**Logos Universality Mentality Education Novelty: Law**
ISSN: 2284-5968 | e-ISSN: 2458-1046
Covered in: ERIH PLUS, HeinOnline, CEEOL, Index Copernicus, CrossRef, CrossCheck, J-GATE, Google Scholar, Ideas RePeC, Econpapers, Socionet, KVK, WorldCat.

2018, Volume 6, Issue 2, pages: 26-47 | doi: https://doi.org/10.18662/lumenlaw/10

# Legal Remedies for Personal Data Protection in European Union

**Carmen Tamara UNGUREANU**[1]

[1] Faculty of Law, Al. I. Cuza University from Iasi, Romania,
carmen.ungureanu@uaic.ro

**Abstract**: In Romania, in the vibrant discussions on General Data Protection Regulation (GDPR), one of the issues less explored deals with the legal remedies for personal data protection. This is the topic of the present study, considered in an international – cross border context which is structured in two parts. In the first part terms frequently used will be explained and clarified. The second part will be focused on the core issue, meaning the pathways - the administrative way and the judicial way - data subject have at his/her disposal for restauration of the violated right, the fundamental right to the protection of personal data.
If the administrative way is chosen, data subject has the right to lodge a complaint with a supervisory authority. If data subject is choosing the judicial path, he/she has the right to act either against the supervisory authority or against the controller or processor.

**Keywords:** *GDPR; data subject; data protection; administrative proceedings; judicial proceedings.*

**How to cite:** Ungureanu, C. T. (2018). Legal Remedies for Personal Data Protection in European Union. *Logos Universality Mentality Education Novelty: Law, 6*(2), 26-47. https://doi.org/10.18662/lumenlaw/10

## Introduction

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (European Parliament, 2016), and repealing Directive 95/46/EC on General Data Protection Regulation (European Parliament, 1995) is going to be applied starting from 25th of May 2018 in all of the European Union (EU) member states. GDPR has as a declared goal the safeguarding of the personal data protection fundamental right [art. 1 (2)]. From a legal perspective, this safeguarding can become effective using legal remedies in all the cases in which the personal data protection right is violated.

Such violations of the personal data protection right should fall within the *temporal scope* of GDPR when taking place *after* the 25th of May 2018. The proceedings brought after the 25th of May 2018, but dealing with infringements committed before this date, will be solved by the previous rules, applicable at the moment of the violation.

Regarding the *territorial scope* of GDPR, its rules should be applied to all situations in which a controller or a processor has an establishment in EU, regardless of whether the processing of personal data takes place in the EU or not [art. 3 (1)]. Furthermore, GDPR applies to the processing of personal data of data subjects who *are* in the EU by a controller or a processor without an establishment in the EU, if the processing of data is related to the offering of goods or services to such data subjects *in the EU* or to the monitoring of their behaviour as far as their behaviour takes place within the EU [art. 3 (2)].

Until the application of GDPR, the current rules regulating personal data protection are art. 16 from the Treaty on the Functioning of the European Union (TFEU, 2012), art. 8 from the Charter of Fundamental Rights of the European Union (2012), 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 (1995), the latter transposed in the Romanian national law as the Law no. 677/2001 for the protection of individuals with regard to the processing of personal data and on the free movement of such data (Romanian Parliament, 2001)[1], with its subsequent modifications.

The beneficiary of personal data protection regulation is a natural person, called *data subject*. In this study the ways the data subject has at

[1] Romania had transposed the european directive before of 2007, year of adheresion to the EU, as a required action for *acquis* alignement.

his/her disposal in data infringements cases will be identified. Only the violations in a cross-border context will be considered. The data subject having his/her habitual residence in *Romania will be taken as a reference system*, in an attempt of guiding him/her to the competent authority for dealing with the judicial issues arising from the data protection violations.

## 1. Violation of the right to the protection of personal data. Terminology clarifications.

To facilitate a better understanding of the issues the study is dealing with, it will be first explained what *personal data* means, who is the *data subject*, who is *responsible* for data protection, what is an *international/cross-border context*, what kind of *damages* can data subject suffer, what *type of liability* may be triggered by a violation of the right to the protection of personal data and which pathways the data subject may follow to *restore the violated right*.

### *1.1. What does personal data mean?*

According to art. 4.1 GDPR personal data is *any information* relating to an identified or identifiable individual, that is, the data subject. The concept of personal data has a very broad meaning. Thus, such information refers to the identification of the individual, through his/her name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

### *1.2. Who is the data subject?*

The data subject is a natural person. The right to the protection of personal data is considered a non-patrimonial fundamental right. In contracts, the data subject could be a party in the so-called consumer contracts, having the role of consumer, user, subscriber, depending on the legal relationship he/she enters (Şandru, 2016: 199). The legal person, as a rule, cannot be holder of the right to data protection, meaning it cannot be data subject. However, legal entities or groups of individuals could have their data protected in some European countries, such as Austria and Italy (Şandru, 2016: 199).

