ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „ALEXANDRU IOAN CUZA" DIN IAȘI
TOMUL LXIV, ȘTIINȚE JURIDICE, 2018, SUPLIMENT

SOLUȚIONAREA LITIGIILOR PRIVIND DATELE CU CARACTER PERSONAL

SETTLING THE DISPUTES REFERRING TO PERSONAL DATA PROTECTION

ANDREEA ȘERBAN[1]

Rezumat: Noua reglementare a datelor cu caracter personal oferă persoanei vizate – persoana ale cărei date sunt prelucrate de către operator – o poziție de control asupra modului în care informațiile despre sine sunt utilizate, acest control traducându-se printr-o serie de drepturi pe care legislația europeană pune mare accent în Regulamentul general privind protecția datelor. În vederea asigurării respectării drepturilor sale, persoana vizată are la dispoziție două căi de acces la justiție: calea administrativă și calea judiciară. Prezentul studiu prezintă principalele aspecte ale parcursului juridic al unui litigiu în materia datelor cu caracter personal, relevând rolurile părților implicate în litigiu.
Cuvinte-cheie: protecția datelor cu caracter personal, soluționarea litigiilor, plângeri privind protecția datelor, RGPD

Abstract: The new legislation referring to personal data gives to the data subject – the person whose data is processed by a controller – a position of control over the manner in which the personal information is used, this control being represented by a series of rights that the European legislation greatly emphasizes in the General Data Protection Regulation. In order to ensure the adherence to their rights, the data subject can address the issue in an administrative or civil litigation path. This paper outlines the main aspects of the judicial process of a dispute referring to personal data, underlining the roles of the involved parties.
Keywords: personal data protection, settling disputes, complaints referring to data protection, GDPR

1. Preliminary considerations

The protection of personal data is guaranteed by a series of international, European and national legal instruments, giving the data

[1] PhD student, `Alexandru Ioan Cuza` University of Iasi, Faculty of Law, email: andreeaserban20@yahoo.com.

subject – the person whose data is processed – means of protecting their personal information against any illicit processing. At the European level the principles that stand for the protection of personal data are covered by the new legislation – the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data known as the General Data Protection Regulation[2] (hereinafter, the Regulation).

The access to justice of the data subject for defending and protecting their new privacy-related rights[3] meets the characteristics of different legal mechanisms specific to all forms of liability – in this paper we shall have into consideration mainly the contravention and the civil liability[4].

In the following study we intend to present these mechanisms in the light of the new Regulation that has been applied since the 25th of May 2018. Through the Regulation, the data protection laws across the Member States of the European Union have been automatically harmonized, given the fact that this legislative act is a pan-European Regulation that has replaced the Directive no. 95/46 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data[5] and has repealed any national law that transposed the aforementioned directive. We can easily observe that certain issues referring to the protection of personal data have been extensively addressed in the new piece of legislation and that the control of the data subject over their personal information has been greatly improved.

2. General viewpoints on the rights to privacy and protection of personal data

[2] 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), Official Journal of the European Union L 119/1, 4 May 2016, applied starting the 25 May 2018.

[3] For example: the right to be forgotten, the right to object and so on.

[4] G. Zanfir, *Protecția datelor personale. Drepturile persoanei vizate*, Ed. C.H.Beck, Bucharest, 2015, p. 206.

[5] 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, Official Journal L 281, 23 November 1995.

During the recent decades, a particular focus has been placed on the concept of privacy and the confidentiality of the information. The private life has been perceived as the expression of a person's personality and, at the same time, the ability of citizens to control how the information about them is enacted[6]. The notion of confidentiality is closely related to those regarding the human dignity and the inviolability of the personality, the latter being defined as the independence, the dignity and the integrity of the unique self-determinant essence of a person[7]. In one of the earliest judicial cases that recognized the existence of the right to privacy, *Paversich v New England Life Insurance Co.*[8], the court expressed the concern over the use of a person's information and picture for commercial purposes without consent and considered that such actions as assaults to the integrity of the individual; the practices of using the personal information for the commercial purposes transforms the person into a good that serves the economic needs of others. In a community so deep into the trade of human values, it is degrading that a person becomes part of the commerce against their will[9].

