Article 8 of the Charter. This provision sets data protection as a fundamental right of EU law and "elevates the provision on data protection to a 'provision of general application' under Title II alongside other fundamental principles of the EU"[47]. So even if personal data processing takes place within one MS, the EU has set that is has to be protected as a fundamental right.

The second part of Article 16 sets the obligations of EU institutions to legislate in the area of personal data protection. It sets the mandate of EU institutions to adopt legislation on data protection, also leaving room for MS to adopt national legislation. This part establishes protection of personal data within EU institutions and other bodies and within each MS. So the EU legislator adopts the main tasks of both EU and national authorities to ensure effective fulfilment of Article 16(1) of the TFEU, but their execution is left to the MS, in so far as EU law allows. The last sentence of Article 16(2) provides that the independent authorities (meaning national DPA's) must oversee these rules. As confirmed by the CJEU in *European Commission v Republic of Austria* and *European Commission v Federal Republic of Germany* in relation to the independence of national DPA's, MS can lay down the specific regulatory framework to ensure effective protection of personal data as envisaged by the EU.

---

[45] 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), *OJ L* 119, 4.5.2016, pp. 1–88.

[46] TFEU, Art. 16.

[47] F. Ferretti. "A European Perspective on Data Processing Consent through the Re-conceptualization of European Data Protection's Looking Glass after the Lisbon Treaty: Taking Rights Seriously". *European Review of Private Law*, 2-2012, p. 480.

1.2.2. The Charter of Fundamental Rights of the European Union

With adoption of the Lisbon Treaty, the Charter has been granted the same legal status as primary law of the EU, as prescribed by Article 6 of the Treaty of the European Union (hereinafter – TEU). One of the fundamental rights protected by the Charter is personal data protection. Article 8 of the Charter sets:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.[48]

It is important to stress that unlike in the ECHR, data protection has been set as a separate fundamental right from private and family life (Article 7 of the Charter). It is even argued that no UN human rights convention addresses data protection as a specific provision, but merely deduces this right from the right to privacy.[49] Thus, it is a clear statement and signal from the EU legislator that personal data is a specific right which requires protection. Article 8 of the Charter is in some way similar to Article 16 of the TFEU, firstly, providing that data protection is a fundamental right and, secondly, emphasizing that compliance with the respective norm should be overseen by an independent authority, meaning national DPAs. This has also been reconfirmed by the CJEU in *European Commission v Republic of Austria,* where the Court established that

> the requirement that compliance with European Union rules on the protection of individuals with regard to the processing of personal data is subject to control by an independent authority derives from the primary law of the European Union, inter alia Article 8(3) of the Charter of Fundamental Rights of the European Union and Article 16(2) TFEU.[50]

As discussed in Chapter 1.1.2 of this research, Article 8 of the Charter is commonly used by the CJEU in order to emphasize the importance of data protection in the EU. It is argued that with adoption of the Lisbon Treaty and the Charter becoming a part of EU primary law, the CJEU has substantially expanded protection of rights to data privacy, using the Charter as the legal basis for ensuring the level of protection.[51]

---

[48] Charter, Art. 8.

[49] D. McGoldrick. "The Charter and United Nations Human Rights Treaties" in Peers, S., Ward, A. *The EU Charter of Fundamental Rights. Politics, Law and Policy.* Oxford: Hart Publishing, 2004, p. 112.

[50] CJEU case C-614/10, *European Commission v Republic of Austria*, EU:C:2012:631, para. 36.

[51] F. Fabbrini. "The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court" in Vries, S., Bernitz, U., Weatherhill, S. *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing.* Oxford: Hart Publishing, 2015, p. 218.

1.2.3. EU Data Protection Directive

The Data Protection Directive is considered to be the main EU legal instrument on personal data protection. It defines what personal data is, what can or cannot be done with such data and, moreover, which national and EU institutions are competent to act in the field of data protection.

The Data Protection Directive was adopted in 1995, when only 1% of the EU population was using the Internet and such companies as Facebook, Twitter or Google were not yet operating.[52] Thus, it cannot be considered a modern piece of legislation, and possibly it does not effectively ensure data protection in today's context. Nevertheless, the CJEU is using its powers to interpret the legislation so it would be possible to apply its provisions to current issues. Upon implementation of the Directive, the MS were allowed some room for manoeuvre and the possibility to introduce specific rules. This possibility has been recognized by the CJEU, stating that it can be done if the provisions of the Directive have so provided and only if it is done in accordance with the Directive's objective – "maintaining a balance between the free movement of personal data and the protection of private life"[53]. MS have used this opportunity to "adapt" the Directive to the national specifics of their data protection laws and, thus, currently data protection legislation varies across the EU.

The Data Protection Directive has a very broad scope of application. As Article 3(1) of the Directive sets, it is applicable to any kind of processing of personal data (wholly or partially, using automatic means or otherwise). Article 3(2) of the Directive sets when it is not applicable – firstly, when the processing falls outside of Community law or is in any case related to public security, defence or any activities of the State in areas of criminal law, and secondly, when processing is carried out by a natural person for purely personal or household needs.[54] As Advocate General Kokott has set in her opinion in *Satamedia*, the Directive has such a broad scope of application, "which already reaches almost beyond the establishment of the internal market"[55].

The Data Protection Directive sets the obligation on MS to set up an independent national DPA which would serve certain functions and have certain powers. This aspect of the Directive will be analysed in Chapter 1.3.2.

1.2.4. General Data Protection Regulation

On 4 May 2016 the General Data Protection Regulation was published in the EU Official Journal. This regulation will substitute the Data Protection Directive and will create single data protection legislation in all EU MS. Work on this regulation has been extensive and long, as the first announcement from the European Commission as to the need for such regulation was in 2010.[56] The norms of the General Data

---

[52] O. Lynskey. *The foundations of EU data protection law*. New York, NY: Oxford University Press, 2015, p. 4.
[53] CJEU case C-101/01, *Criminal proceedings against Bodil Lindqvist*, para. 97.
[54] Data Protection Directive, Art. 3(2).
[55] Opinion of Advocate General Kokott, Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, EU:C:2008:266, para. 53.
[56] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive

Protection Regulation are more complex and elaborate and introduce new concepts in data protection legislation as well as establishing new data protection bodies. As this research focuses on competences and their division among EU and national institutions and bodies, it is important to illustrate the main changes in this area following the entry into force of the General Data Protection Regulation. This analysis is contained in Chapter 3.3 of the research.

1.2.5. National data protection laws

As mentioned before, the national legal norms of data protection in EU MS vary slightly. As the Data Protection Directive has been implemented differently, there are currently 28 different data protection regulations in the EU. For the purposes of this research, the author will not analyse the different provisions relating to the concepts of data protection, but will focus on the main differences in terms of competences of data protection authorities.

In general, the strictness of data protection norms varies greatly among MS. In such states as France, Germany, Spain and Belgium, data protection is heavily regulated, but in "newer" MS such as Lithuania, the level is rather moderate.[57] The differences can be seen both in the wording and scope of legal norms, as well as the administrative set-up for monitoring compliance. For example, most EU MS have one DPA, which administers data protection issues. Nevertheless, Germany has a DPA for each federal unit, each supervised by the Federal Data Protection Commissioner. Additionally, the legal setup of national DPAs is different – for example, in Finland, the national DPA consists of a Data Protection Ombudsman that cooperates and refers matters to the Data Protection Board, which can then act further on matters referred to the Ombudsman.[58] Thus, the competences attributed to the national authority may vary depending on national legislation.

A common position for MS data protection laws is that the DPA has the competence and right to start an investigation upon receiving a complaint from a data subject or upon suspicions of violation.[59] Moreover, as the Data Protection Directive provides for an obligation to cooperate with other DPAs, this aspect is observed in all MS, but not strictly regulated and without specific provisions in this regard. The consequences of a breach are rather different in terms of type of liability (administrative or criminal) and the amount of fines applicable. A large part of MS data protection rules provide for an administrative penalty.[60] But some MS, such as Belgium, France, Denmark, Finland, Italy and Germany, have established a possibility of criminal liability for certain violations of personal data protection. Thus, the

approach on personal data protection in the European Union. 4 November 2010, COM (2010) 609.

[57] DLA Piper. Data Protection Laws of the World. Available at: https://www.dlapiperdataprotection.com/#handbook/world-map-section Last visited on 10 March 2017.

[58] *Ibid*.

[59] European Union Agency for Fundamental Rights. Data Protection in the European Union, the role of National Data Protection Authorities, p. 21. Available at: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf Last visited on 10 March 2017.

[60] For example, data protection regulation of Latvia, Austria, Hungary, Ireland.

competences for imposing certain penalties and fines are different among MS and vary depending on the type of breach. In addition, the types of breaches and the penalty amounts are also rather different and can range from several hundred euros (for example, the maximum penalty in Lithuania is 579 euros)[61] to several thousand euros for each day of breach[62]. France has especially large penalties and legal persons can be fined up to 1.5 million euro.[63]

Such disparities and different approaches to data protection can cause several issues in terms of cooperation and competences of national MS in cross-border situations. Data controllers can choose to establish themselves in a MS which has more relaxed legal norms, thus furthering forum shopping. Additionally, following *Weltimmo*, one violation can be investigated and penalised in different MS, thus applying different data protection laws and reaching different conclusions. This can fail to ensure uniform application of EU law and the duty of sincere cooperation as well as creating lack of legal certainty. Moreover, as interpretations of violations vary, the same violation can be interpreted as a criminal offence or just administrative liability. This aspect will be analysed in more detail in Chapter 3.2.

