The Rule of Law and EU Data Protection Legislation
Some Controversial Issues in light of the new EU General Data Protection Regulation

Toptchiyska, Denitza
New Bulgarian University

Corresponding Author: Denitza Toptchiyska, denitza.t@gmail.com

Abstract
The article aims to analyse the evolution of the EU data protection legislation against the rule of law standards related to quality of law, formal justice and protection of human rights, focusing on some recent controversial issues related to the application of EU data protection model to technological environment. The analysis looks into the concepts of data controller and data processor as they are essential for the allocation of responsibilities in the processing of personal data as well as for the identification of applicable legislation. Further it considers the right to be forgotten and the implementation of the balance test in cases when there are opposing rights and legitimate interests of the data subject and data controller. The analysis is made on the basis of the EU data protection legislation, that is currently in force, the Opinions of the Article 29 Working Party and the case law of the Court of Justice of the EU (CJEU), which provides guidance on the uniform interpretation of the data protection concepts at EU level. The article also takes in consideration the current reform in the field of data protection in the frames of which in 2016 the new General Data Protection Regulation has been adopted.

Keywords: the rule of law, data protection, data controller, the right to be forgotten

Introduction
The rule of law is a philosophical, political, and legal concept that has been adopted as a fundamental political and legal principle due to its importance in modern society. Complexity of its understanding is a result of the conceptual unity of ethical, political and legal elements which form the basis of a variety of definitions.
(Tamanaha, 2004, p.91). From the aspect of legal theory, the rule of law is a normative concept indicating the ideal for construction and functioning of the legal system. In this sense, it is a standard for assessing the quality of law that from analytical perspective is considered in contemporary theory as a dynamic system of principles and rules, general and individual that defines its own internal validity criteria.

The article aims to analyse the evolution of the EU data protection legislation against the rule of law standards, more specifically related to quality of law, formal justice and protection of human rights, focusing on some recent controversial issues related to the application of EU data protection model to the technological environment. The analysis looks into the concepts of data controller and data processor as they are essential for the allocation of responsibilities in the processing of personal data as well as for the identification of applicable legislation. Further it considers the right to be forgotten and the implementation of the balance test in cases when there are opposing rights and legitimate interests of the data subject and data controller. Finally the main problematic issues are outlined and commented.

The modern concept for the rule of law

The rule of law has different manifestations in the national legal systems due to specific political, cultural and legal traditions. In the modern society, however, the concept of the rule of law should respond to two major challenges. First, the trend towards strengthening of the importance of international and transnational law in the process of globalization, which is closely linked with the development of new technologies and the Internet. And second, it is necessary to develop a definition for the rule of law that is practicable and measured through specific indicators. With this purpose definitions of the rule of law have been adopted by United Nations (UN) (United Nations Security Council, 2004, par.6), the Council of Europe (CoE) (Council of Europe, 2011) and the European Union (EU) (European Commission, 2014).

The modern concept for the rule of law aims not only at limiting arbitrary political power, but also at creating legal certainty and predictability, protecting individual and human rights. The minimum standard of the concept is composed of formal and material (substantive) parts. The formal part includes a set of standards and
requirements for the quality of law based on the principles of formal justice. Their content is a projection of the main functions of law, namely to guide individuals’ behaviour and to balance their interests. The material (substantive) part of the minimum standard of the concept of rule of law requires the protection of individual rights and notably the human rights that are indispensable element of social justice. In this sense, the effectively functioning legal system is an indicator that the rule of law standards have been achieved.

The set of standards regarding the legal system forming the formal part of the concept for the rule of law is dynamic. The main standards that have evolved as mandatory elements of the formal aspect of the concept are generality, publicity, limiting the number of norms with retrospective effect, clarity, lack of controversy, feasibility, stability, consistency and compliance with the principle of proportionality. The formal aspect of the rule of law concept also covers requirements regarding the institutional mechanism of the legal system as separation of powers, limitations on discretionary powers and standards related to judicial procedures. The significance of these standards justifies their perception as separate abstract principles formulated in positive law.