Article 8 of the European Convention on Human Rights[10] addresses the issue of respect for the right to privacy, all situations being covered without limiting the private life exclusively to the right to live free from indiscretions and perceiving the technological progress as a relevant aspect for dealing with any case of personal data process[11]. In *Leander v Sweden*[12] judicial case, the European Court of Human Rights stated that the data storage on a computer and the communication of such data, together with the refusal to offer to the interested person the possibility of combating this processing represents an infringement of the personal right to respect for their privacy.

---

[6] F.H. Cate, *Privacy in an information age*, Washington D.C., Brookings Institution Press, 1977, p. 19.

[7] E. Bloustein, *Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser*, 39, N.Y.U., I. Rev. 962, 971, 1964.

[8] Court of Georgia, United States of America, decision from the 3rd of March 1905, [Online] at http://faculty.uml.edu/sgallagher/pavesich_v.htm, accessed at 7 February 2018.

[9] J. Kahn, *Privacy as a Legal Principle of Identity Maintenance*, Faculty Scholarship 406, 2003, p. 375, [Online] at https://open.mitchellhamline.edu/, accessed at 7 February 2018.

[10] European Convention on Human Rights, Council of Europe, 4 November 1950, Rome, [Online] at https://www.echr.coe.int/Documents/Convention_RON.pdf.

[11] M. Voicu, *Protecția europeană a drepturilor omului. Teorie și jurisprudență*, ed. I, Ed. Lumina Lex, Bucharest, 2001, p. 162.

[12] ECHR, *Leander v Sweden*, decision no. 116 from 26 March 1987, [Online] at https://hudoc.echr.coe.int.

The right to a private life gives to an individual the ability to control the personal data that refers to them. Thus, the data subject – the person who can be identified or identifiable through data process, according to the Regulation – may decide on how the information can be used and the manner in which they can protect the data. With this into consideration, in the following paragraphs of this paper we shall present a relevant issue that determined the modification and the update of the data protection legislation and its impact on the judicial instruments and measures the data subject has when protecting their personal information.

In the recent years, the European citizens have shown a particular concern for the protection of their privacy, especially the information that referred to them. The year of 2013 was the beginning of a series of events that prompted a greater attention over the importance of personal data. In the United States of America, Edward Snowden gave to the press classified documents that showed how the National Security Agency (herein, the NSA) had undertaken spying actions not only on the general public, but also on different embassies and communication systems belonging to certain governments, by tracking telephone conversations or illegally accessing the electronic mail[13]. This situation has had a great impact on the European society, being observed that the Directive no. 95/46 was not sufficiently applied and did not answered to all the questions and the issues raised in the judicial practices, the privacy not being efficiently protected. As a result of the Snowden – NSA situation, both the American and the European legislators have reviewed and revised the enactment of data protection from the perspective of privacy as data confidentiality and national security[14]. Although part of the legal opinions of the American courts pointed out the positive aspects of maintaining a high level of the protection and confidentiality of personal data, the practice is still prioritizing the security disputes by bringing arguments for infringing the privacy for national security reasons[15].

[13] For details, refer to M. Alkhammash, *Information security for national security: The Snowden and NSA case study*, Munich, GRIN Verlag, 2014, [Online] at https://www.grin.com/document/308419, accessed at 14 January 2018.

[14] L. Alboaie, *Interpretarea principiilor privacy by design în era cloud computing*, in the Scientific Annals of Alexandru Ioan Cuza University of Iasi, Tomul LXIII, Juridical Sciences Series, 2017, Nr. II, p. 27.

[15] A. Dimitrova, M. Brkan, *Balancing National Security and Data Protection: the Role of EU and US Policy-Makers and Courts before and after the NSA Affair*, in Journal of Common

In the European Union we have identified an increasing concern for how the personal data is processed which subsequently let to the legislative reform in this matter. Even though issues such as public security and safety are relevant topics for the Member States of the EU and can be raised in disputes related to data protection under certain conditions, the confidentiality of the personal information still remains a priority.

