LIFTING THE VEIL OF THE GDPR TO DATA SUBJECTS

Laura-Cristiana SPATARU-NEGURA[*]
Cornelia LAZAR[**]

Abstract

Every natural person is entitled to personal data protection regardless of his or her nationality, residence, race, age, gender, language, religion, political and other affiliations, ethnicity, social background and status, wealth, birth, education, social position or any other personal characteristic. Europe's clock is now ticking with regards to data protection: just in a few days, on 25 May 2018, a new EU data protection framework - the Regulation (EU) 2016/6791, will apply and will be directly applicable in all the Member States. This new General Data Protection Regulation governs the processing by an individual, a company or an organisation of personal data relating to individuals in the EU. Having in view the impact this regulation has for the entire world, we consider that it should be very well analysed.

The aim of this study is to raise awareness and improve knowledge of data protection rules established by the GDPR. It is recommended for legal professionals and non-specialist legal professionals, and other persons working in the field of data protection. Additionally, this study intends to provide guidance to data subjects as for their rights under the GDPR and to give some relevant examples from our daily life in which data breaches happen.

Keywords: *data protection, data subjects, GDPR, personal, Regulation (EU) 2016/6791.*

1. About Data Protection in Europe

This study provides an overview of the GDPR applicable to data protection in relation to the data subjects' rights. Data is personal data if it relates to an *identified* or at least *identifiable* natural person. If data about such a person is being processed, this person is called the "data subject". Personal data can be contained in computer files or in paper records (*e.g.* telephone numbers, addresses, financial information, photographs, satellite images, car registrations, ID numbers, e-mail addresses, health records).

Looking into the history of individual rights, we note that a right to protection of an individual's private life against intrusion from others (especially from the state), was for the first time foreseen in an international legal instrument in Article 12 of the United Nations Universal Declaration of Human Rights of 1948 on respect for private and family life:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks[1].

This legal provision influenced the development of other human rights instruments in Europe. At the European level, there are several pieces of legislation on data protection, created by both the European Union (hereinafter the "*EU*") and the Council of Europe (hereinafter the "*CoE*"), which have been applied by the international jurisdictions through the years (the case law of the Court of Justice of the European Union and of the European Court of Human Rights are relevant).

In the present, the main important acts in Europe are:

a) at the CoE level - the European Convention for Human Rights (Article 8 – Right to respect for private and family life, home and correspondence), as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Article 8 of the Convention recognizes the right to protection of personal data, which guarantees the right to respect for private and family life, home and correspondence, and lays down the conditions under which restrictions of this right are permitted. The Convention 108 is the only legally binding international instrument in the field of data protection.
b) at the EU level - the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

At the EU level, both primary and secondary EU law[2] regulates the data protection field. The primary EU law comprises the treaties, namely the Treaty on European Union (TEU), the Treaty on the Functioning of the European Union (TFEU), the Charter of Fundamental Rights of the European Union. The secondary EU law comprises the regulations, directives and decisions of EU adopted by the EU institutions.

[*] Assistant Professor, PhD, Faculty of Law, "Nicolae Titulescu" University, Bucharest (e-mail: negura_laura@yahoo.com).
[**] Data Protection Officer, E-solution Manager, Ecoprotech Engineering, Green Group (e-mail: cornelia_gabor@yahoo.com).
[1] Available online at http://www.un.org/en/universal-declaration-human-rights/.
[2] For more information on sources of EU law, please see Nicolae Popa, Elena Anghel, Cornelia Ene-Dinu, Laura-Cristiana Spataru-Negura, *Teoria generala a dreptului. Caiet de seminar*, third edition, C.H. Beck Publishing House, Bucharest, 2017, p. 153.

As mentioned above, the main EU legal instrument on data protection, in force at this moment, is the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the "*Data Protection Directive*")[3].

From 25 May 2018 the only binding legal instrument at the EU level shall be the General Data Protection Regulation (hereinafter the "*GDPR*") - Regulation (EU) 2016/679[4]) adopted on 27 April 2016. By this regulation, the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the EU. When the GDPR shall take effect, it will replace the 1995 Data Protection Directive.

Because of the importance of the data protection field, the EU institutions have decided to adopt this piece of legislation through a regulation (instead of a directive) because unlike a directive, it does not require domestic governments to pass any enabling legislation and so it is directly binding and applicable[5].

The GDPR provides data subjects with several rights that can be enforced against undertakings that process personal data. All undertakings acting as controllers are directly affected by the rights afforded to data subjects, while the undertakings acting as processors are affected to a lesser degree.

In Article 1 paragraph (1) of the GDPR it is underlined that:

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

According to Article 4 paragraph (1) of the GDPR, there is no need for high-quality identification of the data subject; it is sufficient that the natural person concerned be identifiable:

'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

A person shall be considered identifiable if a piece of information contains elements of identification through which the person can be identified, directly or indirectly.