1.3. Competent EU and MS institutions and bodies

1.3.1. European Commission

The European Commission is the executive body of the EU. As such it is responsible for proposing legislation, adopting new agreements, implementing EU policies and managing overall operations of the EU. The duties, obligations and competences of the Commission are established in Article 17 of the TEU. In terms of personal data protection, the European Commission provides proposals for new legislative acts in data protection, serves as the communicator with third countries, negotiates agreements concluded with third countries and adopts adequacy decisions.[64] For example, the Commission is the body which proposed the newly adopted General Data Protection Regulation and which communicated with the United States of America over the new framework for data transfer outside the EU, following the invalidity of the "safe harbour" regime. According to Article 25 of the Data Protection Directive, the Commission plays a very important role in establishing the framework for personal data transfer outside the EU.[65]

The Commission has the power to commence infringement proceedings against a MS in case of breach of EU data protection rules. This power has been

---

[61] *Supra* note 57.
[62] In the case of Belgium, where the national DPA administered a daily fine of EUR 200,000 to Facebook for noncompliance with national data protection rules. See Commission for the Protection of Privacy of Belgium. Judgment in the Facebook case. Available at: https://www.privacycommission.be/en/news/judgment-facebook-case. Last visited on 10 March 2017.
[63] *Supra* note 57.
[64] M. Kuschewsky. "European Union" in *Data Protection & Privacy. Jurisdictional comparisons*, p. 262.
[65] According to Art. 25(4) of the Data Protection Directive, the Commission has the competence to determine if a third country can ensure adequate levels of protection and Art. 25(4) sets that the Commission can enter into negotiations with that third country, if necessary.

exercised mostly in cases regarding MS failure to ensure complete independence of the national DPA, as required by the Data Protection Directive.[66] Additionally, the Commission has the power to evaluate if third countries can ensure adequate levels of data protection, thus creating the so-called "white list" of states, where the level of data protection is in line with EU law requirements.[67] Once the Commission has issued a decision on the level of protection, MS are required to comply with it. Nevertheless, following the CJEU ruling in *Schrems* national DPAs have the discretion to review Commission decisions if a claim is brought disputing the credibility or legality of the decision.[68] This was done by the German DPAs, which collectively adopted the view that other grounds for transfer of personal data outside the EU had to also be considered invalid and contradicted the position of the Commission.[69]

Under the newly adopted General Data Protection Regulation, the Commission

> obtains extensive policymaking powers through the possibility of adopting delegated acts and implementing measures in numerous instances, including by specifying standard forms, procedures and mechanisms.[70]

Changes following adoption of the General Data Protection Regulation will be analysed in Chapter 3.3.

1.3.2. National Data Protection Agencies

The requirement for setting up a national DPA is established in both primary and secondary EU law. Article 16(2) of the TFEU and Article 8 of the Charter both refer to the requirement for an independent national authority. In addition, Article 28 of the Data Protection Directive sets the specific obligation for MS to create such authorities. The administrative framework can be specified by the MS themselves, so there are many differences in the setup, management and running of national DPAs.[71] It can be said that the national DPAs are a governmental institution between the EU and MS, ensuring protection of both EU law and national law, while nevertheless remaining independent. Their position can be considered hybrid, as they are attached both to the national legal system as well as that of the EU.[72]

Article 28(3) sets the powers of national DPAs. First, they have the power to investigate claims, collect information and require access to data in order to perform

---

[66] For example, CJEU case C-518/07, *European Commission v Federal Republic of Germany*, EU:C:2010:125; CJEU case C-614/10, *European Commission v Republic of Austria*; CJEU case C-288/12, *European Commission v Hungary*, EU:C:2014:237.
[67] *Supra* note 64, p. 272.
[68] CJEU case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, EU:C:2015:650, para. 65-66.
[69] C. Ritzer, C. Zieger, D. Ashkar, M. Evans. "German Data Protection Authorities Suspend BCR approvals, question Model Clause transfers." Available at: http://www.dataprotectionreport.com/2015/10/german-data-protection-authorities-suspend-bcr-approvals-question-model-clause-transfers/. Last visited on 10 March 2017.
[70] *Supra* note 64, p. 263.
[71] P. Schütz. "Comparing formal independence of data protection authorities in selected EU Member States". Available at: http://regulation.upf.edu/exeter-12-papers/Paper%20265%20-%20Schuetz%202012%20-%20Comparing%20formal%20independence%20of%20data%20protection%20authorities%20in%20selected%20EU%20Member%20States.pdf Last visited on 10 March 2017.
[72] Hijmans, 2016, p. 287.

their supervisory duties.[73] Second, DPAs have effective powers of intervention, such as issuing opinions (also authorizing data processing, if required), ordering the blocking of data processing, erasure or destruction of data or any other temporary or permanent ban on processing for the controller, as well as referring matters to national political institutions.[74] Third, the Data Protection Directive gives national DPAs the power to engage in legal proceedings when there have been violations of national data protection norms or bring violations to the attention of judicial authorities.[75]

Article 28(1) of the Data Protection Directive sets the obligation to ensure the independence of national DPAs. Independence is a crucial aspect in data protection regulation in the EU, as it is also present in Article 8 of the Charter as well as in Article 16(2) of the TFEU. It is further emphasized by the CJEU in multiple cases, where the court has strictly interpreted this provision stating that the principle of independent national DPAs is crucial. In *Commission v Germany*, the Court analysed if the state's supervision of a DPA which monitored the processing of non-public sector data in a specific region is an intrusion and violation of the independence principle. The CJEU concluded that this principle

> precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.[76]

Thus, the Court has clearly indicated that national DPAs must be independent in all aspects, in order to guarantee that their performance and decisions are not influenced by external actors. In this case the CJEU affirmed that state intervention is contrary to the requirement of independence set in Article 28(1) of the Data Protection Directive. A similar conclusion was derived in *Commission v Hungary*, where the Court assessed whether removing the Hungarian Data Protection Supervisor from his position before the expiry of his term is considered a breach of the requirement of independence according to Article 28(1) of the Data Protection Directive. Here the CJEU set that such action too should be considered a violation of the requirement of independence as

> the threat of such premature termination to which that authority would be exposed throughout its term of office could lead it to enter into a form of prior compliance with the political authority, which is incompatible with the requirement of independence.[77]

This case law confirms the CJEU's position on the strict requirement of independent national DPAs. Only with a high level of independence can the right to personal data protection be ensured throughout the EU, without threats of intrusion from the state or political authorities. The requirement of independence is one of the main issues which arises when discussing the competences and level of cooperation between

---

[73] Data Protection Directive, Art. 28(3).
[74] *Ibid*.
[75] *Ibid*.
[76] CJEU case C-518/07, *European Commission v Federal Republic of Germany*, para. 30.
[77] CJEU case C-288/12, *European Commission v Hungary*, para. 54.

national DPAs, national parliaments and EU institutions. This aspect will be analysed in detail in Chapter 3.

Clearly, national DPAs play a crucial role in the area of personal data protection in the EU. MS are obliged to ensure the existence of DPAs and EU primary law establishes them as bodies of a constitutional nature. This means that DPAs have to ensure cooperation between the EU and their respective national institutions, as well as cooperate with each other. This duty is also stressed by the CJEU and further emphasized in the General Data Protection Regulation, as discussed in Chapter 3.

1.3.3. CJEU

As the CJEU is one of the fundamental institutions of the EU and by itself could be a subject of an article, the author will analyse only the role of the CJEU in terms of personal data protection and its contribution in ascertaining the competences of national and EU institutions and bodies.

Professor Hijmans has set three main functions of the CJEU in matters of personal data processing, deriving them from Sweet's three functions of the constitutional role.[78] Firstly, as Article 19(1) of the TEU sets, the CJEU serves as the interpreter of EU legal norms and ensures their uniform application. It acts as a constitutional court which balances the relationship and powers between the EU and MS, thus developing constitutional principles of judicial review.[79] So the Court has the obligation to ensure that legal norms are interpreted correctly, in line with fundamental rights and general principles of EU law.

Secondly, the CJEU ensures that MS are committed to their integration according to the Treaties, meaning that the Court ensures that MS comply with their obligations under EU law.[80] This can be seen in many personal data processing cases, for example *ASNEF and FECEMD*, where the Court precluded a MS from introducing additional provisions on legitimate grounds for personal data processing, which would be contrary to the Data Protection Directive.[81]

Thirdly, the CJEU is an "intermediary" in cases, when the EU or MS are overstepping their competences or introducing legal norms which are outside their competence. For example, this could be seen in *Digital Rights Ireland*. In this case, the Court was asked to evaluate a certain provision of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on 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)[82]*.* Instead, the Court set

---

[78] Hijmans, 2016, p. 169.; S.A. Sweet. "The European Court of Justice" in P. Craig, G. de Burca. *The evolution of EU law.* 2nd edition. Oxford; New York: Oxford University Press, 2011, p. 121.
[79] Hijmans, 2016, p. 169.
[80] *Ibid*.
[81] CJEU joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, EU:C:2011:777, para. 48-49.
[82] 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

that this Directive as such is contrary to Articles 7 and 8 of the Charter and declared it invalid as the EU legislator had "exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter." [83] The Court's role as an intermediary could also be seen in *Weltimmo*, where the Court established the jurisdiction of national DPAs if a violation involves more than one MS data protection rules.[84]

Given that the Data Protection Directive is a rather outdated law, the CJEU has in recent years served as gap-filler in order to address modern problems. This is a very positive aspect as personal data processing is an area which develops day by day. It is crucial that a powerful institution such as CJEU can ensure legal certainty and effective judicial review of new problems, thus taking the role of an activist in personal data protection. Presumably, the Court will need to take this role also in the future following implementation of the General Data Protection Regulation. Given that law-making in the EU is not a very speedy process, inevitably the legislator will not be able to address new problems associated with means of data processing, new technologies and new businesses in short order. Thus, the CJEU will need to address these problems by interpreting new legal norms.