As a result of the 2013 Edward Snowden situation, the Austrian Maximillian Schrems submitted a complaint to the Data Protection Commissioner requesting that his personal data to not be transferred by Facebook Ireland[16] to the United States of America[17]. Schrems argued that the American state did not offer a sufficient and adequate protection for the processed personal information, with a particular reference to the situation caused by Edward Snowden and the NSA. The complaint was rejected for the lack of evidence that the NSA had access to the information referring to the data subject and for the conformity of the Commission Decision no. 2000/520, known as *Safe Harbour*, which attested the sufficiently high level of protection ensured by the USA. Schrems addressed to the Irish High Court, requesting a preliminary ruling regarding the compulsoriness of the National Supervisory Authority to comply with the Commission Decision no. 2000/520. Having into consideration that if the dispute should be settled under Irish law, the Authority would be required to comply with the request and therefore to prove that the USA provided the adequate protection of the data for which the processing (the interception of electronic communications between Ireland and the United States) to comply with the Irish Constitution[18]. This case is known as *Schrems I*. The Court of Justice of the European Union decided in 2015 the invalidation of the Commission Decision no. 2000/520. Following this judgment a second trial, *Schrems II*[19], began at the Irish High Court in order to determine whether the transfer of personal data between the European Union and the United States of America

Market Studies, 2017, p. 8-10, [Online] at www.sciencedirect.com, accessed at 16 January 2018.

[16] CJEU, Judgment of 6 October 2015, *Schrems*, C-362/14, p. 28.

[17] The main establishment of Facebook is in the United States of America.

[18] For details, refer to F. Coudert, *Schrems vs. Data Protection Commissioner: a Slap on the Wrist for the Commission and New Powers for Data Protection Authorities*, from 15 October 2015, [Online] at http://europeanlawblog.eu, accessed at 5 February 2018.

[19] The High Court of Ireland, the judgment of Judge Costello, from 3 October 2017, *Commisioner for Data Protection v Facebook Ireland Ltd. and Maximillian Schrems*, case no. 4809 P/2016.

and the rights of the European citizens are adequately protected by the standard contractual clauses used by Facebook[20]. The case was later sent to the Court of Justice of the European Union to determine whether these contractual clauses should be invalidated just as the Commission Decision no. 2000/520. Also, concerns were raised referring to the effective remedies available to the European Union citizens to protect their rights with regard to their personal data[21].

We can observe that the number of cases regarding the protection of privacy and personal data has been increasing, at least at the Court of Justice of the European Union. The doctrine[22] has established three categories of cases based on the European case-law: (1) *cases where the distinction between two rights*, possibly enacted by international legal instruments, *is relatively apparent* – such as the *Tele2Severige AB*[23] case where the Court has made the distinction between the right to privacy and to protection of personal data, stating *that Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in* the European Convention on Human Rights*[24]*, (2) *cases in which the distinction is not apparent*, as found in *Schrems* case, where the Court affirmed *the important role of personal data protection in the light of the fundamental right to respect for privacy*, failing to differ and delimit the two rights and (3) *cases that refer to the protection of personal data as a subsidiary category* – where the Court considered that the fundamental right to data protection is part of the fundamental right to privacy[25]. For the latter category we can give as example the case of *YS*[26], where the Court concluded that *it must be noted that the protection of the fundamental right to respect for private life means, inter alia, that that*

[20] For details, refer to *Schrems v. Data Protection Commissioner*, [Online] at https://epic.org/privacy/intl/schrems/, accessed at 5 February 2018.

[21] For details, refer to A.J. LaFrance, L. Hartnett, *Irish High Court Issues Judgement in „Schrems II" Case,* from 4 October 2017 [Online] at www.securityprivacybytes.com, accessed at 5 February 2018.

[22] A. Dimitrova, M. Brkan, *op. cit.*, p. 13

[23] CJEU, Judgment of 21 December 2016, *Tele2 Sverige AB v Post-och telestyrelsen*, C-203/15.

[24] *Idem*, p. 129.

[25] A. Dimitrova, M. Brkan, *op. cit.*, p. 16.