### *1.3. Who is responsible for data protection?*

In GDPR, the liability for data protection rests with the *controller* (mainly) and the *processor* on behalf of the controller.

As art. 4.7 GDPR states, *the controller* is a 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 [art. 4.8 GDPR].

Anyone who decides to process personal data of others is a controller *in accordance* with GDPR; if several people are involved in the same processing, they are considered *joint controllers*. A processor is a *separate legal entity* whose task is the processing of personal data on behalf of the controller. The processor becomes a controller if he uses the data for his personal purposes without following the controller`s instructions (FRA, 2014: 50).

Therefore, the persons held liable for the protection of personal data are the controller and/or the processor. It is from the *power of control and decision* on other person`s personal data and not from the data processing itself that this status derives (Şandru, 2016: 202).

The processor works over the personal data on behalf of the controller on the basis of a contract. As a rule, this contract has a commercial nature, being a service agreement; the controller is the beneficiary and the processor is the service provider. It is possible that the controller is a smaller enterprise and the processor a large corporation that has the power to dictate the conditions in which it offers its services. For example, the controller concludes a cloud computing[2] contract with a cloud provider and stores personal data in the cloud. The cloud provider, on the basis of party autonomy and contractual freedom, may subcontract (Ungureanu, 2015: 26).

A *natural person* who processes personal data in a *purely personal or household activity* is not a data controller [art. 2 par. (2) (c) GDPR]. However, if the activity through which data is processed is not exclusively personal or domestic, the individual acquires the status of personal data *controller*. For example, in the case of Bodil Lindqvist (C-101/01), the European Court of Justice (ECJ, 2003) considered that the act of referring on an Internet page to various persons and their identification, either by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies so that these data become accessible to an indefinite number of persons, constitutes processing of personal data, as this activity cannot be interpreted as being associated with activities carried out in private or family life.

[2] Cloud computing means distributed computing through a network, the Internet, and consists of the ability to make a program or an application work at the same time in multiple computers connected to each other.

### *1.4. What does international/cross-border context mean?*

The right to data protection will be seen in this paper in an international/cross-border context, meaning in situations where the collecting, processing or transferring of personal data involves an international element/cross-border element. The international element is the fact that makes a legal relationship come into contact with two or more different legal orders.

In GDPR is only defined the term of cross-border processing, as meaning either: „(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State." [art. 4.23 GDPR]. For example, Facebook (with its establishment abroad) collects, processes and transfers personal data from data subjects with habitual residence in Romania on the basis of the agreement between the social network and the data subjects; this represents a cross-border situation.

### *1.5. What kind of damages can data subject suffer?*

The right to the protection of personal data is a non-patrimonial, human right, indissolubly connected to the right to privacy. Violation of this right may cause to the data subject moral and/or material damage (Ungureanu, 2017: 139-141).

The GDPR does not determine what is meant by the breach of the right to data protection, nor is the notion of damage defined. It is only stipulated that the data subject has the right to bring a legal action if he/she considers that his/her right to data protection has been violated as a result of data processing in a non-compliance with the GDPR provisions [art. 79 par. (1) GDPR]; also, the data subject who has suffered material or moral damages is entitled to compensation [art. 82 par. (1) GDPR].

In a study conducted in 2014 by *The European Union Agency for Fundamental Rights* (FRA & CE, 2014), there was found that some of the most frequent sources of personal data violations were the Internet-based activities of the data subject, including social networks, online contracts such as online shopping, email accounts, misuse of personal data by global Internet companies. Another source was considered direct marketing and

commercial prospecting without the consent of the recipient, through profiling and selling personal data by controllers or processors to third parties. The same study showed that those interviewed described the damage suffered as a result of the infringement of the right to data protection as being of a psychological and social in nature, such as emotional distress or reputational damage. Participants also, although less frequently, reported financial losses (FRA, 2014: 3-4). Usually, the damages data subjects suffer concern a large number of people, nevertheless, with a small financial reflection on each person.

In legal literature several types of damages are distinguished: moral damages (psychological and emotional), reputational harms, damages related to data subject dignity, financial loss, vulnerability issues, physical injuries, discrimination on different criteria (Lynskey, 2015: 196; Schwartz & Solove, 2012: 51).

In GDPR the damages that data subject may suffer as a result of the violation of his/her right to the protection of personal data are determined in the recital no. 75. The infringements of data protection right, in GDPR words, „could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.”.

### *1.6. Characterization of liability for restauration of data subject violated right*

The way of liability characterization determines the legal regime applicable to the protection of personal data.

The natural person`s personal data can be collected, processed and transferred in multiple and various relationships in which he/she enters, either with public authorities or private organizations or natural persons.

For example, a consumer`s personal data is collected and processed when private contracts are concluded, called consumer contracts. These data are used both for the contract performance and for the conclusion of future contracts by accomplishing what is called *profiling*. According to GDPR (art. 4.4): „`profiling` means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person`s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;".