1.3.4. European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) is an independent European supervisory authority, established in 2004 in accordance with Article 286 of the Treaty establishing the European Community [85] and derives its legal basis in Regulation 45/2001. Even though the EDPS is an important EU body in the area of data protection, it is an internal EU body which concerns personal data protection within EU institutions. Indeed, it acts as the DPA of the EU as an administrative body. Thus, as the purpose of this research is to analyse competences between EU and national institutions, the actions and competences of the EDPS will only be analysed from this perspective.

The EDPS was established in order to serve as an independent intra-EU DPA. As Regulation 45/2001 sets, the main tasks of the EDPS are to monitor data processing by EU institutions, ensure application of Regulation 45/2001 and any other EU legal norms that ensure protection of fundamental rights and freedoms in terms of data processing, and advise EU institutions, bodies and data subjects on all matters relating to personal data protection.[86] Additionally, the representative of the EDPS is a member of the Article 29 Working Party and thus participates in issuing opinions on various topics relating to personal data processing in the EU.

---

available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), *OJ L* 105, 13.4.2006, pp. 54–63.

[83] CJEU joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others*, EU:C:2014:238, para. 69.

[84] CJEU case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság,* EU:C:2015:639.

[85] Treaty establishing the European Community (Consolidated version 2002), *OJ C* 325, 24.12.2002, pp. 33–184.

[86] Regulation 45/2001, Art. 41(2).

The EDPS is subject to the same requirement of independence as national DPAs (see Chapter 1.3.2). Even though it has no direct link to national DPAs,[87] Article 46(f)(i) of Regulation 45/2001 sets the obligation to the EDPS to cooperate with national DPAs:

> to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body.[88]

The EDPS is a part of the institutional cooperation mechanism and represents the EU perspective and thus operates very closely with the Article 29 Working Party.[89] Moreover, if the European Commission has brought an infringement procedure to the CJEU, the EDPS serves as a supporter of the European Commission and EU position. The role of the EDPS in cooperation with the national authorities is analysed in detail in Chapter 3.1.2.

1.3.5. Article 29 Working Party

The Article 29 Working Party is an independent EU advisory body on personal data protection. As can be derived from the name, the Article 29 Working Party is established by Article 29(1) of the Data Protection Directive, which reads:

> The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up. It shall have advisory status and act independently.[90]

The Article 29 Working Party is composed of the representatives of national DPAs of each MS, as well as representatives of the EU data protection authority (EDPS) and a representative of the European Commission.[91] The main tasks of the Working Party are set in Article 30 of the Data Protection Directive as well as the Rules of Procedure of the Working Party[92] and Article 15(3) of the e-Privacy Directive.

The first task, set in Article 30(1)(a) of the Data Protection Regulation is to

> examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures,[93]

thus giving explanations and interpretations of the provisions of the Data Protection Directive so as to ensure uniform application. Next, the Working Party must give opinions to the European Commission regarding the "level of protection in the Community and in third countries"[94]. The Working Party issues opinions regarding the level of personal data protection in the EU as well as any third country, which is necessary, for example, for a data controller in order to ensure that transferring data

---

[87] Hijmans, 2016, p. 353.
[88] *Supra* note 86, Art. 46(f)(i).
[89] *Supra* note 87, p. 354.
[90] Data Protection Directive, Art. 29(1).
[91] *Ibid*, Art. 29(2).
[92] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. Rules of Procedure. Available at: http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf. Last visited on 10 March 2017.
[93] Data Protection Directive, Art. 30(1)(a).
[94] *Ibid*, Art. 30(1)(b).

to a third state is safe and in line with EU standards. Additionally, the Working Party is an advisory body which gives advice to the Commission on amendments to the Data Protection Directive or any other legal norm regarding personal data protection and ensuring observance of rights and freedoms of natural persons regarding personal data processing.[95] Furthermore, the Working Party also issues opinions on codes of conduct prepared at the EU level.

This institution gives opinions and communications on topical data protection issues, as well as interpreting and clarifying EU data protection legislation. Given that it is similar to a forum of representatives of national DPAs and EU data protection institutions, it serves as a guiding institution in all matters related to data protection. The core objectives of the Working Party are to (a) provide expert opinion on matters relating to data protection from MS level to the Commission, as well as provide such opinions to EU institutions and bodies and the general public, (b) promote uniform application of the norms envisaged in EU legal norms regarding data protection and encourage cooperation between national DPAs, (c) advise EU institutions on measures which could affect the rights and freedoms of persons regarding the processing of their personal data.[96]

Even though the opinions of the Working Party are not binding, they are well used by the European Commission, the CJEU and national DPAs. For example, the Latvian DPA uses the guidelines and opinions of the Working Party for their own information materials, such as publications and explanatory notes on several data processing concepts.[97] Thus, this institution's opinions are crucial in shaping the existing data protection area of EU law and ensuring uniform application of EU data protection rules in MS. But the legal setup and non-binding nature of the Working Party can cause certain issues in relation to cooperation between national and EU data protection authorities. This will be further analysed in Chapter 3.1.2.

[95] *Ibid*, Art. 30(1)(c).
[96] Tasks of the Article 29 Data Protection Working Party. Available at: http://ec.europa.eu/justice/data-protection/article-29/files/tasks-art-29_en.pdf. Last visited on 10 March 2017.
[97] Datu Valsts inspekcija (Latvian Data Protection Agency). Publications. Available at: http://www.dvi.gov.lv/lv/jaunumi/publikacijas/. Last visited on 10 March 2017.

2. DIVISION OF COMPETENCES IN THE AREA OF DATA PROTECTION

2.1. Concept of shared competence in EU law

The EU as a legal formation is based on attributed competence, meaning it can act only as far as the Treaties allow it. As set in Article 5(2) of the Treaty on European Union (hereinafter – TEU):

> Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.[98]

So, the EU can only act so far as MS have given it the competence to act. In general, the TFEU provides for three types of competences for the EU – exclusive competence, shared competence and supporting / co-ordinating competence. In this research, the focus will be on shared competence, as personal data protection falls within this area.

Article 2(2) of the TFEU prescribes that

> When the Treaties confer on the Union a competence shared with the Member States in a specific area, the Union and the Member States may legislate and adopt legally binding acts in that area. The Member States shall exercise their competence to the extent that the Union has not exercised its competence. The Member States shall again exercise their competence to the extent that the Union has decided to cease exercising its competence.[99]

This Article defines what is understood as shared competence in the area of EU law. It is considered that all matters which are not specified in Articles 3 and 6 of the TFEU (dealing with exclusive and supporting/coordinating competences, respectively), shall be considered to fall within the area of shared competence.[100] As Craig has put it, "shared competence is a default position in the Lisbon Treaty"[101]. In the particular case of data protection, Article 16 of the TFEU has provided that the EU legislator shall have the competence to legislate in certain areas of data protection, leaving MS with some room for manoeuvre. Moreover, as data protection is not listed as an area of exclusive or supporting/coordinating competences, it is considered as a shared competence. Data protection is a

> competence which the Union shares with the Member States and which it exercises with due regard for the principles of subsidiarity and proportionality.[102]

As Article 2(2) of the TFEU states, the MS possibility to act is pre-empted by actions already taken by the EU, meaning the MS may act only so far as the EU has not

---

[98] Consolidated version of the Treaty on European Union (TEU), *OJ C* 326, 26.10.2012, pp. 13–390, Art. 5(2).
[99] TFEU, Art. 2(2).
[100] P. Craig. *EU Administrative Law. 2nd edition.* Oxford; New York: Oxford University Press, 2012, p. 377.
[101] P. Craig, G. de Burca. *EU Law. Text, cases and materials.* 6th edition. Oxford; New York: Oxford University Press, 2015, p. 102.
[102] Hijmans, 2016, p. 117.

acted. In fact, there are several different ways in which MS and the EU may share competence to act. Firstly, a MS will only lose its competence to act if the EU has exercised its competence to act. It is said, "legislative instruments of the Union, once adopted and entered into force, have a blocking effect on the competences of the Member States"[103]. Thus, once the EU acts (i.e. adopts legislation in a certain area), the MS lose their competence to act. Any national measure adopted by a MS will thus be invalid. As in the case of data protection, the EU has adopted the Data Protection Directive, so that MS are precluded from adopting such legislative acts on data protection which would be contrary to this directive, of course with the exception of measures needed to transpose it into their national law. Nevertheless, MS competence is lost only to the extent that the EU has exercised its competence. As set in Protocol No 25 of the TFEU,

> When the Union has taken action in a certain area, the scope of this exercise of competence only covers those elements governed by the Union act in question and therefore does not cover the whole area.[104]

Thus, the EU may only act to a certain extent, leaving MS with the possibility to act further. For example, the EU legislator may harmonize a particular area only minimally or only in a certain aspect, thus leaving the MS with room for action in that particular area.[105] Such is the case of the Data Protection Directive, which gives the MS the possibility to adopt stricter national norms. As the CJEU has set in *Lindqvist* and *Huber*:

> The approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.[106]

Nevertheless, the Court has set that MS are precluded from "adding" norms, which would be contrary to the Data Protection Directive – they may only "provide for a mere clarification"[107] of the principles set in the directive.

Further, the EU may (if the provisions of the TFEU provide for it) adopt further legislation in a particular area or, alternatively, cease the exercise of competence altogether. In that case, the MS would regain all competence in the particular area. As of adoption of the General Data Protection Regulation, it can certainly be expected that the MS will only lose more competence in the area of data protection.