The data subjects have several rights under the GDPR (please see Chapter 3 of the GDPR - *Rights of the data subject*).

For instance, Article 12 of the GDPR regulates the need of "*[t]ransparent information, communication and modalities for the exercise of the rights of the data subject*". In order that the data subject understand the information provided by the controller, the latter must use "*a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*"[6]. Additionally, the "*information shall be provided in writing, or by other means, including, where appropriate, by electronic means*"[7] or orally (when the data subject requested it specifically, provided that the identity of the data subject is proven by other means.

We consider that such information given to the data subject should not consist of privacy policies that are difficult to understand or excessively lengthy.

This communication between the controller and the data subject shall be done "*without undue delay and in any event within one month of receipt of the request*"[8]. This deadline may be extended by two further months where necessary, depending the complexity and number of the requests, but the controller shall have to inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Usually, the controller shall communicate the information free of charge (except for the cases when the requests from a data subject are manifestly unfounded or excessive, raising a problem of repetitiveness)[9]. In this kind of bad faith situations, the controller shall be able to charge a reasonable fee to the data subject (for the administrative costs incurred) or to refuse to act on the request, but the controller shall have to demonstrate the manifestly unfounded or excessive character of the request.

To limit the risk that third parties gain unlawful access to personal data, under the GDPR the controllers should require data subjects to provide proof of identity before giving effect to their rights.

According to Articles 13-15 of the GDPR, the data subject shall have the right to obtain information and access to personal data. Depending if the personal data has been or not obtained from the data subject, the legal provisions are different (Article 13 of the GDPR

[3] Available online at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

[4] Available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

[5] For more information on different types of EU legislation, please see Augustin Fuerea, *Dreptul Uniunii Europene*, Universul Juridic Publishing House, Bucharest, 2016, p. 45 and following; Mihaela Augustina Dumitrascu, Roxana Mariana Popescu, *Dreptul Uniunii Europene, Sinteze si aplicatii. Editia a II-a, revazuta si adaugita*, Universul Juridic Publishing House, Bucharest, 2015, p. 120 and following; Laura-Cristiana Spataru-Negura, *Dreptul Uniunii Europene – o noua tipologie juridica*, Hamangiu Publishing House, Bucharest, 2016, p. 92 and following.

[6] Please see Article 12 paragraph (1) of the GDPR.

[7] *Idem.*

[8] Please see Article 12 paragraph (2) of the GDPR.

[9] Please see Article 12 paragraph (5) of the GDPR.

when collected from the data subject and Article 14 when not been obtained from the data subject). In both cases, the controller shall provide the data subject with certain information (*e.g.* the identity and the contact details of the controller, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the recipients or categories of recipients of the personal data, the period for which the personal data will be stored, the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability, the right to lodge a complaint with a supervisory authority), except for the case when the data subject already had the information [Article 13 paragraph (4) and Article 14 paragraph (5) letter a) of the GDPR].

According to Article 15 of the GDPR, the data subject is entitled to obtain from the controller "*confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data*" and certain information.

Section 3 of Chapter 3 of the GDPR regulates the rectification and erasure rights of the data subject. In relation to the right of rectification, the position taken through the GDPR is mostly the same as in the Data Protection Directive.

It is normal that in case of errors of personal data regarding a data subject, he or she must be entitled to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Even in case of incomplete personal data, the data subject shall have the right to have complete the respective information, including by means of providing a supplementary statement.

In certain cases (*e.g.* the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing, the personal data have been unlawfully processed), the data subject shall be entitled to obtain from the controller the erasure of personal data concerning him or her, without undue delay. Therefore, the controller shall have the obligation to erase the respective personal data without undue delay. We consider that the GDPR created a broader right to erasure than the Data Protection Directive, therefore the undertakings shall face a broader spectrum of erasure requests than during the Data Protection Directive.

There are certain exceptions to this right (*e.g.* if the processing is necessary for exercising the right of freedom of expression and information, for reasons of public interest in the area of public health, for the establishment, exercise or defence of legal claims)[10].

Under Article 18 of the GDPR, the data subject shall be entitled to obtain from the controller restriction of processing in certain situations (*e.g.* the data subject contests the accuracy of the personal data enabling the controller to verify the accuracy of the personal data, the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead, the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims).

In case of rectification or erasure of personal data or restriction of processing, the controller shall be held to send a notification "*to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it*"[11].