If the right to data protection is violated, on what grounds will the controller or the processor be liable? Is there a contractual liability or a tortious one? The answer is complex and should be given in each case, considering its particularities. As a rule, the tortious liability is triggered.

### *1.7. Which are the ways the data subject could follow to restore the violated right?*

It should first be noted that the legal remedy is a two ways road: the data subject has the right to restore the violated personal data right; at the same time, the controller or the processor has the right to counter against the measures taken by the competent supervisory authority, either in an administrative court or a civil one. This paper will focus only on the pathways the data subject could follow.

Violation of the right to data protection does not necessarily lead to litigation. The data subject has several ways to restore the violated right. According to art. 77-82 GDPR, the data subject may initiate administrative proceedings and civil court proceedings. Judicial proceedings in a civil court may be conducted after or in parallel with, and independently of, administrative proceedings.

The competent authority to restore the violated right depends on the qualification of the legal situation and the path that the data subject chooses to follow: the administrative or judicial way[3].

*The administrative pathway*. Mainly, administrative proceedings are related to the right of the data subject to lodge a complaint with a

[3] We will not deal with criminal liability in this study.

supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement.

The supervisory authority is an independent public authority in a Member State that has the role of monitoring and controlling the processing of personal data. The supervisory authority has several tasks and competencies (art. 51 et seq. GDPR), such as: it may impose a temporary or definitive limitation including a ban on processing of personal data, it may order the rectification or erasure of personal data or restriction of processing, it may start the proceedings for a criminal investigation; it may order the suspension of data flows to a recipient in a third country or to an international organization; it may impose administrative fines; it may conduct investigations *ex officio* or when receiving complaints etc. The supervisory authority applies frequently administrative fines. For example, Facebook was amended by France`s National Commission for Informatics and Freedom (CNIL) on May 16, 2017, with 150,000 euros for the massive use of personal data for advertising purposes (Schneider, 2017). On 11 September 2017, the Spanish Personal Data Protection Agency fined Facebook with 1.2 million euros for the collection of users` personal data without obtaining their explicitly expressed consent (Hetz & Binnie, 2017).

*The judicial pathway*. When the data subject chooses the judicial remedy, he/she has two possibilities: either to bring proceedings in an administrative court (administrative litigation) against the supervisory authority or to seize a civil court with a lawsuit filed against the controller or the processor, aiming the restoration of the violated right, sometimes through a material or non-material compensation.

## 2. Competent authority to restore the violated right

Competent authority could be either a supervisory authority or a national court; the latter can be an administrative court or a civil court.

### *2.1. The administrative pathway*

For lodging a complaint on the infringement of personal data right the data subject should go to the competent supervisory authority. According to the provisions of art. 77 par. (1) GDPR, the competent supervisory authority is that of the place of data subject`s habitual residence, his/her place of work or of the place where the personal data protection violation has occurred.

The data subject may therefore choose to lodge the complaint with one of the following supervisory authorities, situated at:

- the place of his/her habitual residence;
- his/her place of work;
- the place of the infringement.

None of these concepts is defined in the GDPR.

The data subject`s citizenship or nationality does not play any role in determining the competence of the supervisory authority. For example, a natural person of Chinese nationality who is habitually resident in Romania is subject to GDPR provisions. If the same person has his/her place of work in Romania, he/she will be subject to GDPR, as well.

### *2.1.1. What does habitual residence mean?*

There is no definition in GDPR. In other EU instruments, the notion is not defined even though it is used. In the case-law of the ECJ, an autonomous interpretation was given to the term. For example, in case T-298/02 (no. 51) the ECJ ruled that „the place of habitual residence is that in which the official concerned has established, with the intention that it should be of a lasting character, the permanent or habitual centre of his interests. For the purposes of determining habitual residence, all the factual circumstances which constitute such residence and, in particular, the actual residence of the official concerned must be taken into account"; in a decision given in the case C-589/10[4], the ECJ ruled that a person cannot have simultaneously two habitual residences in the territory of two different Member States. In case C-255/13, the ECJ ruled that if an EU national residing in a first Member State remained in a second Member State for a long (11-year) period due to illness, this is not sufficient to consider that his habitual residence is in the second Member State.

In cases C-509/09 and C-161/10 (*Kylie Minogue and eDate Advertising*), the ECJ stated that „The place where a person has the centre of his interests corresponds in general to his habitual residence. However, a person may also have the centre of his interests in a Member State in which he does not habitually reside, in so far as other factors, such as the pursuit of a professional activity, may establish the existence of a particularly close link with that State.". „The judgment of the ECJ confirms that the connecting factor`centre of interests` only holds for infringement of personality rights in an Internet context." (Van Calster, 2016: 153).