Shared competence must be carried out in respect to principles of subsidiarity and proportionality, as well as the principle of sincere cooperation. These principles provide for the pathway which has to be followed when exercising shared competence.

---

[103] *Ibid*, p. 121.
[104] Sole Article of the Protocol (No 25) of the TFEU on the exercise of shared competence, *OJ C* 326, 26.10.2012.
[105] P. Craig. *EU Administrative Law,* p. 379.
[106] CJEU case C-101/01, *Criminal proceedings against Bodil Lindqvist*, para. 95; CJEU case C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, EU:C:2008:724, para. 50.
[107] CJEU joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, para. 35.

2.1.1. Principle of subsidiarity and proportionality

There are several basic principles which MSs and the EU must observe when dealing with issues that fall within shared competence. When exercising powers to act in an area of shared competence, the EU and MSs must observe the principles of subsidiarity and proportionality. As established by Article 5(3) of the TEU,

> Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.[108]

So, the principle of subsidiarity provides that EU will abstain from any legislative action if the objectives of this legislation can be achieved more effectively at MS level.

This Article must be read in conjunction with Protocol No 2 of the TFEU, which sets how this principle must be applied. The principle applies to draft legislative acts only and prescribes that the European Commission must consult widely before proposing legislative acts.[109] Most importantly, this principle provides that the Commission has to send all legislative acts to MS parliaments simultaneously as sending them to other EU institutions.[110] The MS are thus given the opportunity to send a reasoned opinion to the President of the European Commission, the European Parliament or the Council, if they consider that the proposed legislation does not comply with the principle of subsidiarity.[111] Moreover, the EU institutions mentioned must take this reasoned opinion into consideration.[112] Ultimately, if the European Parliament by a majority of votes or 55% of the members of the Council decides that the legislation is contrary to the principle of subsidiarity, the legislation will not be given further consideration.[113] It is considered that the Commission takes seriously MS concerns of violations of the subsidiary principle, especially those of more powerful MS.[114]

Additionally, if a legislative act has been adopted, but a MS still considers it to be contrary to the subsidiary principle, according to Article 8 of Protocol No 2 of the TFEU, a MS has the possibility to bring an action to the CJEU. Nevertheless, it is considered that such actions are rarely successful due to "the low-intensity judicial review"[115] of the CJEU.

Subsidiarity goes hand in hand with the principle of proportionality. Article 5(4) of the TEU sets

---

[108] TEU, Art. 5(3).
[109] Protocol No 2 of the TFEU on the application of the principles of subsidiarity and proportionality, *OJ C* 326, 26.10.2012, Art. 2.
[110] *Ibid*, Art. 4.
[111] *Ibid*, Art. 6.
[112] *Ibid*, Art. 7(1).
[113] *Ibid*, Art. 7(3)(b); P. Craig, G. de Burca. *EU Law. Text, cases and materials. 6th edition.* p. 98.
[114] P. Craig, G. de Burca. *EU Law. Text, cases and materials,* p. 103.
[115] *Ibid*, p. 101.

> Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.[116]

Thus, actions taken by the EU must be in line with, and not overstepping, the aims which have to be achieved. This principle is established as a general principle of EU law by the CJEU. When elaborating on this principle, the Court has set that

> When there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued.[117]

In order for the CJEU to evaluate whether the principle of proportionality is observed, the relevant interests must be identified and some value must be attributed to them.[118] Further, the Court would have to assess if the measures adopted were appropriate to achieve the aims and could the aim have been achieved by adopting less onerous measures.

As mentioned above, the MS have the right to send a reasoned opinion to the President of the Commission, the Parliament or the Council if they consider that a legislative act is not in accordance with the principle of subsidiarity. Nevertheless, the MS are not provided with the right to submit arguments on observance of the principle of proportionality. According to Craig, this is regrettable, as division of these principles is difficult and it is hard to see the reasoning why MS should be afforded the right to argue on subsidiarity but lack the right to submit their opinions on proportionality.[119] Further the author will analyse the principle of sincere cooperation, which is crucial when exercising shared competences and also when cooperating between national and EU institutions.

2.1.2. Principle of sincere cooperation

One of the general principles of EU law is the principle or duty of sincere cooperation, which is established by Article 4(3) of the TEU

> Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks, which flow from the Treaties. The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union. The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure, which could jeopardise the attainment of the Union's objectives.[120]

Thus, MS are free to act in so far as the Treaties allow it, but in all circumstances MS must mutually assist each other, ensure the fulfilment of common EU goals and abstain from any actions which could hinder achievement of these goals. Even though this principle is very often associated with exercise of competences, for example, when concluding an international agreement, it has general application and

---

[116] TEU, Art. 5(4).
[117] CJEU case C-331/88, *The Queen v Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa and others*, EU:C:1990:391, para. 13.
[118] P. Craig. *EU Administrative Law*, p. 591.
[119] *Ibid*, p. 394.
[120] TEU, Art. 4(3).

has to be observed by the EU and MS in all their actions. It has been said that, as such, "it operates as a constitutional safeguard for the protection of the EU's interests"[121].

This principle prescribes that the national and EU institutions and bodies must work together when achieving EU aims and tasks. The CJEU has expressed that this is an expression of solidarity within the system of the EU.[122] This principle encompasses several duties of a MS. First, MS must implement EU legislation and secure its legal certainty in order for citizens to be able to identify their rights under EU law.[123] Second, MS must ensure that EU law is being observed and have to ensure effective legal protection of EU legal norms. This obligation can only be set aside if such policing of EU law would create public disorder or it would be contrary to the fundamental rights or civil liberties of the MS.[124] Third, the MS are obliged to penalise infringements of EU law, similarly as they would penalise any infringements of national laws. And finally, MS must take all necessary action to implement EU law and, if there are any obstacles in doing so, must notify the European Commission of such circumstances.

Moreover, the CJEU has expressly set that national courts are under the obligation to interpret national law which gives effect to a EU directive in such a way as to ensure achievement of the aims of EU legislation.[125] This is known as the *Marleasing* principle, stemming from a CJEU case, where the Court set:

> In applying national law, whether the provisions in question were adopted before or after the directive, the national court called upon to interpret it is required to do so, as far as possible, in the light of the wording and the purpose of the directive in order to achieve the result pursued by the latter.[126]

So in all circumstances, pursuant to the principle of sincere cooperation, MS are obliged to act and adopt decisions or other measures in a way which would be consistent with the aims of the EU and EU legislation.

By virtue of Article 13(2) of the TEU, this principle is applicable not only to MS actions towards the EU, but also among EU institutions. The European Commission, the Parliament, the Council and other institutions must cooperate with each other in order to attain common EU goals and objectives. As the CJEU has set in *European Parliament v Council of the European Union*:

---

[121] P. van Elsuwege. "The duty of sincere cooperation (Art. 4 (3) TEU) and its implications for the national interest of EU Member States in the field of external relations" (paper presented at the UACES 45th Annual Conference, Bilbao, 7-9 September 2015), p. 2.
[122] CJEU joined cases C-6/69 and C-11/69, *Commission of the European Communities v French Republic*, EU:C:1969:68, para. 16.
[123] D. Chalmers, G. Davies, G. Monti. *European Union Law: Cases and Materials. 2nd edition.* Cambridge, United Kingdom: Cambridge University Press, 2010, p. 224.
[124] *Ibid*.
[125] J.T. Lang. "Emerging European General Principles in Private Law" in Bernitz, U., Groussot, Z., Schuylok, F. *General Principles of EU Law and European Private Law.* Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2013, p. 72.
[126] CJEU case C-106/89, *Marleasing SA v La Comercial Internacional de Alimentacion SA*, EU:C:1990:395, para. 8.

> Inter-institutional dialogue, […], is subject to the same mutual duties of sincere cooperation as those which govern relations between Member States and the Community institutions.[127]

The principle of sincere cooperation is also crucial in the activities of national DPAs. As will be illustrated in more detail below, national DPAs have the obligation to cooperate with each other, to communicate and resolve data protection issues or violations collectively, if needed. Article 28(6) of the Data Protection Directive has specified this, setting that the principle of sincere cooperation applies also to independent national DPAs. As reconfirmed by the CJEU in *Weltimmo*:

> Supervisory authorities are to cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.[128]

Thus, DPAs must cooperate with each other, for example, when investigating a breach of data protection rights. But further analysis in Chapter 3 will show this is sometimes not the case.

It can be seen that the principle of sincere cooperation is a broad principle which is present in all relations between MS and EU institutions. It involves multiple obligations both for MS and the EU, which can also be seen in the field of data protection. The TEU sets the general obligation of sincere cooperation and, moreover, the Data Protection Directive specifically sets this obligation for national DPAs. The possible problems and particularities associated with this cooperation and competences will be discussed in more detail in the next Chapter.

[127] CJEU case C-204/86, *European Parliament v Council of the European Union*, EU:C:1995:91, para. 23.
[128] CJEU case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, para. 52.

3. COOPERATION AND OVERLAP OF COMPETENCES BETWEEN EU AND MS INSTITUTIONS AND BODIES IN DATA PROTECTION

The aim of this article is to analyse whether there is any overlap, confusion or uncertainty in terms of competences between national and EU institutions and their obligation and effectiveness of cooperation. In order to fulfil this aim, this Chapter will discuss the existing relationship between data protection institutions in the EU, the recent case law of the CJEU and future developments that will follow after the General Data Protection Regulation comes into force. The level of cooperation and possible overlap of competences can be analysed on two levels. The competences and cooperation between EU and national institutions will be analysed on the vertical level. Competences and cooperation between different national DPAs will be discussed on the horizontal level.