The concept of the rule of law is closely associated with formal justice, the core of which is the idea of equal treatment (Hart, 2012, p. 157). Formal justice sets standards both with respect to legislative process and content of legal rules, as well as regarding their application. Limiting the concept of formal justice within the concept of procedural justice, which requires only correct application of the legal rules is a prerequisite for incorrect and restrictive understanding of the concept of the rule of law.

The material (substantive) part of the rule of law concept requires effective protection of individual rights and notably the human rights, as an indispensable component of the modern concept of social justice. In a recent report adopted by the Venice Commission (Council of Europe, 2016, p.45) collection of data and surveillance are considered as an area where the application of the rule of law standards is of high importance. Fast technological development and growing use of personal data require implementation of effective legal infrastructure in order to deal with the privacy and data security implications that are raised.
The evolution of EU data protection legal framework

In the second half of the 20th century the rapid progress of information and communication technologies (ICT) and the Internet provided the possibility to increase the amount of automated data processing. In turn this process created prerequisites for violating the privacy of individuals not only by the state but also by private entities and individuals and raised many legal and ethical issues. The regulation of ICT and the Internet is a result of a complex interaction between different social subsystems, institutions and forces, formed largely as a result of the specific context and culture (Gasser, U., 2014, p.16). In the context of technological innovation different jurisdictions adopt two basic approaches in regulating the digital space: first, development and introduction of new rules and second, application of existing legislation (Gasser, U., 2014, p.16).

The process of developing specific legal approach aimed to reconcile the free flow of information across countries with the protection of the fundamental rights and freedoms of individuals in particular their right to privacy with respect to the processing of personal data started in the international organisations. At the end of the 20th century UN, CoE, OECD and APEC adopted documents regarding data processing. Despite the common model on which the regulations are based, there are differences regarding the degree in which the right to privacy is protected.

The EU data protection legislation has been introduced following the Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data. In 1995 the EU Data Protection Directive has been adopted with the aim to ensure free flow of personal data between Member States and to protect the fundamental rights and freedoms of individual in particular their right to privacy (Directive 95/46/EC, art. 1 (1). The EU implemented a data protection model based on technology neutral concepts and principles whose application is not limited to a specific technological context and in this way avoids the risks of legislative gaps. However the EU data protection legislation faced the challenge to be often interpreted and modernised in order to respond to the implications that new technologies pose for the privacy of individuals in order to ensure a trusted environment.
The EU Data Protection Directive 95/46/EC as a legal instrument is the basis for harmonization of national data protection regulations of the EU member states. At EU level guidance on the uniform interpretation of the data protection regulation is provided by the Article 29 Working Party acting as an advisory body on data protection issues for the European Commission (Directive 95/46/EC, art. 30). At national level the supervisory authorities are responsible for monitoring the application of national data protection legislation. The judgements of the CJEU also have strong impact on the implementation of the data protection model in EU. As a result of a procedure for preliminary ruling related to the interpretation of the EU law, they have obligatory force inter partes, i.e. for the parties that initiated the procedure. At the same time, the judgments have also de facto erga omnes effect regarding the national courts in EU that are obliged to apply them (Judgment of the Court of Justice, Case 283/81 (October 6, 1982). When a new context raises any serious doubt as to whether the previous case-law may be applied in that instance, the national courts must bring a request before the CJEU for a new interpretation (Court of Justice of The European Union, 2012, par. 12).

The importance of protecting privacy of individuals with respect to the processing of their personal data in EU has been reinforced with the recognition of the data protection right among the modern third generation rights in the Charter of Fundamental Rights of the European Union (Art. 8 of the Charter). The Charter explicitly recognised the right to data protection of individuals in all aspects of life: private, public and professional. In 2010 the European Commission launched a strategy to strengthen EU data protection rules with the aim to protect individuals’ data in all policy areas, including law enforcement, while reducing administrative burden to business and guaranteeing the free circulation of data within the EU (European Commission, 2010).