[26] CJEU, Judgment of 17 July 2014, *YS c. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie*, C-141/12 and C-372/12.

person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner[27].

Having all these in mind, we intend to see to what extent the new regulation responds to the needs of the European citizens, which are the measures they can adopt and which remedies can be used in disputes referring to the personal data.

3. The actors of data protection disputes

The European Regulation underlines the importance of personal data – the information regarding an identified or identifiable natural person such as the name, address and so on[28]. The Regulation guarantees the protection of the personal information by establishing certain legal instruments for protecting the right to data protection[29] from which the other rights recognized by the normative act derive.

Therefore, any person whose personal data have been processed, if suffered a material or moral prejudice, has the possibility to notify the National Supervisory Authority. The data subject – a national of a Member State of the European Union – will have the same procedural means as provided by the civil procedure code or the specific law governing procedural aspects of each Member State.

According to article 80 of the Regulation, on behalf of the data subject a complaint can be filed by institutions, organizations or associations, as well as other legal persons if their rights have been infringed or if the rights of the data subject have been unlawfully accessed[30]. A practice in this regard is already being created: the aforementioned Maximillian Schrems has set up a non-governmental organization called *None of your business (noyb)*[31] that is concerned with respecting the rights of the data subjects by collecting complaints and take action in courts on behalf

[27] *Idem*, p. 44.

[28] C.T. Ungureanu, *Protecția datelor cu caracter personal în contractele internaționale*, in the Scientific Annals of Alexandru Ioan Cuza University of Iasi, Tomul LXIII, Juridical Sciences Series, 2017, Nr. II, p. 138.

[29] M. Brkan, *Data Protection and European Private International Law*, EUI Working Paper RSCAS 2015/40, p. 2.

[30] For details, refer to *European Data Protection Regulation - Information sheet*, published on 1 March 2016, p. 7, [Online] at www.privacy-europe.com, accessed at 10 February 2018.

[31] [Online] at www.nyob.eu.

of more data subjects for protection their rights[32]. On the very first day of enforcing the Regulation 2016/679, on the 25th of May, *noyb* has filed 4 different complaints over forced consent against *Google* (in France), *Instagram* (Belgium), *WhatsApp* (Hamburg) and *Facebook* (Austria). What can be easily observed is that the four complaints were filed on behalf of the data subject who has requested to be represented by the non-profit organization under article 80 paragraph (1) that refers to the following: *the data subject shall have the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects; rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in articles 77,78 and 79 on his behalf, and to exercise the right to receive compensation referred to in article 82 on his or her behalf where provided for by Member State law.* Looking at the 2nd paragraph of the same article, a more data subject friendly approach can be noted: *Member States may provide that any body, organization or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to article 77 and to exercise the rights referred to in articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.* This *data subject – centered approach* derives from the fact that the organization can state the infringement and take action without actually needing the mandate of the data subject and therefore show its concern with regard to the public interest of having the right to data protection and privacy respected. Yet, the body that is being referred to in article 80 is limited in this case only to the complaints that can be lodged at the courts established in the Member State where it is lawfully registered. As we can see in the four complaints filed by *noyb*, except the one against Facebook, all the others have been filed in different Member States. A practice where the not-interested-in-profit activity takes precedence has not yet been formed and

[32] For details, refer to C. Stupp, *Privacy crusader Schrems starts NGO to bring more tech firms to court*, published on 29 November 2017, [Online] at https://www.euractiv.com/section/data-protection/news/privacy-crusader-schrems-starts-ngo-to-bring-more-tech-firms-to-court/, accessed at 27 February 2018.

therefore, given that all the complaints filed so far are based on article 80 paragraph (1) it can be deduced that this provision can be used as a loophole for attracting certain data subjects that can offer the apparent reason against a controller and the interested mandated body can take over the complaint.

According to article 4 of the Regulation, the data controller is *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*. The processor is *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.* By processing, we understand *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.* The extraterritorial effect of the Regulation refers to the extension of the scope also to the controllers and processors outside the European Union and to the processing operations that regard the supply of goods or services to the natural persons located within the EU or to the monitoring of their behavior. As a novelty in the field of data protection, we note that, according to article 27 of the Regulation, controllers and processors outside the European Union that are subject to the European laws on personal data protection must appoint a representative to act in the EU on their behalf.