3.1. Vertical division of competences and cooperation

3.1.1. Division of competences and cooperation between the European Commission and national DPAs

As set in the previous Chapter, the competences of national DPAs are, firstly, established by Article 16 of the TFEU and, secondly, by Article 28 of the Data Protection Directive. In addition, this division is also governed by the general principles of shared competences in the EU. Thus, the issue of competences and cooperation on the vertical level must be analysed from this perspective as well as taking into account the special legal standing of national DPAs. As the analysis will show, some aspects are debatable, particularly the balance between the independence of national DPAs and the competences and influence of the Commission.

As indicated in Chapter 1.3.2, the independence of national DPAs is considered a crucial aspect when ensuring effective data protection in the EU. This has been expressly set in the primary law of the EU (Article 16(2) of the TFEU and Article 8(3) of the Charter), the Data Protection Directive as well as being continuously confirmed by the CJEU. When looking at the nature and legal setup of a national DPA it is evident that it stands between the EU and MS. Its mandate is set in both EU law and national law, so it balances between both of these governmental bodies, yet still retaining its independence. This hybrid nature and specific setup initially seems not to be in line with the general understanding of shared competences in EU law, which provides for a clear division as to when the EU or MS should act or abstain from action.

This relationship and competences was one of the issues discussed in the CJEU judgment in *Schrems*. In this case the CJEU analysed if national authorities are competent to review individual claims regarding a Commission decision on data protection (in this particular case – the Commission decision on "safe harbour"

principles[129]). The Court set that both the Commission and national DPAs are competent to find that a third country does or does not ensure an adequate level of protection for personal data.[130] But once the Commission has adopted such a decision, it becomes binding on the MS and their DPAs. So, as the general principles of exercise of shared competence sets, once the EU has acted in the particular area of law, the MS no longer have the right to act contrary to this action and must observe it. But in this particular case, the CJEU stated that

> a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.[131]

The Court went on to affirm that neither Article 8(3) of the Charter nor Article 28 of the Data Protection Directive excludes from the competence of national DPA the oversight of personal data transfers to a third country which has been the subject of a Commission decision.[132] Moreover, the Court has set that national DPAs can examine "with complete independence"[133] whether such Commission decisions are in line with the Data Protection Directive. So even if the Commission has the competence to adopt such decisions, MS do not lose their competence to review them and find them incompatible with the provisions of the Data Protection Directive. Indeed, if a Commission decision has been found invalid (only by the CJEU)[134], the MS regain their full competence in regard to the particular subject area and can adopt decisions on the particular matter. With this decision, the Court firmly set that independent national DPAs are a crucial aspect in ensuring effective data protection in the EU and their competences in ensuring data protection in EU should not be compromised by Commission decisions. But it could create confusion for a DPA in terms of how far it can go when disputing such a decision. Indeed, soon after *Schrems*, there was wide confusion or uncertainty within national DPAs, which reacted differently to the judgment. A German DPA issued a statement that it would no longer permit data transfer to the United States of America on the basis of standard contractual clauses[135], even though this ground for transfer was considered safe by the Commission[136]. This position was soon followed by other German DPAs.

---

[129] European Commission decision 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, *OJ L* 215 , 25/08/2000, pp. 0007-0047.

[130] CJEU case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, EU:C:2015:650, para. 50.

[131] *Ibid*, para. 53.

[132] *Ibid*, para. 54.

[133] *Ibid*, para. 57.

[134] CJEU joined cases C-188/10 and C-189/10, *Melki and Abdeli*, EU:C:2010:363, para. 54; CJEU case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, para. 61.

[135] Schleswig-Holstein Data Protection Agency. "ULD Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14." Available at: https://www.datenschutzzentrum.de/artikel/981-.html. Last visited on 10 March 2017.

[136] European Commission Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems). Brussels, 6.11.2015, COM(2015) 566 final, p. 14.

They agreed on the position that other grounds for data transfer as set in the Data Protection Directive do not ensure protection of the rights of Europeans as required by the CJEU and thus should not be used by data controllers.[137] There was no common ground or position in the EU, which can be burdensome and confusing, for example, for a data controller based in several MS and transferring data outside the EU.

In other cases the CJEU has set that a national DPA is not free from any parliamentary influence because the national parliaments have to appoint the management of the authority and define its power, as well as grant financing.[138] Even if in other aspects such as taking decisions or investigating violations it must "remain free from any external influence"[139], this freedom from influence is limited, as DPAs cannot be completely separated from both EU and MS oversight. The Commission has the competence to issue adequacy decisions and has to ensure consistent application and observance of EU law in MS. It is reasonable to assume that this can be done only if national DPAs communicate with the Commission and provide required information. Nevertheless, as the CJEU has set in *Commission v Austria*, the requirement to provide information is liable to subject a DPA to indirect influence from the executive body (i.e. the national government or the Commission), which is incompatible with the criterion of independence referred to in Article 28(1) of the Data Protection Directive.[140] The executive body has the right to exercise scrutiny in order to secure compliance of the authority with the general legal order, but it must not go beyond this, in order to safeguard the authority's independence.[141] So it can be argued that a fine line exists between the need for consistent application of EU data protection rules and possible indirect influence of national DPAs, which hinders their independence.[142]

As the Data Protection Directive requires, the DPAs must in some way cooperate with the Commission in order effectively to ensure personal data protection. But during this cooperation, the Commission should refrain from undue influence on the DPAs so as to avoid hindering their independence. This sensitive cooperation mechanism can be observed in the operations of the Article 29 Working Party, which is the main cooperation mechanism between the EU and MS in data protection. Even though the Commission is a member of the Working Party, it does not have any voting rights and cannot participate in adopting decisions or opinions.[143] Thus, the Commission can express its opinion and participate in meetings of the Working Party, but it cannot influence decisions by casting its vote. This ensures that the opinions and recommendations are not "guided" or unduly influenced by the power of the Commission and its agenda.

---

[137] C. Ritzer, C. Zieger, D. Ashkar, M. Evans. "German Data Protection Authorities Suspend BCR approvals, question Model Clause transfers".
[138] CJEU case C-518/07, *European Commission v Federal Republic of Germany*, para. 43.-44.
[139] *Ibid*, para. 25.
[140] CJEU case C-614/10, *European Commission v Republic of Austria*, para. 63.
[141] A. Balthasar. "'Complete Independence' of National Data Protection Supervisory Authorities". *Utrecht Law Review*, Vol. 9, Issue 3 (July) 2013, p. 37.
[142] Hijmans, 2016, p. 379.
[143] Data Protection Directive, Art. 29(3); Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. Rules of Procedure, Art. 17(1).

As can be seen from the considerations above, the division of competences in data protection and the special nature of national DPAs is a complex issue. There is a fine balance between what the Commission is competent to do, to what extent it can influence the DPAs' independence and when a DPA is competent to act or not. The legal norms in this respect are not very precise and detailed, so the competences and cooperation mechanisms have to be derived from the reasoning of the CJEU and assessed individually. As illustrated, this can cause uncertainties, confusion and formation of increasingly different approaches. This further confirms the need for a new regulatory framework, such as the General Data Protection Regulation, which would resolve these issues effectively. As Chapter 3.3 will illustrate, the new Regulation provides certain mechanisms in this regard.

3.1.2. Division of competences and cooperation between other EU institutions and national DPAs

As discussed previously, alongside the Commission there are several EU institutions and bodies which can facilitate cooperation between national and EU institutions. Such EU bodies as the Article 29 Working Party and the EDPS contribute to cooperation, as well as having certain competences in the area of data protection in the EU.

The Article 29 Working Party is the main EU body which serves as the cooperation point between national DPAs. As it is composed of heads of national DPAs as well as the EDPS and a representative of the Commission, it is considered to form the common viewpoint on EU data protection rules. By cooperating in terms of issuing a common opinion or a recommendation, the members of the Working Party are said to contribute to the uniform application of national rules adopted pursuant to the Data Protection Directive.[144] But some issues regarding the competences of the Working Party and its cooperation with national DPAs can create discrepancies.

According to the Data Protection Directive, the MS have the obligation to designate a representative who will be a part of the Working Party.[145] The requirement to be a part of the Working Party is set in EU law and MS cannot deviate from it. If a representative is not able to participate in a meeting of the Working Party, the MS must communicate this to the Working Party and designate an alternative member who can participate in the meeting but who does not hold voting rights.[146] So it has been established that during meetings, the viewpoint of all MS is expressed and heard. Such meetings create a forum for national DPAs, thus enabling them to exchange views, opinions, best practices and methods for ensuring uniform application of EU law. As each MS has only one vote, the opinions adopted equally reflect the view of all MS, not taking into account the economic status, population or other factors of the MS and putting all DPAs on the same level.

But, even though this seems to create very effective cooperation between national DPAs, there are some deficiencies. Firstly, the legal formation of the Article

[144] Hijmans, 2016, p. 350.
[145] Data Protection Directive, Art.29(2).
[146] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. Rules of Procedure, Art. 8 and Art. 17(2).

29 Working Party provides that it only has "advisory status"[147]. So, the Working Party has no competence to influence national DPAs or adopt a binding decision. The recommendations and opinions are non-binding; thus MS can choose not to follow them, in case they so wish. Existing EU legal norms do not provide for a requirement for MS to follow or in any way respect the recommendations or opinions of the Working Party. Indeed, it is possible that such requirement could compromise the essential condition for national DPAs to remain independent. This is also indicated as one of the problems in terms of DPA cooperation by the Working Party itself. It has set that

> the legal nature of the opinions and its influence on the national level should possibly by clarified and reinforced, while respecting the independence of DPAs.[148]

Furthermore, representatives of DPAs can abstain from actively participating in adoption of opinions.