In 2016 after a long process of consultations within the EU a new General Data Protection Regulation has been adopted (Regulation (EU) 2016/679). The Regulation shall apply from 25 May 2018. The Regulation aims to establish a single set of rules valid across EU, to provide more efficient protection of the individuals’ fundamental rights and in particular the right to privacy and to ensure economic growth with more adequate regulatory environment for the enterprises. With this in
view the article aims to analyse below some controversial issues related to data protection.

**Some controversial issues in data protection**

**The concepts of data controller and data processor in technological environment**

The concepts of data controller and data processor are essential in the EU data protection model. They form the basis for allocation of responsibilities for ensuring lawful processing of personal data and for defining the applicable data protection legislation (Article 29 Data Protection Working Party, Opinion 1/2010). According to the legal definition included in the EU Directive 95/46/EC, the data controller is an individual, legal entity or other body that alone or jointly with others determines the purposes and means of the data processing (Directive 95/46/EC, art. 2 (d). According to the EU Data Protection Directive the data controller is responsible for the lawful processing of personal data and ensuring the rights of data subjects. The concept of data controller should be distinguished from the concept of data processor that is the party which undertakes only the processing of personal data on behalf of the controller (Directive 95/46/EC, art. 2 (e).

The comprehensive approach towards data protection is considered as an advantage of the EU data protection model. However the assessment of the effectiveness of the EU Data Protection Directive indicates as a weakness the simplistic definitions of data controller and data processor which cannot adequately cover all entities involved in the data processing in an interconnected technological environment (Robinson, Graux, Botterman, & Valeri, 2009). As an example a cloud based free email service could involve separate storage and mailing functionalities for the customer while having a different legal entity providing analysis of clients’ e-mails based on which advertisements are shown to the customer. The case of social media could be even more complicated as is the case of social networks for example users act both as data subjects and data controllers when they share not only personal information but also information related to other individuals.

In its Opinion 1/2010 the Article 29 Working Party aims to clarify the concepts of data controller and data processor in view of globalization and increased complexity.
of the organizational and technological ways for data processing. The Working Party emphasises the importance of clear and uniform interpretation of the concepts as a way to achieve effective implementation of EU data protection model. Clarifying the idea behind the concept of “data controller”, the Working Party highlights that although the concept has been developed on the basis of Convention 108 of the Council of Europe, it has evolved to have its independent meaning under EU law. According to the Convention 108 provisions the data controller is only the individual or body that is competent to decide the purposes and means of personal data processing, while under the EU law as data controller is qualified the body that factually determines them, even in the cases when it is done contrary to the law. Technological environment like cloud computing or social media environment usually require factual analysis to be done in order to distinguish data controller and data processor.

According to the interpretation of the legal definition, in order an actor in data processing to be qualified as a processor, it should be an individual or separate legal entity that undertakes the data processing on behalf of the data controller. The EU Data Protection Directive requires a contract or a binding legal act to regulate the relations between data controller and data processor in order to ensure that the delegation of processing will not entail lower standard of data protection (Directive 95/46/EC, art. 17 (3)). However the Working Party reiterates that although the contracts can help to clarify the case, the factual analysis prevails. According to the analysis of the Working Party it could lead most often to divergent interpretations.

The EU Data Protection Directive provides that the controllers determine the purposes and means of the data processing. According to the interpretation provided by the Working Party, the determination of the purposes of the data processing qualifies the actor as data controller. The determination of the means of processing refers to decisions ensuring the lawfulness of the data processing and more specifically its compliance with the data quality principles. Such decisions always qualify the actor as data controller. However concerning the technical or organizational means of data processing, the decision can be taken by the data controller or to be delegated to the data processor.
The Working Party recommends that the contract between the data controller and the data processor should be in written form for evidence purpose and shall have a minimum content, stipulating in particular that the data processor shall act only on instructions from the controller and implement technical and organizational measures to adequately protect personal data. According to the interpretation provided by the Working Party the contract does not have constitutive effect for the controller/processor relations. In addition the Working Party underlines that regardless if the contract has been prepared by the controller or the processor if the controller agrees on the contract it takes the responsibility to comply with the legal requirements for lawful processing (Toptchiyska, 2014).