In the spirit of the ECJ „habitual residence" interpretation in other areas, it could be considered that the data subject whose data protection

[4] All the ECJ case-law may be retrieved from www.curia.eu/

right has been violated is habitually resident in the Member State where the centre of his or her permanent or usual interests is located.

### *2.1.2. What does data subject`s place of work mean?*

The following places could be considered:

- Place of work where the data subject carries out his/her work under an *individual contract of employment*.

- Place of work where the data subject carries out a work under other contracts, such as *a civil or a commercial* one for the provision of professional services; for instance, services provided by an architect or a lawyer, employed to perform a particular service.

- If the data subject carries out a work under *any contract*, on the territory of *several countries*, part of them or all of them outside the EU, the question arisen is which place of work should be considered. In order to answer the question the interpretation given by the ECJ to the Brussels I Regulation - EU Regulation 1215/2012 – (European Parliament, 2012) could be used. The data subject place of work could be there where he/she has the habitual place of work.

The concept of 'habitual place of work' was interpreted by the ECJ in the cases C-125/1992 and C-383/1995, in the sense that an employee who carries out his/her work in more than one State usually works where he/she has actually set the centre of his/her work, from where he/she fulfils the essential part of his/her duties (Stone, 2010: 140). In the absence of such a centre, the ECJ established in the case C-37/2000 that the duration of the work should be taken into account, the habitual place of work being where the work was done for the longest period of time (Stone, 2010: 141).

### *2.1.3. What does the place of infringement mean?*

Could a natural person who is habitually resident in a state outside of the EU and is on holiday in an EU member state benefit from GDPR, if he/she has his/her right to personal data protection violated? Theoretically yes, because, according to art. 3 par. (2) „This Regulation applies to the processing of personal data of data subjects who *are* in the Union [...]". If, for example, an American who is habitually resident in the US is on vacation in Bucharest and orders a smartphone via Internet from an EU-based professional by paying with a credit card, his personal data will be collected, processed, transferred by the professional, who is acting as a controller. If the US person`s right to data protection is infringed, he may lodge a complaint with a supervisory authority from Romania, in accordance with GDPR. How will he/she prove that the violation of his/her right to data

protection has taken place in Romania? Given the nature of data flowing through the Internet from one database to another in a very short time, a few minutes, databases being located in many corners of the world, it is very difficult to prove that the infringement originates in a particular state.

The data subject could practice *forum shopping*[5] having a wide array of choices. The data subject will choose to go to the supervisory authority that is most convenient, both financially and practically (avoiding traveling abroad) and last but not least, that authority which would answer in a more convenient way to data subject problem.

In searching for the most convenient solution the data subject should compare different rules applicable in different Member States by different supervisory authorities and choose the „winning one", the most suitable for its interests. This is possible because, although the GDPR is harmonizing the provisions on personal data protection in the EU Member States, there are issues left unresolved or left to the Member States to resolve. For example, according to art. 23 GDPR, the national law applicable to the controller or the processor may, by a *legislative measure*, restrict the scope of the obligations and rights set out in the GDPR under certain conditions (Voigt & Bussche, 2017: 219-222).

According to art. 55 par. 1. GDPR each supervisory authority is competent for the performance of the tasks assigned to and the exercise of the powers conferred on it on the territory of its own Member State. This means that in the cases of collection, processing, international transfer of personal data, several supervisory authorities from different Member States are competent. Before GDPR, controllers and processors faced different interpretations of their obligations in the view of the various national supervisory authorities with which they interfered. There is an attempt to eliminate this risk through the provisions of art. 56 GDPR. It is introduced a so called, *one-stop-shop competence mechanism* that makes *only one* national supervisory authority responsible *for a case* (Voigt & Bussche, 2017: 191). These provisions are advantageous for the controller/processor that, with regard to the cross-border processing of personal data, only interferes with the lead supervisory authority. The lead authority is the supervisory authority of the main establishment or of the single establishment of the controller or processor.

[5] *Forum shopping* refers to the practice used by parties in some cases consisting in searching through multiple courts or, in this particular case, through multiple supervisory authorities in order to file the case to one that is most likely to give that party the result he/she wants.

Despite this *one-stop-shop competence mechanism* there are exceptions to the rule and different parallel proceedings, which diminish its practical utility (Voigt & Bussche, 2017: 191).

The supervisory authority with which a complaint has been lodged will settle it in accordance with the procedural rules laid down by the law of the State on whose territory it is established (Voigt & Bussche, 2017: 204). There are no rules in GDPR on this matter. Therefore, different supervisory authorities will apply different procedural rules.

The complaint of the data subject may have as its object the violation of his/her rights protected by GDPR provisions. The data subject must prove that he/she has suffered damage as a result of that violation.

The supervisory authority is required to inform the complainant (the data subject) on the progress and outcome of the complaint, including the possibility of a judicial remedy.

If the supervisory authority fails to handle the complaint or inform the data subject on the progress of it within three months counting from the filing date, the data subject may take legal action.