If there is a data infringement resulting from the activity of the controller or processor, the question raised in doctrine referred to the form of liability. Would that be a contractual or a civil liability? It depends. In a situation where a contractual obligation between the data subject and the controller or processor is not respected, the processing of personal data being part of the contractual performance, we have into consideration the contractual liability. If no contractual obligation has been subject to a non-performance action, then we shall have into consideration the civil liability[33].

The regulation brings forward as new means of strengthening data protection the appointment of a Data Protection Officer (DPO) within the

[33] C.T. Ungureanu, *Căile legale de restabilire a dreptului la protecția datelor cu caracter personal încălcat în raporturi de drept internațional*, in Dreptul, no. 10 of October 2018, p. 84-85.

institutions operated by a data controller and a processor, according to article 37 and 38 of the Regulation. This officer does not assume the responsibility for ensuring the protection of data, yet he is named this way due to his duties and not his obligations[34]. The role of a data protection officer is to ensure that the controller processes and determines the means and purposes of the personal data processing according to the provisions of the Regulation regarding data protection[35].

Article 4 paragraph 21 of the Regulation defines the supervisory authority as the independent public authority established by a Member State. Article 51 of the same legal act refers to the fact that each Member State ensures that one or more independent public authority have the responsibility to monitor how the new European provisions apply to protect the fundamental rights and freedoms of the data subject whose personal information is processed also for facilitating the free movement of personal data. The Regulation establishes that this authority may give administrative sanctions.

In the following parts of this paper, we want to determine the roles of the potential parties in the disputes related to data protection and which remedies and legal instruments can be used in these situations. We also want to establish which administrative or judicial authorities are competent in such cases. We will consider to ways of settling these disputes, namely the administrative path and the litigation before the civil courts.

4. The administrative path

The controller has the obligation to take the necessary technical and organizational - administrative measures to ensure that the data processing takes place in accordance with the provisions of the regulation. Also, as part of a data protection policy, the controller must ensure an adequate level of data security through various mechanisms, the Regulation mentioning, inter alia, at article 32 *the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services* and the possibility to make the data available to the data subject.

[34] For details, refer to A. Săvescu, *Cum trebuie să fie DPO (responsabilul cu protecția datelor)*, [Online] at https://goo.gl/kVtAYY, accessed at 2 March 2018.

[35] [Online] https://goo.gl/nJiVJ2, accessed at 2 March 2018.

The main purpose of this new Regulation is to give to the European citizens – the data subjects – the control over the whole process of storing and processing their data, by granting them additional rights such as the right of access to data, the right to rectification and to erasure and so on. If the controller does not comply with the new requirements, the data subject has the administrative remedy as the most used legal tool to protect their personal data.

The Directive 46/95 did not specify a certain administrative remedy, leaving it to the Member States to determine how the situations in the field of personal data would be addressed[36]. This path has its central point in the activity of the supervisory authority.

Each authority shall have the competence on the territory of the state of establishment to monitor any operation of processing of data that affects the data subjects or is transferred outside the European Union when the processing is addressed to the data subjects that do not reside within a Member State. The supervisory authority has the tasks of conducting investigations and public awareness campaigns regarding the risks, rules and rights referring to personal data processing and also facilitates the access to an administrative remedy by receiving and handling complaints[37]. In Romania, the National Supervisory Authority for Personal Data Processing known as ANSPDCP *receives, analyzes and solves complaints related to the processing of personal data falling within the scope* of the Regulation, according to article 1 of the Procedure for handling complaints[38].

Under the Regulation, the supervisory authority can place administrative remedies against the controller or the processor. If the processing is not carried out in compliance with the provisions of the Regulation, the authority has corrective powers, according to article 58 paragraph 2, namely to *(a) to issue warnings […], (b) to issue reprimands[…], (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation, (d) to order the controller or processor to bring processing*

[36] M. Brkan, *op. cit.*, p. 4.