Despite the difficulties in the interpretation of the concepts of data controller and data processor the new EU General Data Protection Regulation does not change the definitions. However new provisions are included that clarify the legal relations between the data controllers in one processing and the data controller and data processor. In case of joint controllers, the Regulation requires that they determine in a transparent manner their respective responsibilities for compliance with the obligations in particular as regards the exercising of the rights of the data subject. Moreover the Regulation provides that irrespective of the terms of the arrangement, the data subject may exercise his or her rights in respect of and against each of the controllers (Regulation (EU) 2016/679, art. 26 (1) and (3). The provision is obviously in favour of data subjects and should facilitate the exercise of their rights under the Regulation.

Regarding the relations between the data processor and data controller the new General Data Protection Regulation provides that it should be based on governed by a contract or other binding legal act under Union or Member State law. The processor may involve another processor in the data processing only under the authorisation of the controller. In case the processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing (Regulation (EU) 2016/679, art. 28).

Considering the provisions regarding the data controller and data processor in the new General Data Protection Regulation against the standards of the rule of law
concept, it can be concluded that there are improvements. The regulation is much more detailed and adapted to multiple player technological environment. It provides better predictability and legal certainty that the data subjects will be able to identify the responsible data controller and exercise their rights efficiently. However the difficulties to distinguish the data controllers from data processors will still remain following the general definitions that have been kept in the new EU General DP Regulation.

**Rules regarding applicable law**

Global structure of the Internet often raises question related to identifying the applicable national legislation. Regarding the territorial scope (ratione loci) Directive 95/46/EC provides that the national legislation of the Member State applies where the processing is carried out in the context of the activities of an establishment of the controller. The national legislation of a Member State applies also when the international public law refers to it as well as when, although the controller is not established in the EU Member State, for the purpose of processing it uses equipment located in its territory (Directive 95/46/EC, art. 3).

In its judgment on the Google Spain Case the European Court of Justice interpreted broadly the provisions of the Data Protection Directive stating that although the activities of the company established within EU are not connected directly to the processing of data by the search engine GoogleSearch, the processing falls “in the context of activities” of the company, and therefore the Spanish law is applicable (Judgment of the Court (Grand Chamber) of 13 May 2014 in Case C-131/12). The EU Court considers that in view of the main objective of Directive 95/46/EC, namely to ensure the effective protection of fundamental rights and freedoms of individuals, and in particular their right to privacy, the interpretation of the provisions related to the applicability of EU law cannot be restrictive (Judgment of the Court Case C-131/12, par. 52 and 53 ). On this basis, any individual whether a citizen of an EU Member State may request the company providing search services on the Internet on the territory of the Member State of the EU to delete links to websites containing information that violates his rights, even in cases when publication of the information itself is legal. The judgment of the CJEU is in line with the new General Data Protection Regulation (Regulation (EU) 2016/679).
Regarding the territorial scope of application of the EU data protection legislation, the new General Data Protection Regulation introduces two main changes. First, the EU legislation is applicable when the personal data are processed in the context of the activities of an establishment in EU not only of the controller but also of the processor, regardless of where the processing takes place (Regulation (EU) 2016/679, art. 3, par. 1). According to Directive 95/46/EC only the activities of the data controller are linked to the applicability of EU law. The difficulties in differentiating the data controller from data processor in the technological environment because of its complex infrastructure and the multiple players involved in the data processing poses the risk of excluding applicability of EU law. For this reason the new provision is a positive change in the EU data protection legislation.