The supervisory authority, on the basis of its powers and the content of the filed complaints by the data subjects, may take various actions against controllers/processors that have breached the right to the protection of data subject personal data. The corrective actions to be taken from the supervisory authority are laid down in art. 58 par. (2) GDPR. The measures taken by the supervisory authority may be challenged with a complaint or a judicial action in accordance with the national law of the State where the supervisory authority is established.

### *2.2. The judicial pathway*

The judicial pathway the data subject has the possibility to follow consists in two types of actions:

- a action against the supervisory authority,
- a civil action directed against the controller or the processor.

#### *2.2.1. Judicial action brought against the supervisory authority*

The data subject and the controller/processor may, equally, bring actions against the supervisory authority. In this study will be analysed only those that *data subject* has at his/her disposal.

The data subject may sue the supervisory authority when:

- he/she has not received an answer from the supervisory authority within three months from the date of filing his/her complaint for violation of the right to the protection of personal data [art. 78 par. (2) GDPR], or

- he/she has received a response from the supervisory authority in the form of a legally binding decision, which the data subject considers not satisfactory and decides to bring it to court [art. 78 par. (1) GDPR].

According to art. 78 par. (3) GDPR, the court having jurisdiction over the action against the supervisory authority is that of the place where the supervisory authority is established.

The object of legal action being the challenging of an administrative act, jurisdiction will lie with a court of administrative jurisdiction of the place of the supervisory authority establishment. Territorial jurisdiction will be determined using the rules of the court seized. The Brussels I Regulation is not applicable because the supervisory authority acts by virtue of its public power invested by the State on whose territory operates, and according to art. 1 par. 1 of the Brussels I Regulation this applies to civil and commercial matters (Brkan, 2015: 8; Van Calster, 2016: 30).

### *2.2.2. Civil action brought against a controller/processor*

The data subject has at his/her disposal two types of actions: an action for the defence and restoration of his/her violated right (a) and an action for compensation (b). Both actions may take the form of a class/collective action [art. 80 GDPR] (c).

#### *(a). The action for the defence and restoration of the violated right*

According to art. 79 par. (1) GDPR the data subject has the right to take legal action if he/she considers that his/her right to data protection has been violated as a result of data processing without complying with GDPR provisions.

The breach of a right in this case of a non-patrimonial personal right leads to a negative consequence, which may be of a varied nature. If this negative consequence is quantified in a patrimonial manner, it then takes the form of damage, which can be repaired by awarding compensation (Vasilescu, 2012: 571-575).

The data subject has to prove that he/she has suffered damage by the infringement of his/her right to data protection. This damage can be material or non-material. The data subject may consider that the restoration of the violated right requires financial compensation, and then claim it under the art. 82 GDPR, or may ask only for non-patrimonial repairs. The purpose of the action in the latter case is the restoration of the violated right by the cessation of the infringement or by other means provided by law.

If, for example, the data subject chooses to seize a court in Romania, he/she may use the provisions of art. 253 Civil Code, according to which, it

may request either the cessation of the violation and the forbidding of the unlawful act for the future if it is in progress, or the ascertaining of the unlawful character of the act, if the harmful effect persists. The data subject may at the same time require the court to oblige the author of the unlawful act to restore the violated right, either by ordering the author, at his expense, to publish the judgment establishing the violation of the right to the protection of personal data or by any other necessary measures to end the unlawful act or to repair the damage caused.

### *(b). The action for compensation*

Under art. 82 GDPR, *any person* may claim compensation for material or non-material damages caused by the controller/processor as a result of an infringement of the GDPR.

Since the term „any person" is used, this means that not only the data subject may ask for compensation, but also any other person who has suffered damage resulting from the violation of the GDPR provisions.

The GDPR does not specify who are the other persons, other than the data subject, that could be entitled to compensation. This means that the court seized will apply its own rules to determine this issue.

What rules are going to be applied in Romania? In a draft law on the implementation of GDPR it is stipulated that Law 677/2001 (the special law currently in force) will be repealed on the date when the GDPR will start to be applied, meaning from the 25th of May 2018. The Romanian Civil Code (art. 77) refers to the special law for any aspect related to the right to the protection of personal data. With the repealing of the special law (Law 677/2001), the only special law in force will be GDPR. Regarding the issues left unresolved by GDPR which provisions will be applied? A possible answer would be the general provisions of the Civil Code which regulate the protection of personal non-patrimonial rights, the right to the protection of personal data being one of them (art. 252-257) and the rules on contractual and tort civil liability, which are appropriate for each individual situation.

For example, if the data subject was fired due to the fact that a controller had processed his/her personal data in violation of the GDPR and this person had a legal obligation to maintain his/her minor children, theoretically the latter, under art. 82 GDPR, have the right to claim for compensation directly from the controller, who is responsible for repairing the damage suffered by the children, meaning being left without maintenance. It is what in Romanian legal literature is called *damage by ricochet* or *ricochet loss* (Vasilescu, 2012: 578). The plaintiffs should prove the causal

relationship between the wrongful act and the damage and the link with the data subject.