[37] For details, refer to N. Stribbe, *GDPR: the data protection supervisor(s): Who are you? Where are you?*, published on 26 October 2016, [Online] at www.lexology.com, accessed at 15 February 2018.

[38] [Online] http://www.dataprotection.ro/?page=procedura_plangerilor, accessed at 10 November 2018.

operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period, (e) to order the controller to communicate a personal data breach to the data subject, (f) to impose a temporary or definitive limitation including a ban on processing, (g) to order the rectification or erasure of personal data or restriction of processing […] and the notification of such actions to recipients […], (h) to withdraw a certification or to order the certification body to withdraw a certification […], (i) to impose an administrative fine […], (j) to order the suspension of data flows to a recipient in a third country or to an international organization.

Other sanctions can be applied as well. The European Commission has the power to order a controller or processor to notify each stage of data processing and every situation of data protection rights infringement. Another issue refers to the possibility for the national supervisory authority to draw a report containing the information on the measures taken against the controller, including the administrative fines. This measure could possibly damage the good image of the controller[39].

The Regulation also provides in article 58 that, in order to ensure the compliance with the legislative act and its enforcement, the supervisory authority of each Member State may *bring infringement of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings.*

One of the novelties of the Regulation is the competence of the authority to impose sanctions in the form of effective, proportionate and dissuasive administrative fines. The sanctions are provided by article 83, the administrative fines being up to *20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.*

Each natural (the data subject) or legal person (the controller) has the right to an effective judicial against a legally binding decision of supervisory authority concerning them, according to article 78 paragraph (1) of the Regulation. The same article provides in paragraph (3) that the *proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.*

[39] Refer to *GDPR: Administrative Sanctions*, [Online] at www.dilloneustace.com, accessed at 15 February 2018.

5. Civil litigation path

The jurisprudence related to data protection is not fully developed yet. This subject is lacking a significant number of cases that could determine a changing perspective on how data and privacy are being seen by judges. This is most likely due to the fact that citizens have yet to realize the relevance of data protection, the unlimited possibilities regarding the processing of their personal data and their rights. Yet, we can observe that, gradually, the natural persons whose data has been processed have begun to understand the concepts of personal data and how the processing affects them. For example, in a British case, *Google v Vidal Hall*[40], it can be observed that the data subjects choose to appeal to the court even for moral damages without suffering a material damage if their data is not being processed for well-defined purpose or used without their consent. In this case, the complainants have used a particular browser – a soft used to accessing Internet information; they complained about the fact that the defendant, the controller, collected their personal data using *cookies* – the files that are installed in the computer by accessing certain web pages that retain information concerning the user and their activity on the website, without their consent or being informed prior to the processing. The complainants have shown that the defendant used the data to provide commercial services to advertisers using the online space[41].

Although the administrative remedies do not involve a considerable financial or temporary effort, the judicial remedy provided by the judicial authority proves to be the most effective mean of protection as it offers the safeguards of the common law[42].

The Regulation gives to the data subject means of protecting their personal data, by giving him the right to an effective judicial remedy against a supervisory authority – article 78 or against a controller or processor – article 79. If the data subject is not content with the response received from

[40] London Court of Appeal, Case no. A2/2014/0403, *Google v Vidal-Hall*, [Online] at https://www.judiciary.uk/judgments/vidal-hall-v-google/, accessed at 10 November 2018.

[41] Refer to [Online] http://www.5rb.com/case/vidal-hall-v-google-inc/, accessed at 10 November 2018.

[42] S. Șandru, *Protecția datelor personale și viața privată*, Ed. Hamangiu, Bucharest, 2016, p. 265.

the supervisory authority or the data controller, he is given the right to act before a national court[43].

Depending on the action, a claimant can be (1) a natural person – the data subject whose personal data has been unlawfully processed or whose rights provided by the Regulation have been infringed, (2) the controller or the processor or their representatives in the EU, according the article 27 of the Regulation – if the operations of processing data have been subjected to an administrative measure imposed by the supervisory authority or (3) even the data protection authority for defending and protecting the rights of the data subject or for securing the enforcement of the provisions of the Regulation[44].