Second, the General Data Protection Regulation provides that EU data protection legislation will be applicable regarding the data processing of individuals located in EU, regardless of the place of establishment of the controller or the processor. The Regulation refers to commercial services and monitoring behaviour of individuals (Regulation (EU) 2016/679, art. 3, par. 2). Following the new provisions regardless of where the physical server of the data controller or data processor is located, when non-European companies offer services to European consumers they will be subject to the provisions of EU data protection legislation.

The new General Data Protection Regulation provides clearer rules on the territorial scope of EU data protection legislation. It guarantees the application of EU data protection legislation in the cases when personal data of individuals located on the territory of EU are processed. As a result the rule of law standards for legal certainty and predictability will be ensured more effectively.

The right to be forgotten and the processing of personal data on the grounds of legitimate interests pursued by the controller or by a third party

The right to be forgotten aims to guarantee that individuals are allowed, under certain conditions, to request from the data controller deletion of their personal data that they process. The right is not absolute and it should be balanced against opposing rights and legal interests. The right to be forgotten is explicitly regulated in article 17 of the new General Data Protection Regulation. In its Google judgement
the EU Court interpreted the right to be forgotten on the basis of the rights of data subjects included in the current Data Protection Directive in the scope of the data processing activities of Internet search engines.

Directive 95/46/EC provides that the data subjects have the right to obtain from the controller the rectification, erasure or blocking of data the processing of which does not comply with its provisions, in particular because the data are incomplete or inaccurate (Directive 95/46/EC, art. 12 (b). According to the EU Court the data processing carried out by Internet search engines is legitimate on the grounds of article 7(f) of the Data Protection Directive (Judgment of the Court Case C-131/12, par. 73). This provision allows processing of personal data when it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular his right to privacy with respect to the processing of personal data.

Application of Article 7(f) necessitates a balancing of the competing rights and interests concerned. The data subject has the right to object on compelling legitimate grounds to the processing of data relating to him. In the objection the data subject may refer to circumstances related to his particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data (Directive 95/46/EC, art. 14 (a). According to Directive 95/46/EC the data subject's requests should be sent to the data controller processing the data. The controller must examine request and end processing of the data in question, if the request is properly justified. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority for revision. Directive 95/46/EC puts the burden of proof on the existence of certain rights or legitimate interests on the data subject. According to the Opinion of the Advocate General on the Google Spain Case the legitimate interests of the data controller to process personal data in the absence of a data subject's consent, could include: 1/ making information more easily accessible for internet users; 2/ rendering dissemination of the information uploaded on the internet more effective; and 3/ enabling various information society services supplied by the internet search engine service provider that are
ancillary to the search engine, such as the provision of keyword advertising (Advocate general Jääskinen, 2013, opinion on the Case C-131/12). Each of these legitimate interests are consistent with the fundamental rights protected by the Charter of Fundamental Rights of the EU, namely freedom of information and freedom of expression and freedom of economic initiative (Charter of Fundamental Rights of the European Union, art. 11 and 16; Alsenoy, Brendan, Kuczerawy, & Ausloos, 2013).

In its 06/2014 Article 29 Working Group provides guidance on the application of the balance test on Article 7 of Directive 95/46 / EC. In applying the test the following three aspects should be taken into consideration. First, the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, or is otherwise in the public interest, or benefits from recognition in the community concerned. Second, the impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed. Third, the additional safeguards which could limit undue impact on the data subject, such as data minimisation, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, and data portability. Article 29 Working Group highlights the importance of documenting the way in which the balance test is applied as well as the need to motivate cases refusing to data subjects their data to be deleted. Article 29 Working group also recommends implementing a recital to the new Regulation on the key factors to consider when applying the balancing test.

In the Google judgment the CJEU emphasizes that the balance test between competing rights undertaken by the data controller is independent with regard to lawfulness of the processing performed by previous data controllers. In applying the test it should be taken in consideration that the right of data subject to be forgotten prevails over the legitimate interests of the search engines service providers and the general interest of freedom of information (Judgment of the Court Case C-131/12, par. 91). However the right of the public to find any information related to the name of a person on the Internet will have priority in case the data subject is involved in public life (Judgment of the Court Case C-131/12, par. 97). The judgment of the CJEU
provoked controversial reaction mainly focusing on the negative effect it could bring on the freedom of information and freedom of expression.