In order to illustrate the negative effects of lack of clear cooperation mechanisms and binding nature of the recommendations, the case of the Google privacy issue investigation has to be mentioned. In 2012 Google announced a new privacy policy, which concerned national authorities. In order to examine the issue, the Working Party set up an *ad hoc* solution and asked the French DPA to take the lead role in investigating the matter.[149] The investigation was informal and Google participated only on a goodwill basis. But once the initial investigation was complete, Google did not react to the initial findings and requests of the Working Party, as it did not have a binding nature.[150] Thus, in order to persuade Google to change its privacy policy, the investigations were continued internally by the national DPAs of France, the Netherlands, the United Kingdom, Spain and other MS. These DPAs were said to cooperate and share information and findings among each other,[151] and the process resulted in several MS fining Google for breach of national data protection rules. Findings and fines differ among MS, as the investigations were conducted on the basis of respective national data protection rules. So even though some MS imposed a fine and requested compliance, this case illustrates the adverse effects of lack of a binding nature of opinions of the Working Party. Even though the Working Party was the initiator of the investigation and communicated the findings to Google, this was not taken into account, as there was no legal basis for requesting compliance. The Working Party can address an issue and bring it to the agenda of national DPAs but it does not have the competence and effective cooperation mechanisms which would ensure EU-wide compliance. Moreover, national DPAs are not required by any norms to react to issues raised by the Working Party. Indeed,

---

[147] As set in Data Protection Directive, Art.29(1).
[148] Article 29 Working Party. Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC, Ref. Ares(2011)444105 - 20/04/2011, p. 6.
[149] Article 29 Data Protection Working Party letter to Google, Brussels, 16.10.2012. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf Last visited on 10 March 2017.
[150] D. Kloza, A. Moscibroda. "Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law". *International Data Privacy Law*. Vol. 4, No. 2 (2014), p. 126.
[151] *Ibid*.

although Google's privacy policy was applicable to all EU MS, nevertheless, only few authorities pursued an investigation and imposed fines.

Even though there is no strict requirement to follow decisions and participate actively in meetings, MS tend to follow the recommendations of the Working Party. It can be said that by cooperating with this EU body, the MS are fulfilling their duty of sincere cooperation as the Working Party strives to establish uniform application of EU law and EU interests. Recommendations usually contain very clear and descriptive mechanisms on how to solve certain issues (for example, following a new CJEU judgment, which establishes a new obligation or duty for DPAs) as well as detailed explanations of certain terms. So, national DPAs are given clear instructions and they do not have to invest their own resources in this aspect. Moreover, as these recommendations can be in line with EU objectives, the MS can apply them in order to ensure uniform application of EU law and avoid possible risks of failure to comply with EU law. Thus, the actions of the Working Party diminish the risk of failure to observe the principle of sincere cooperation.

As a member of the Article 29 Working Party and as a EU internal DPA, the EDPS also contributes to enhancing cooperation. This EU body is competent to address data protection issues and violations in EU institutions but does not have competence to adopt decisions or recommendations that would affect national DPAs. Indeed, it should be viewed similarly to any of the 28 independent national DPAs in terms of its competence to affect other national DPAs. Neither the procedure for appointing heads of the EDPS nor its management procedure is linked to national DPAs.[152] But, as with any other national DPA, it has the general obligation to cooperate with other national authorities.[153] This obligation is equal to that of national DPAs and the EDPS Rules of Procedure[154] provide for specific action to be taken in this cooperation. Article 44(2) of the Rules of Procedure set that the EDPS shall exchange all relevant information, also information relating to best practices, as well as request national DPAs to exercise their powers and respond to such requests from DPAs, develop and maintain contacts with members of national authorities and cooperate with any other EU joint supervisory authorities (for example, the Schengen Information System).[155] This requirement to cooperate is more elaborate than that of the Data Protection Directive. But, as the EDPS should be viewed as an independent DPA, it does not have a specific mandate to enhance cooperation between the EU and MS in terms of data protection.

As opposed to the legal requirement for national authorities, the EDPS has the obligation to participate in actions of the Article 29 Working Party.[156] Contrary to the Commission, the EDPS has voting rights. As elaborated by the EDPS Rules of Procedure,

> [EDPS] shall contribute actively to the discussions and drafting of documents published by the Working Party which aim at providing a common interpretation of data protection legislation and giving expert advice to the

[152] Hijmans, 2016, p. 353.
[153] Regulation 45/2001, Art. 46(f)(i).
[154] Decision of the European Data Protection Supervisor of 17 December 2012 on the adoption of Rules of Procedure, *OJ L* 273 of 15.10.2013.
[155] *Ibid*, Art. 44(2).
[156] Regulation 45/2001, Art. 46(g).

> European Commission. In such cases, the EDPS shall put forward the Union perspective, where appropriate.[157]

So although the EDPS does not have any discretion in choosing the level of activity in meetings of the Working Party, it has a general duty of cooperation.[158] This sets the EDPS as an active promoter of the EU viewpoint on data protection and safeguards "legitimate and effective control of compliance with data protection rules"[159].

It can be said that other EU institutions and bodies such as the Working Party and the EDPS contribute to advancing cooperation between the EU and national authorities. The Working Party, as a forum for national DPAs, has the power to enhance cooperation between national and EU authorities. Nevertheless, it lacks reinforcement power and has no competence to issue binding recommendations or opinions. The EDPS has the obligation to cooperate with national authorities, but it operates as an independent DPA, thus it has no specific mandate to enhance cooperation between national and EU institutions. Following adoption of the General Data Protection Regulation, the setup and competences of the Article 29 Working Party will be changed, as it will be reincarnated into the European Data Protection Board. This aspect will be further analysed in Chapter 3.3.

3.2. Horizontal division of competences and cooperation

3.2.1. Division of competences of national DPAs

In order to analyse the level of horizontal cooperation and its particularities, it is first necessary to establish the division of competences between national DPAs. The theoretical background of MS competence in the area of data protection can be seen in Chapter 2, but for the purposes of this research it is important to assess in detail the horizontal division of competences among national DPAs.

The competences of national DPAs should be analysed from the perspective of cross-border issues. It is exactly cross-border situations or disputes where a clash or overlap of competences can arise and create problems in terms of effective protection of personal data. The clash of applicable law and competences of different national DPAs has been reviewed by the CJEU in *Google Spain* and *Weltimmo*. In both cases the CJEU was asked to evaluate if a national DPA is competent to review a certain issue and, if necessary, penalise the data controller for violation.

In *Google Spain*, the CJEU established that a data controller who is incorporated outside the EU but processed personal data in any of the MS through its establishment has to observe the data protection law of that MS.[160] Thus, the national DPA of that MS is competent to act in case such controller has possibly violated national data protection rules. A similar conclusion was derived in the later case of *Weltimmo*. In that case, among other questions, the CJEU was asked to establish whether a national DPA is competent to act even if, based on the criteria

---

[157] *Supra* note 154, Art. 45(2).
[158] H. Hijmans. "The European data protection supervisor: The institutions of the EC controlled by an independent authority". *Common Market Law Review*, (2006) 43, p. 1322.
[159] Hijmans, 2016, p. 354.
[160] CJEU case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, EU:C:2014:317, para. 58.

laid down in Article 4(1)(a) of the Data Protection Directive, the law of another MS is applicable.[161] So, in general, could the DPA of one MS act if the national data protection law of another MS would apply to the situation at hand? The Advocate General and the CJEU both concluded that the national authority has the competence to investigate any complaint it receives, "irrespective of the applicable law"[162]. But, if that national authority would conclude that the law of another MS applies, it would not be competent to impose penalties and would have to refer the case to the national DPA of that MS.[163] By doing so, the DPA would observe the obligation of sincere cooperation. This is an important conclusion for both national DPAs and data controllers. The DPAs are thus clearly given the possibility to investigate any possible data protection violations irrespective of the fact that the controller is registered in another MS. Data controllers have to take into consideration that their actions must comply with the data protection rules in each MS where they are "established".[164]

The *Weltimmo* ruling has set to emphasise the ruling in *Google Spain* in terms of national DPA competences. Previously, it was considered that a company can be established in one MS, operating in accordance with the data protection laws of that MS and other DPAs would not be competent to act. This setup was widely used by the big data controllers such as Facebook (located in Ireland and thus operating by the data protection rules of Ireland), Amazon (operating under the data protection rules of Liechtenstein) and others. Following *Weltimmo*, these companies, if they can be considered "established" in other EU MS, must also comply with national data protection laws of these MS. And, most importantly, any national DPA can examine and investigate their actions and find them in breach of their national data protection rules.

This is exactly what the Belgian DPA did in November 2015, when it required Facebook (located in Ireland) to cease the use of a special cookie which allowed collecting personal data of persons who had not logged into Facebook. The Belgian court stated that such activities could be considered as collecting personal data, which is contrary to Belgian national data protection laws as data subjects have not given their consent.[165] Moreover, the court set a fine of 250,000 euro per day if Facebook failed to cease processing such data. It is important to stress that these actions by Facebook had previously been investigated by the Irish DPA and found to be in compliance with local data protection law.[166] Moreover, the Belgian DPA did not cooperate with the Irish DPA when concluding the investigation, possibly refraining from such actions as the viewpoint or national legislation differed in this aspect. Following the judgment, Facebook complied and started requiring users to log into Facebook to view certain content, which is what the court had required.

---

[161] Opinion of Advocate General Cruz Villalón on CJEU case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, EU:C:2015:639, para. 44.
[162] CJEU case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, para. 54.
[163] *Ibid*, para. 57.
[164] The CJEU has expressly defined what actions of the data controller could result in it being considered established in a MS in accordance with the Data Protection Directive. CJEU case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, para. 29.-31.
[165] Commission for the Protection of Privacy of Belgium. Judgment in the Facebook case.
[166] Hijmans, 2016, p. 355.