The lawsuit for damages is filed against the controller involved in the data processing operations. If the damage was caused by a processor, it is liable for the damage caused by processing only in the case of non-compliance with obligations of GDPR specifically directed to processors or in the case of an action outside or contrary to lawful instructions of the controller [art. 82 par. (2) GDPR].

Both the controller and the processor are exempt from liability if they prove that they are not responsible in any way for the event that caused the damage [art. 82 par. (3) GDPR].

The controller and the processor are held liable for the entire damage towards the data subject who has suffered the damage. If a controller or a processor has paid full compensation for the damage, that controller or processor is entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage [art. 82 par. (4) and (5) GDPR].

*Courts having jurisdiction to hear disputes*.

The data subject may opt between several competent jurisdictions, meaning he/she could do *forum shopping* in this case, as well. Thus, according to art. 79 par. (2) GDPR data subject may seize:

- The court of the Member State where the controller or the processor has *an establishment*. The data subject may choose *any establishment* of the defendant, regardless of whether this is its principal place of business or only a branch or a subsidiary. This possibility for the data subject is derived from the textual wording ("*an establishment*" rather than "*the establishment*") and aims to protect the data subject, who is considered to be vulnerable (by giving him/her more options).

- The court of the Member State where the data subject has his/her habitual residence. Regarding the notion of habitual residence, the issues discussed above when analysing the administrative way are also applicable here. If the controller or the processor is a public authority of a Member State acting in the exercise of its public powers, the only competent court is that of the defendant`s seat. As a rule, in this case, the defendant`s seat coincides with the plaintiff`s habitual residence.

### *(c). Class/collective actions*

In art. 80 GDPR are regulated two forms of class action: the first one refers to the data subject right *to mandate* a not-for-profit body,

organisation or association to act on his/her behalf, having its mandate to take all legal steps relating to the protection of his/her personal data; in the second one, the not-for-profit body, organisation or association acts *independently* of the data subject`s mandate, having the possibility to exercise all the rights granted to the data subject, if it is considered that the rights of a data subject under GDPR have been infringed as a result of the processing.

Class action originates in common law legal system. A class action is a legal procedure which enables many individuals who may *collectively* bring individual actions having the same object or a similar object against the same defendant to act as a group, their claims being determined in the one suit (Mulheron, 2006: 3) and therefore presents notable advantages as lower litigation costs, opportunity for plaintiffs to seek relief for small amounts of money, greater judicial efficiency and uniformity in dealing with similar cases.

The first form of class action in GDPR is the so called *opt-in class action*. Members of a group become parties to the class action only if they are willing to do so; according to the GDPR, the data subjects injured by a controller/processor give mandate of representation to a not-for-profit body, organisation or association, which will be the joint representative of all the data subjects.

The second form of action class in GDPR is the so called *opt-out class action*. Members of a group are represented by a not-for-profit body, organisation or association in an action against a defendant without expressing their consent. Only in the case they *do not* want to participate in the collective action they have to manifest their volition (Dobson, 2016: 184).

In order to act on behalf of the data subject, with or without his/her mandate, the not-for-profit body, organisation or association must meet three conditions:

- have been properly constituted in accordance with the national law of a Member State,
- have statutory objectives which have to be of public interest,
- be active in the field of protection of data subjects` rights and freedoms with regard to the protection of their personal data.

The legal steps the not-for-profit body, organisation or association may take on behalf of the data subject involves the lodging of a complaint with the supervisory authority, the exercise of legal proceedings against the supervisory authority or against the data controller or processor, as well as the exercise of the right to receive compensation. *All these legal steps are*

*admissible only if they are acknowledged by the national law of the Member State in which the seized court or authority is located.*

Member States are free to regulate these types of class action. In GDPR there are not any rules on this matter. Although binding rules have not been adopted in EU law, but only recommendations, the current trend is to admit class action procedures in continental law, as well. Following the European Commission Recommendation no. 2013/396/EU on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law (European Commission, 2013), more than half of the Member States have complied with the Recommendation and have adopted legislation in this field. The Recommendation aimed at establishing a general framework with principles applicable to violations of rights *in all areas*.

Sectorial, all Member States, including Romania, have in their national laws provisions on *actions for an injunction* resulting from the transposition of Directive no. 2009/22/EC on injunctions for the protection of consumers` interests (European Parliament, 2009)[6]; on *actions for damages* following the transposition of Directive no. 2014/104/EU on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (European Parliament, 2014)[7]; on *actions mounted by consumer associations with a view to eliminating unfair terms in consumer contracts*, following the transposition of Directive no. 93/13/EEC on unfair terms in consumer contracts (European Parliament, 1993)[8].