The data subjects have also a new right under the GDPR - the right to data portability. This means that individuals are allowed to obtain and reuse their personal data for their own purposes across different services. This right allows them to copy or transfer personal data easily from one IT environment to another, in a safe and secure way, without hindrance to usability. For certain undertakings, this new right creates a significant additional burden, requiring substantial investment in new systems and processes, while for other undertakings creates a significant opportunity to attract customers from the competitors.

In case the data subjects are not satisfied because of the data processing, they have the right to object, at any time, to processing of personal data concerning them[12]. Controllers are obliged under the GDPR to provide additional information to data subjects regarding this right, and we consider that this will require revisions to standard data protection policies and privacy notices.

The GDPR preserves the position taken through the Data Protection Directive (with only minor amendments) regarding the right to not be evaluated based on automated processing. According to Article 22 of the GDPR, the "*data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*". However, Article 22 paragraph (2) letter c) of the GDPR clarifies that the explicit consent of the data subject is a valid basis for evaluation based on automated profiling.

The rights enshrined in Chapter 3 of the GDPR can be subject of certain restrictions imposed by the EU or the Member States legislation, if "*such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:*

a) national security;

[10] Please see Article 17 paragraph (3) of the GDPR.
[11] Please see Article 19 of the GDPR.
[12] Please see Article 21 of the GDPR.

b) defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
i) the protection of the data subject or the rights and freedoms of others;
j) the enforcement of civil law claims"[13].

In the next section we aim to give several examples to frame certain situations that come under the GDPR, in order to see concretely how data protection influences our lives.

2. The Impact of the GDPR on Data Subjects, Data Controllers and Data Processors. Remedies and Sanctions

2.1. Analyzing the Impact of the GDPR on Data Subjects

GDPR will completely change the interaction of data subjects with the undertakings that have access to their personal data. Through the GDPR's right to information not only will they become more aware on what personal data is, but also on how granulated and microscopic data - when correlated - can lead to big data analysis.

The information mechanisms developed by the national and European data protection authorities will play a major role in raising awareness regarding the data subject's rights under GDPR. The Article 29 Working Party has already developed a set of Guidelines regarding GDPR's main articles implementation – with respect to the data subject's right, so that GDPR compliance becomes more at ease.

GDPR compliance becomes thus, a blessing for data subjects, while for online platforms, marketers, banking and insurance institutions it becomes a real challenge.

Online platforms and mobile applications (such as LinkedIn, Facebook, Google) must adapt their policies regarding the usage and sharing of personal data, so that they become compliant with the GDPR. The mechanisms through which online platforms inform their users regarding the collection, storage, sharing and usage of their data must be changed so that the opt in to different services will no longer be automated or preselected, and will become, starting with 25 May 2018, an aware, fully responsible given consent. Thus, we will no longer witness automatical subscription to email marketing, automatic sharing of data between platforms or cross platform integrations without our given consent. We are underlining the importance of awareness related to GDPR's definition of consent, as consent can no longer be subject to interpretation – when giving consent the user must be informed on the following information: the type of data that the platform collects, how the data is being used, with whom it is shared, where it will be transferred, and, most importantly, for how long it will be retained. In their quest for GDPR compliance, platforms rush into reconstructing their pages so that the user is properly informed.

One of the largest online banking platforms – PayPal - just revealed a list of partners to which the platform might share your personal data with: a list of "just" 690 comercial partners (banks, marketers, call centers) and authorities (*e.g.* international agencies, fiscal entities) to whom PayPal might reveal some of your most important data: *e.g.* full name, banking account, business details, contact details, transactions details. Prior to 1 January 2018, the webpage did not contain any of the above-mentioned information and none of its users really knew to whom PayPal revealed the information to[14].

Besides being informed on what data will be processed and in what way, from the very moment when creating a user account on an online platform, starting with 25 May 2018, the data subjects will be able to ask data controllers access to what personal data they hold on them. We should see to what extent large social platforms (*e.g.* Facebook) will also give access on the data they historically collected before the 25 May 2018. It would be logic for the data subject to have access both to present and hystorical data, as long as the platform continues to use hystoric data.

The most recent privacy case related to Facebook dates back to February 2018, when a Belgian court threatened to fine the social giant with 250,000 euro a day or up to 100,000,000 EUR if Facebook continues to track people on third party websites and does not delete all data on Belgium citizens holding an account on the platform or not[15]. Just a short Google search using the following keywords "Facebook fined privacy", will lead to no less than 8 million results.

[13] Article 23 paragraph (1) of the GDPR.
[14] List available online at https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list.
[15] Available online at https://www.reuters.com/article/us-facebook-belgium/facebook-loses-belgian-privacy-case-faces-fine-of-up-to-125-million-idUSKCN1G01LG.

In 2017, a Spanish court fined Facebook with 1,200,000 EUR after the national data protection agency proved that Facebook collected and used utilized personal data for advertising purposes[16]. The platform had been collecting data on people's sex orientation and religious beliefs both from the Facebook platform and third-party platforms, without consent.