Nevertheless, the DPAs of the Netherlands, France, Spain, Hamburg and Belgium issued a common statement requiring Facebook to "comply with these orders in all territories of the EU as a means of contributing to ensure consistency with the requirement"[167] of EU law. Thus, following the ruling in *Weltimmo*, DPAs are keen to ascertain their competences and act, even simultaneously.

It is evident that such practice is not very effective, as it can create considerable confusion. DPAs can be confused in terms of who is competent to do what. Moreover, there can be unnecessary confusion for data controllers and data subjects as to what legal resources they can rely on, not to mention the elevated expenses, required resources and increased administrative burden for DPAs as well as possible conflict of competences.[168] If several DPAs investigated the same operations that a data controller carried out in their MS, it is probable that they would all reach different conclusions, apply their national law differently and fail to apply EU law uniformly. Or, in the alternative, act similarly as the Belgian and Irish DPAs have done, avoiding cooperation and issuing completely different decisions. So, even though *Weltimmo* has given more power and in some way clearer competences to national DPAs, it has created confusion and uncertainty for data controllers and data subjects. The presence of multiple competent DPAs can render each DPA less independent as it could be influenced by the decisions of other DPAs. It is argued that such a setup

> risks generating a situation of uncertainty that can undermine the effective protection of data subjects' rights, frustrate the legitimate expectations of data controllers and, eventually, decrease the authoritativeness of the DPAs called to oversee the process of personal data.[169]

Additional risks from this arise in terms of cooperation between national DPAs. This aspect will be analysed in the next Chapter.

The issue of competences could be resolved with adoption of the General Data Protection Regulation, which would, firstly, ensure that there is only one data protection regulation in EU and, secondly, specifically provide for such one-stop-shop mechanism by creating a lead supervisory authority, which would administer all issues in relation to the specific data controller which was established in the MS. This new development will be further analysed in Chapter 3.3.

3.2.2. Cooperation between national DPAs

As established in the previous Chapter, the national DPAs should cooperate with each other in order to ensure effective data protection in the EU. But as further analysis will illustrate, this is in many ways a hard aim to achieve due to lack of precise legal provisions and clear cooperation mechanisms. So, even though the

---

[167] Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium. Available at: https://www.privacycommission.be/sites/privacycommission/files/documents/Common%20Statement%20Facebook%20-%20final%20-withOUT%20signatures.pdf. Last visited on 10 March 2017.

[168] P. Balboni, E. Pelino, L. Scudiero. "Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation", *Computer law & security review* 30 (2014), p. 394.

[169] *Ibid*, p. 396.

CJEU has set the obligation to the DPAs to cooperate, the current legal setup hinders it.

The obligation of horizontal cooperation is set in Article 28(6) of the Data Protection Directive. This Article sets that a DPA is competent to exercise its powers within its MS, it can be asked to do so by a DPA of another MS and DPAs must cooperate with each other "to the extent necessary for the performance of their duties"[170]. Even though this Article puts forward the obligation to cooperate, it does not however set the exact procedure or specifics for such cooperation. Indeed, this is also not stipulated in any other provision of the Data Protection Directive or any other EU legal act. This lack of legal framework for cooperation creates several problems and uncertainties, which will be discussed in detail further.

Presumably, the issue of cooperation can arise in situations when a data controller is established in more than one MS and the possible data protection breach is of a cross-border nature. In such a situation, pursuant to Article 28(6) of the Data Protection Directive, the DPAs of the respective MS should cooperate in order to investigate the matter fully. But, as set out above, DPAs operate under the national law of their MS, so there would not be a single application of law. The actions of the data controller could be considered a violation of data protection laws in one MS, but not in another. Or in the alternative, one authority could consider the situation as not violating national data protection laws or find other violations in the same situation. The Article 29 Working Party has set that such different application of data protection laws across the EU "could have serious ramifications for the credibility of the EU data protection framework, both within the EU and at a global level"[171]. This can also be seen from previous cases of cooperation between national DPAs, such as the case of Google privacy policy investigations analysed in Chapter 3.1.2. This illustrates the main problems of the currently existing EU data protection legislation and disparities among MS. It can be argued that such problems should not exist as MS are obliged to observe the duty of sincere cooperation, which also envisages the obligation to interpret national law implementing EU law as close to the aim and purpose of respective EU legislation. But in reality this may not be the case.

When looking at this situation further, it is clear that many practical implications could arise in the process of cooperation. As currently there is no framework on the procedure of cooperation, DPAs are free to establish it themselves. For example, the form of communication is not specified, thus MS could face difficulties choosing a legitimate way of communicating. This problem could be more evident if the situation involved more DPAs – how would communication be organized and who would ensure that all DPAs involved have access to the same information? As current EU norms do not provide for a specific mechanism, the DPAs are free to disagree and fulfil their obligation to cooperate in a manner most suitable to them. It is possible that a DPA would follow the requirements of national administrative law, but again, the possible clash of national legal norms is an issue. Indeed, it is possible that national administrative law prescribes that the official language of communication should be the national language. So, for example, a

[170] Data Protection Directive, Art. 28(6).
[171] Article 29 Working Party. Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC, Ref. Ares(2011)444105 - 20/04/2011, p. 5.

Latvian DPA would have to send a letter to a Danish DPA in Latvian. But this is clearly not effective and burdensome to the Danish DPA, who would then have to spend its resources on translation. And even if both DPAs would informally agree on communication in one language, the choice of language could be burdensome. Many similar practical issues remain unclear. For example, the time for providing information, the amount and format of information exchanged, methods of investigation, and so on. Respective national laws would regulate these issues, thus uniformity would be hard to obtain, if not impossible.

It should be considered that cooperation could also be hindered by national confidentiality obligations. Sharing information on investigation can include some personal data of the data subjects involved. Thus transferring this information to another authority should be done with due care, as the Data Protection Directive allows such actions, but does not regulate this aspect in detail.[172] Moreover, as the current legal framework stands, national DPAs do not have any specific requirements as to which other public authorities may receive this data and how should it be treated if the matter proceeds to litigation.

Further, the applicable legal norms do not provide for a specific obligation on DPAs to cooperate. The wording of Article 28(6) of the Data Protection Directive sets that "[e]ach authority *may* be required to exercise its powers by any authority of another Member State"[173] (emphasis added). This does not give a clear duty to a DPA to commence any action at the request of another DPA and only refers to the possibility to do so. But this obligation should be fulfilled as a principle of EU law, i.e. cooperation between DPAs should be regarded as an extension of the principle of sincere cooperation pursuant to Article 4(3) of TEU. Moreover, national DPAs should respect this obligation of cooperation as a reflection of federal good faith.[174]

In its advice paper, the Article 29 Working Party has also recognized the practical implementation of Article 28(6) of the Data Protection Directive as problematic and has proposed possible solutions for resolving problems. In this paper, the Working Party puts forward solutions as to how national DPAs should communicate and organise cooperation. Moreover, it suggests that the European Commission could consider developing rules or obliging a DPA to cooperate with other authorities and provide them with the necessary information, if the specific case could create significant repercussions at EU level and affect other authorities.[175] The problems illustrated above could lead to slow and burdensome cooperation and result in ineffective protection or further violation of a data subject's rights.

A study of effectiveness of cooperation between national DPAs and EU competition authorities has revealed that cooperation between DPAs could be more effective if, (a) there were a specific and binding legal basis with a structured and detailed set of rules for cooperation, (b) this legal basis would define forms of cooperation, its conditions and procedures and (c) it would include provisions on

[172] *Ibid*.
[173] Data Protection Directive, Art. 28(6).
[174] Hijmans, 2016, p. 364.
[175] *Supra* note 171, p. 4.

exchange of confidential information.[176] As Chapter 3.3 will illustrate, the EU legislator has also arrived at similar conclusions and tried to implement these aspects in the General Data Protection Regulation.

3.3. Future development of the General Data Protection Regulation

Even though this article has been based on the EU data protection law as it stands at the time of concluding this research, following adoption of the General Data Protection Regulation in May 2016, it is crucial to analyse future changes. By the end of May 2018, the EU MS will be bound by the General Data Protection Regulation and thus there will be only one data protection regulation throughout the EU. Among other novelties introduced, the General Data Protection Regulation will change the competences of both national and EU institutions and, moreover, create new data protection bodies. The author will briefly illustrate the main changes which the new Regulation has introduced, in terms of the issues and topics discussed in this article.

The new Regulation is the result of long and intensive deliberations between the EU and MS, in order to find the most suitable new legal mechanism for EU data protection. As the existing norms, especially the Data Protection Directive, did not successfully address the current issues and problems, a new uniform regulation was crucial. The Commission has set that one of the objectives of the new Regulation is to

> establish a "one-stop-shop" for data controllers in the EU; to ensure stronger powers and adequate levels of resources (to DPAs) for enforcement and control; to develop binding cooperation procedures and effective mutual assistance between DPAs; to rationalise the current governance system to help ensuring a more consistent enforcement.[177]

So, this Regulation addresses and tries to resolve these issues of DPA competence in cross-border issues as well as enhance cooperation by providing clearer and more precise mechanisms for it.

In regard to competences of national DPAs, the new Regulation introduces a new concept of the lead supervisory authority. As Article 56 of the Regulation sets,

> […] supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor […].[178]

This provision establishes the "one-stop-shop", where one national DPA would be competent to act and issue decisions, even if the data controller were also established in other MS. This mechanism has been encouraged and supported also by the Council of the European Union, which has said that this mechanism is needed

---

[176] D. Kloza, A. Moscibroda. "Making the case for enhanced enforcement cooperation between data protection authroties: insights from competition law", p. 135.
[177] European Commission. Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 SEC(2012) 72 final.
[178] General Data Protection Regulation, Art. 56(1).