If the data subject seeks to coerce the controller or the supervisory authority to issue, revoke or annul an administrative act referring to the processing of personal data or to challenge a decision of the data protection authority, they must address to the administrative court. If they seek compensation or damages for the unlawful processing of data, the data subject will seek the common law court[45].

Article 80 of the Regulation provides the possibility for an entity to lodge a complaint or to exercise the rights to a judicial remedy on behalf of the data subject or data subjects. This type of action is called a *class action* and, according to the provisions of the Regulation, there are two kinds in the matter of data protection: either a data subject mandates an entity to represent them and take action on their behalf, either the entity, independent from the request of the data subject, has the possibility to exercise the rights recognized to the natural persons if it considers that these rights have been infringed following the processing. The first form is similar to an *opt-in class action* – the data subject must want and has requested the representation by an entity. The second form is similar to an *opt-out class action* – it is not necessary for the consent of the data subject, yet only if they do not want to be represented, they have to express their will[46].

Not only the provisions of the Regulation give to the data subject the possibility to benefit from an effective remedy against the supervisory

[43] European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European Data Protection Law*, 2014, p. 127.
[44] S. Șandru, *op. cit.*, p. 265.
[45] *Ibidem.*
[46] For details, refer to C.T. Ungureanu, *op. cit.*, 2018, p. 93-95.

authority or against the controller and processor, respectively, it also offers the right to compensation in the situations involving more or less complex data processing. The data subject is entitled to be compensated by the controller or the processor if they suffered a material or non-material damage as a result of non-compliance with the Regulation.

The Regulation does not particularize the forms of liability in the data protection disputes. Article 82 provides that *any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.* Regarding the processor, they are liable *for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller*. According to article 82 paragraph (3), the controller or the processor will be exempt from liability if they prove not to be responsible for the event that caused the damage.

The Regulation is applicable in all Member States of the European Union. According to article 3, the provisions of the Regulation apply *to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*. There is no priority rule with regard to the court that has the territorial jurisdiction to solve a dispute. The data subject has the possibility to benefit from an effective remedy from the court that is closest to their residence. Yet, if the processing is carried out by a public authority that acts according to its public powers and competencies, the complaint can be lodged only at the closest court to the establishment of that authority[47].

Under the Council of Europe legislation, infringing the right to data protection in a contracting state to the European Convention on Human Rights constitutes an infringement of the article 8 of the same convention, which may lead to a legal action before the European Court on Human Rights after all the internal available remedies have been exhausted[48]. If the ECHR finds a contracting state in violation of any right protected by the European Convention on Human Rights, that State has the obligation to

[47] G. Zanfir, *op. cit.*, p. 220.

[48] ECHR, *Trăilescu v Romania,* Decision from 22 May 2012, 5.666/04 and 14.464/05: the Court stated that the claimant cannot invoke the infringement of his right as long as all the internal available remedies have not been exhausted.

enforce the given judgment and the measures taken in this situation must end the on-going judicial process and, if possible, to limit the negative consequences for the applicant. The judgment can be enforced by adopting measures to prevent similar situations and even by modifying the national legislation[49]. When a violation of the European Convention on Human Rights if found, article 41 provides the possibility of damages being awarded to the claimant at the expense of the involved contractual state[50].

6. Conclusions

The Regulation is already having a major impact on data controllers and processors. Under the new enactment, the data subjects have acquired an extensive control over their personal data and, if well informed, they are able to track every step of the data processing and act upon any deviation of the controller or the processor from the provisions of the Data Protection Regulation.

An issue is represented by the possibility of a data subject to be represented according to article 80, through class actions. We wonder whether this provision will not provide a legislative gap that could be used by entities to secure their own interests. Entities are already providing these services with the visible and public purpose of obtaining sufficient funds for militating for an efficient data protection.

Certainly, the new provisions are beneficial to the data subject who can obtain damages even for less significant infringements. However, it remains to be seen in practice how they will appreciate the value of their data and how the supervisory authorities and courts will determine the liability in data protection disputes.

[49] European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European Data Protection Law*, 2014, p. 127.

[50] *Ibidem*.