In Romania, the general framework for the admissibility of collective actions is found in art. 37 Code of Civil Procedure, according to which "In cases and conditions stipulated *exclusively by law*, claims, defences and actions may be filed by persons, organizations, institutions or authorities who, without justifying a personal interest, act to protect the rights or legitimate interests of persons in special situations or, where appropriate, to protect a

[6] The Directive has been transposed into Romanian legislation by Government Decision no. 1553/2004 on certain modalities for cessation of illicit practices in the field of the protection of consumers' collective interests (Romanian Gorvernment, 2014).

[7] The Directive has been transposed into Romanian legislation by Government Emergency Ordinance no. 39 of 31 May 2017 on damages actions in cases of violation of the provisions of the competition law, as well as for amending and completing the Competition Law no. 21/1996 (Romanian Government, 2017).

[8] The Directive has been transposed into Romanian law by Law no. 193/2000 regarding the abusive clauses in the contracts concluded between professionals and consumers (Romanian Parliament, 2000).

group or general interest.". There are no provisions on collective actions in special laws, except for those listed above, as a result of the transposition of European directives. These are not, however, applicable to the protection of personal data. Therefore, although according to art. 80 GDPR collective actions can be brought in courts, in the absence of a law regulating them, in Romania the class actions lawsuits are put on hold.

Meanwhile, collective actions may be brought using different legal vehicles like the joinder of cases or the assignment of claims (European Commission, 2018: 2).

Another solution that could be practiced by data subjects with habitual residence in Romania would be to bring legal proceedings against a controller/processor in a court of a Member State where the controller/processor has an establishment and collective redress mechanisms are available. The data subject could mandate a not-for-profit body, organisation or association constituted under the law of that Member State to sue on his/her behalf or could become a member of such a not-for-profit body, which would act independently of his/her consent in case it ascertains infringement of the right to the protection of personal data.

Before starting the application of GDPR, the ECJ faced such a situation in case C-498/16 - Judgment of 25 January 2018 – (ECJ, 2018). The plaintiff, Mr. Schrems, filed an action against Facebook in Vienna, Austria, on his own behalf, as well as an assignee of the claims of other seven data subjects with habitual residence in other EU Member States as well as in non-EU countries. Schrems is the founder of a non-profit association, NOYB (https://noyb.eu/), based in Austria. The plaintiff was not, however, NOYB, but Schrems. According to Austrian law, a class action can be brought by forming an *ad hoc* group, which assigns their rights to a representative (Shelley, 2015).

## Conclusions

The data subject with habitual residence in Romania has several legal remedies at his/her disposal for protection of the fundamental right, the right to the protection of personal data. These remedies multiply if one takes into consideration the data subject possibility of doing *forum shopping* under the conditions provided in the GDPR.

According to art. 77-82 GDPR, the data subject may initiate *administrative proceedings* and *judicial proceedings*. Judicial proceedings may be conducted after or in parallel with, and independently of, administrative proceedings.

The determination of the competent authority to restore the violated right depends on the qualification of the legal situation and the path that the data subject chooses to follow: the administrative pathway or the judicial one.

For the data subject with habitual residence in Romania one of the most provocative ways of restoring the violated right is the use of a class action. Until the adoption of a national legislation on class action, the data subjects have an open path through the not-for-profit bodies set up in states with appropriate legislation. We consider that class actions will be the most beneficial way to repair the damages suffered by the data subjects, even in cases in which the controller/processor imposes clauses prohibiting class actions in adhesion contracts, as an adversarial reaction. Can these clauses be effective? The answer is a complex one and it depends on the law applicable to personal data disputes.

## References

Brkan, M. (2015). Data protection and european private international law. In *Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2015/40* (pp. 1-38). doi:10.2139/ssrn.2631116

Charter of Fundamental Rights of the European Union. (2012). *Official Journal of the European Union, C 326*, 2012, October 26.

Dodson, S. (2016). An opt-in option for class actions. *Michigan Law Review*, *115*(2), 171-2013.

European Commission. (2013). Recommendation no. 2013/396/EU of the European Commission on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law. *Official Journal of the European Union, L 201*, 2013, July 26.

European Commission. (2018). *Report on the implementation of the Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union law (2013/396/EU).* Retrieved from http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52018DC0040

European Court of Justice (ECJ). (2003). *Case of Bodil Lindqvist (C-101/01).* Retrieved from http://curia.europa.eu/

European Court of Justice (ECJ). (2018). *Case no. C-498/16, Maximilian Schrems v Facebook Ireland Limited.* Retrieved from http://curia.europa.eu/juris/liste.jsf?num=C-498/16

European Parliament. (1993). Directive no. 93/13/EEC on unfair terms in consumer contracts. *Official Journal of the European Union, L 95*, 1993, April 21.

European Parliament. (1995). Directive 95/46/EC 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. *Official Journal of the European Communities, L 281*, 1995, November 23.