The right to be forgotten has been explicitly recognized in the new General Data Protection Regulation, providing that the data subject have the right to obtain from the controller the erasure of personal data concerning him or her (Regulation (EU) 2016/679, art. 17). The Regulation provides the grounds on which the data subject may request erasure of his personal data, including the cases when the personal data are no longer needed for the purposes they were collected or processed, withdrawal of the consent for the data processing or the data processing is unlawful on other grounds. The data subject may also object the processing on grounds related to his particular situation, when the processing is done without consent for execution of tasks in public interests or as necessary for the purposes of the legitimate interests pursued by the controller or by a third party (Regulation (EU) 2016/679, Article 6 (1), (e) and (f).

The General Data Protection Regulation allocates the burden of proof on the data controller to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject (Regulation (EU) 2016/679, art. 21 (1). The importance of the right to object is highlighted by the obligation of the controller to inform explicitly, separately and clearly the data subject about it from the first time of their communication. Along with the other requested information, the data controller should provide information to the data subject about the legitimate interests pursued by the controller or by a third party on the grounds of which the personal data processing will be done (Regulation (EU) 2016/679, art. 14 (2), (b). Moreover the Regulation lists the rights and interests that can override the right to privacy of data subject: including exercising the right of freedom of expression and information, compliance with legal obligation, public interest, etc. When the controller is obliged to delete the personal data he must inform controllers that process the personal data about the request of data subject. The obligation is quite vague and depends on the of available technology and the cost of implementation. In addition there is no requirement all controllers that process the data to be informed.
The new Data Protection Regulation provides much clearer and detailed provisions on the right to be forgotten than before as well as guarantees that the data subjects will be able to exercise their right effectively. However there are no clear guidelines on application of the balance test when the data are processed on the grounds of legitimate interests of the controller or a third party. Introducing clear procedures and criteria will greatly reduce the potential risk to censor information and will create the necessary legal certainty in the activities of data controllers.

**Conclusions**

The concept of the rule of law provides standards aimed to ensure effective functioning of the legal system, creating legal certainty and predictability, protecting individual and human rights. The EU data protection framework is regarded as the highest standard for privacy protection compared to other international legal frameworks. It is based on comprehensive and technologically neutral concepts, which makes them applicable in various technological environments. However their effective implementation requires more detailed and clear regulation. The new EU General Data Protection Regulation attempts to respond to this need as well to provide rules that are more adequate to the technological environment.

On the basis of the data protection issues analysed above it can be concluded that the new EU Data Protection Regulation follows the developments of the previous legislation framework ensuring consistency and high level of protection of individual rights and in particular the right to privacy in the context of automated data processing. The rights of the data subjects are strongly reinforced with additional regulation aimed to guarantee their effectiveness. The new regulation poses questions about the effectiveness of the existing data protection model with regard to abilities of data controllers and data processors to undertake their opposing obligations (for ex. in the case of joint controllers, or in the process of applying the balance test for competing rights and interest etc.). Considering the reality in the technological environment, EU data protection model needs more clear regulation as well as the support of self-regulation measures and deployment of privacy enhancing technologies that are provided in the new EU Data Protection Regulation.
References


ORBIT Journal DOI: https://doi.org/10.29297/orbit.v1i1.16

Judgment of the Court of Justice Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health, No. Case 283/81 (October 6, 1982).


Van Alsenoy B., Kuczerawy A. and Ausloos J.(2013), Search engines after Google Spain: internet@liberty or privacy@peril?, online on https://www.law.kuleuven.be/icri/, (accessed at 15.06.2014)


ORBIT Journal DOI: https://doi.org/10.29297/orbit.v1i1.16