> in order to arrive at a single supervisory decision, which should be fast, ensure consistent application, provide legal certainty and reduce administrative burden.[179]

This creates uniform application of data protection rules, legal certainty and clear expectations. It can be argued that this would create situations where a data controller would specifically choose to locate its main establishment in a more favourable MS; nevertheless, given that the data protection regulation will be mostly similar in all MS, it is not very relevant. It can be argued that the "one-stop-shop" mechanism gives DPAs the widest sense of independence; it puts all DPAs on the same level in terms of their skills, capacity and level of fairness.[180] Together with the more elaborate rules on cooperation, this mechanism should ensure that the provisions of the Regulation and EU law are applied consistently and uniformly, thus also fostering legitimate expectations. Even though some authors have argued that the new Regulation includes some provisions which could hinder the effective use of the "one-stop-shop" mechanism,[181] its real effectiveness will most likely show only with its implementation.

The new Regulation also includes specific provisions on cooperation between national DPAs and EU bodies. Detailed provisions of Chapter VII of the Regulation expressly deal with cooperation between national authorities, mutual assistance, joint operations and consistency mechanisms. For example, Articles 60 and 61 set specific obligations on supervisory authorities to cooperate effectively, free of charge, using standardized electronic forms, without delay and in a certain sequence of actions. So MS will be given clearer instructions on how to cooperate more effectively. The consistency mechanism is a new concept in data protection, which applies

> where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States.[182]

This concept is introduced in order to ensure uniform application of the General Data Protection Regulation by cooperation between national authorities and the Commission, when necessary.[183] In addition, the Commission is given the possibility to implement acts specifying the format and procedures for mutual assistance and arrangements for exchange of information between national and EU data protection institutions.[184] With these detailed provisions and mechanisms, the EU legislator has tried to address the existing problematic issues of cooperation and has taken into account the previous opinion of the Working Party on how to improve cooperation.

One of the biggest novelties of the new Regulation is establishment of a European Data Protection Board (hereinafter – EDPB). The EDPB will replace the Article 29 Working Party and be composed of representatives of the national

---

[179] Council of the European Union. Data protection: Council supports "one-stop-shop" principle, Luxembourg, 7 October 2013, 14525/13, (OR. en) Presse 403.
[180] *Supra* note 168, p. 396.
[181] For example, it is considered that the consistency mechanism of the new Regulation is liable to render the "one-stop-shop" mechanism useless. *Supra* note 168, p. 397.
[182] General Data Protection Directive, recital (135).
[183] *Ibid*, Art. 63.
[184] *Ibid*, Art. 61(9).

authorities and the EDPS.[185] The Commission will be able to participate in meetings, but will not have a voting right.[186] Similarly to national DPAs and the Working Party, the EDPB will be completely independent and will not be authorised by any other institution. The EDPB is established as a guardian of application of the new Regulation and will have the power to request the Commission to perform a multitude of activities in order to ensure effective and consistent application of the Regulation. The EDPB will also have competence to resolve disputes between national DPAs in order to foster the consistency mechanism. In such cases, decisions of the EDPB will be binding.[187] It is presumed that this setup should resolve the efficiency problems of the Working Party.

It is argued that, notwithstanding the elaborate provisions on cooperation and division of competences, the new Regulation may fail to achieve its aims of harmonization of EU data protection laws. This could happen due to the fact that the Regulation still leaves a lot of room for it to coexist with national norms, thus hindering the goal of harmonization.[188] Other authors indicate that the issue of exchange of confidential information is not specifically addressed.[189] Moreover, the historical perspective of personal data protection norms could also disrupt harmonization as, despite two decades of data protection in the EU, MS still hold differing opinions as to the objectives of the regime and the best means of achieving those objectives.[190]

By setting that the new legal instrument is a regulation rather than a directive, the EU legislator "significantly limits the margin of discretion of the Member States"[191]. Taking into consideration existing problems in terms of different legal norms in each MS and lack of clear legal mechanisms to ensure effective cooperation, the EU legislator has acted in accordance with the principle of subsidiarity and proportionality. The view that many cooperation and competence issues may be resolved more successfully on a EU level has been present for a long time and further encouraged also by the Working Party.[192] Furthermore, data protection as such

> can be better regulated at Union level, if only because of the inherent cross-border effects of the action, both within and outside the EU territory, in compliance with the second element of the principle of subsidiarity.[193]

The new Regulation can help achieve EU aims more effectively than MS could on a national level and increase trust in the EU as the guarantor of personal data protection in the EU.[194]

---

[185] *Ibid*, Art. 68(3).
[186] *Ibid*, Art. 68(5).
[187] *Ibid*, Art. 65.
[188] O. Lynskey. *The foundations of EU data protection law*, pp. 71.-72.
[189] D. Kloza, A. Moscibroda. "Making the case for enhanced enforcement cooperation between data protection authroties: insights from competition law", p. 129.
[190] *Supra* note 188, p. 88.
[191] Hijmans, 2016, p. 494.
[192] See Article 29 Working Party. Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC.
[193] Hijmans, 2016, p. 125.
[194] *Ibid*, p. 496.

CONCLUSION

When looking at the general concepts of personal data, the applicable legal norms as well as competent institutions, it is evident that the discrepancies in data protection regulations in MS are noteworthy. As data protection is a shared competence, the MS can adopt national data protection measures slightly differently, taking into consideration the overall aims and objectives of EU law and the particularities of both the Data Protection Directive and rulings of the CJEU. But the current EU legal framework lacks clear and precise norms on division of competences in particular cross-border situations and, moreover, does not provide guidance on cooperation mechanisms. Thus, both horizontal and vertical cooperation and division of competences can be hindered and rendered ineffective and burdensome.

When analysing cooperation on the horizontal level, it can be seen that there is a very thin balance between the Commission's competence to adopt decisions and overlook the application of EU law and the requirement for national DPAs' independence. It is not possible to determine which right stands above the other; thus that conclusion can only be reached by the CJEU when analysing a particular case. But such a lack of clear division and limits to the exercise of the competences of EU and national institutions can cause disputes and ineffective addressing of personal data violations. If a national DPA is not sure if it is competent to act or competent to review a data subject's claim, the rights of that data subject can be hindered. Moreover, if the Commission oversteps its competence when issuing a decision (as it had done with the "safe harbour" principles), the independence and competences of the national DPA are threatened. So, it is difficult to determine the level of cooperation between the Commission and national DPAs that would be in line with (a) the complete independence of national DPAs, (b) the competences of the Commission and DPAs as set in EU law and (c) the general EU legal system in terms of shared competences.

The situation is similar in relationship between the Article 29 Working Party and the EDPS. The Working Party creates a forum for MS to cooperate and exchange views on specific issues, deliberate and arrive at a common conclusion. But it does not have competence to bind MS or data controllers, so there is no obligation on MS to actively participate in its meetings and issuing of recommendations or opinions. Consequently, the recommendations and opinions do not have binding force and following them is a matter for the discretion of national DPAs. This aspect can hinder cooperation and uniform application of EU data protection norms. MS should nonetheless cooperate with the Working Party and follow its guidance in order to fulfil their duty of sincere cooperation. In addition, even though the Working Party (as a collective of several national DPAs) can investigate a possible breach, it has no competence to request compliance. With the current legal setup, this can be done only on a national level, when a national DPA concludes its own investigation and issues a decision. Furthermore, the EDPS has the obligation to cooperate with national authorities, but it operates as an independent DPA; thus it has no specific mandate to enhance overall cooperation between national and EU institutions.

The research shows that the division of competences and cooperation between national DPAs currently holds the most issues and possible causes for ineffective protection of personal data. Firstly, following recent judgments of the

CJEU, the competences of DPAs to act in certain matters are not expressly clear. It has been established that any DPA can investigate a claim raised by a data subject, irrespective of the location of the data controller. So, if a controller processes personal data in multiple MS, the DPAs of all of these MS are competent to review the controller's actions. Even though this seems to ensure greater observation of compliance with data protection norms, it can be confusing to the data subject and controller, it can elevate expenses and required resources for investigation, and result in different conclusions as well as conflicts of competences. Even though, theoretically, this should be resolved by mutual cooperation between national DPAs, the analysis shows that cooperation is far from effective.

EU data protection norms lack clear legal mechanisms to ensure effective cooperation between national DPAs. The law only stipulates the obligation to cooperate. Nevertheless, it does not give any tools to do it. Problems can arise on many levels, for example, in terms of highly practical issues such as time, language, form of communication, materials to be provided, and division of resources. Furthermore, even though DPAs can share their findings in investigations, these are based on national data protection rules and cannot be endorsed by other DPAs. So in a cross-border case, every DPA has to start its own investigation in accordance with national legal norms (both in terms of data protection and administrative or criminal procedure). The same problem could be addressed completely differently in each MS, depending on the particularities of national data protection laws and the competences of national authorities. This is clearly ineffective and does not provide for fast and efficient resolution of a problem and compromises legal certainty, uniform application of EU law and legitimate expectations. These issues clearly illustrate that the current legal framework for cooperation and division of competences in data protection is not effective and can create many obstacles for ensuring data protection in the EU.

With adoption of the General Data Protection Regulation, the legislator has confirmed that there is a pressing need for a new legal setup in EU data protection. Even though it will only come into force in 2018, the future prospects seem hopeful. The new Regulation strives to correct and address, among other issues, the main problems in regards to cooperation and competences of EU and national institutions. As the changes are significant, it is safe to say that the EU data protection world will be put on a new level of advancement.