European Parliament. (2009). Directive 2009/22/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interests. *Official Journal of the European Union, L 110*, 2009, May 01.

European Parliament. (2012). Regulation (EU) No. 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. *Official Journal of the European Union, L 351*, 2012, December 20.

European Parliament. (2014). Directive no. 2014/104/EU on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union. *Official Journal of the European Union, L 349*, 2014, December 05.

European Parliament. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.* Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union Agency for Fundamental Rights (FRA), & Council of Europe (CE). (2014), *Handbook on European data protection* law. Retrieved from https://rm.coe.int/16806b294a

European Union Agency for Fundamental Rights (FRA). (2014). *Access to data protection remedies in EU Member States. Summary*. Retrieved from http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states

Hetz, R., & Binnie, I. (2017). *Facebook sanctionné en Espagne sur la protection des données* [Facebook sanctioned in Spain on data protection]. Retrieved from https://fr.reuters.com/article/technologyNews/idFRKCN1BM1W3-OFRIN

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford, UK: Oxford University Press.

Mulheron, R. P. (2006). *The class action in Common Law legal systems: A comparative perspective.* Portland, USA: Hart Publishing.

Romanian Government. (2004). HG 1553/2004 republicată 2011 privind unele modalităţi de încetare a practicilor ilicite în domeniul protecţiei intereselor colective ale consumatorilor [Government Decision no. 1553/2004 on certain modalities for cessation of illicit practices in the field of the

protection of consumers' collective interests]. *Monitorul Oficial al României, 695*, 2011, September 30.

Romanian Government. (2017). Ordonanța de urgență nr. 39/2017 privind acțiunile în despăgubire în cazurile de încălcare a dispozițiilor legislației în materie de concurență, precum și pentru modificarea și completarea Legii concurenței nr. 21/1996 [Government Emergency Ordinance no. 39 of 31 May 2017 on damages actions in cases of violation of the provisions of the competition law, as well as for amending and completing the Competition Law no. 21/1996]. *Monitorul Oficial al României, 422*, 2017, June 08.

Romanian Parliament. (2000). Legea nr. 193/2000 privind clauzele abuzive din contractele încheiate între profesioniști și consumatori [Law no. 193/2000 regarding the abusive clauses in the contracts concluded between professionals and consumers]. *Monitorul Oficial al României, 543*, 2012, August 03.

Romanian Parliament. (2001). Legea nr. 677 din 2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date [Law no. 677/2001 for the protection of individuals with regard to the processing of personal data and on the free movement of such data]. (2001). *Monitorul Oficial al României, 790*, 2001, December 12.

Șandru, S. (2016). *Protecția datelor personale și viața privată* [Personal Data Protection and Privacy]. Bucharest, Romania: Hamangiu.

Schneider, F. (2017). Données personnelles, Facebook condamné par la Cnil [Personal data, Facebook condemned by CNIL]. Retrieved from https://www.la-croix.com/Sciences-et-ethique/Numerique/Donnees-personnelles-Facebook-condamne-Cnil-2017-05-17-1200847843

Schwartz, P. M., & Solove, D. J. (2012). Reworking privacy law. A memorandum regarding future ALI projects about information privacy law. Retrieved from https://law.duke.edu/sites/default/files/images/centers/judicialstudies/Reworking_Info_Privacy_Law.pdf

Shelley, M. (2015). Towards a uniform European approach to collective redress? *Newsletter of the Consumer Litigation Committee, International Bar Association Legal Practice Division.* Retrieved from file:///C:/Users/User/Downloads/StateofEUClassActions%20(2).pdf

Stone, P. (2010). *EU private international law* (2nd ed.). Cheltenham, UK: Edward Elgar Publishing.

Treaty on the Functioning of the European Union (TFEU). (2012). *Official Journal of the European Union, C 326*, 2012, October 26.

Ungureanu, C. T. (2015). Contractul cloud computing în comerțul international [Cloud Computing Contract In International Trade]. *Revista moldovenească de*

*Drept Internațional și Relații Internaționale*, *37*(3), 25-36. Retrieved from http://rmdiri.md/wp-content/uploads/2015/01/RMDIRI-Nr.-3-20157.pdf

Ungureanu, C. T. (2017). Protecția datelor cu caracter personal în contractele internaționale [Personal Data Protection In International Contracts]. *Analele Ştiinţifice ale Universităţii "Alexandru Ioan Cuza" din Iaşi,* tom LXIII, *seria Ştiinţe Juridice, 2*, 139-141. Retrieved from http://pub.law.uaic.ro/

Van Calster, G. (2016). *European private international law*. Oxford, UK: Hart Publishing.

Vasilescu, P. (2012). *Drept civil. Obligații, în reglementarea Noului Cod civil* [Civil law. Obligations - in the regulation of the new Civil Code]. Bucharest, Romania: Hamangiu.

Voigt, P., & Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR). A practical guide*. New York, USA: Springer International Publishing.