This was one of the first times when multiple data protection agencies in Europe cooperated on an investigation against a large player on the online market. The Spanish data protection agency cooperated with the other agencies from Belgium, France, Hamburg and the Netherlands, and succeeded in proving that Facebook did not inform its users, or third party websites's users, that they were collecting data and to what extent they were using it.

The findings were surprising: user data was being collected with the help of third party cookies[17] placed on Facebook pages or third-party websites. The cookies were collecting data on the user behaviour on the internet pages on which Facebook had placed its cookies (through the *Like* button). Moreover, it further processed the special character collected data - such as religious and sexual orientation - and profiled users, so they could be targeted with marketing campaigns. At no time the users could perceive that their data was being collected, nor did they know how the social giant was going to use it – the purpose and the extent to which Facebook or its partners will use it. What seems even more tragic is that people who never intended to use a social platform such as Facebook had their personal data collected and used simply by browsing websites.

Meanwhile there are constant debates on how Facebook surprises us each time we navigate. Imagine that behind every surprise you get from Facebook there is huge amount of data the platform gathers about you. We should debate few examples here: Facebook knows when you became friends with someone and congratulates you on that, it knows when you were born so it can say happy birthday – and it shares that information with friends and even friends of friends – maybe even with its commercial friends?!

However, while most of us are aware and agree to the above, we may not agree with Facebook keeping information of a picture we took with our phone (the metadata of the picture - timestamp or location, type of camera/phone), it may store our IP address and even smarphone unique identifier, if you are using Facebook on a dayly basis the platform even knows when you wake up and you go to sleep, all based on your usage behaviour[18]. All this information mixed with artificial intelligence could lead to numerous abuse cases.

Starting with 25 May 2018, with GDPR compliance in place, people will no longer be subject to such condemnable practices, as cookies policies will no longer be tacitly accepted – the active consent becoming a must. Moreover, special data can no longer be processed without explicit consent, and some countries have even suggested banning the usage of special data.

GDPR enforces both data subjects and data protection agencies. Data protection agencies are now able to emit sanctions and fines on their own, which until now, in certain countries, was only possible with the help of the courts of law.

One of the most important missions of GDPR was to protect children data subjects and their personal data. Starting this year children data can no longer be processed without the explicit consent of an adult.

In 2016, the largest top toy companies in the United States were fined for using tracking technologies on popular children websites: Viacom had to pay 500,000 USD, Mattel 250,000 USD, JumpStart 85,000 USD[19].

A more proeminent case of 2017 just crushed parent's trust in new generation toys. Parents in Germany were advised to destroy a doll that could spy their children[20]. The name of the spying doll was Cayla and it could be accessed through the internet with the help of a voice recognition software. Moreover, the doll could be controlled with the help of an application. The Bluetooth connection to the doll proved to be so unsecure that any hacker within 15 meters could listen to what happened near the doll and directly speak to the child playing with it. The case raised a huge debate on smart toys and tracking devices related to children usage.

In 2018 some of the European countries banned the usage of smart watches by children. In Germany the above-mentioned case ended with a cooperation between the national data protection and consumer protection agencies.

Artificial intelligence related to toys connected to the internet, will be raising huge problems in the future. Imagine the power of a toy who learns how to speak while interacting with children around the world. GDPR comes just in time to assure that children are protected from abuse.

As for Romania, in May 2016, the Romanian Fiscal Authority published a list of all citizens having outstanding tax payments at that time, also entitled "the

[16] Available online at http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_11-iden-idphp.php.

[17] According to the Tech Terms Computer Dictionary, a "cookie" is a small amount of data generated by a website and saved by your web browser. Its purpose is to remember information about you, similar to a preference file created by a software application. Please see https://techterms.com/definition/cookie).

[18] Please see https://9to5mac.com/2018/03/12/how-to-download-your-facebook-data/amp/.

[19] Please see http://www.dailymail.co.uk/sciencetech/article-3787859/NY-settles-4-companies-stop-tracking-children-online.html.

[20] Please see http://www.bbc.com/news/world-europe-39002142.

shaming list"[21]. It is very interesting that certain payables were contested in the Romanian courts of law, therefore they were very likely to be amended or even cancelled. In this respect, the Romanian data protection authority applied a fine on the Fiscal Authority based on fine capping under current Data Protection Law, amounting to 16,000 RON (approximately 3,500 EUR).

2.2. Analyzing the Impact of GDPR on Data Controllers and Processors

GDPR poses huge amount of pressure on data controllers and processors. It raises a lot of issues that were inexistent until now and both controllers and processors are prone to huge financial efforts in becoming compliant to GDPR.

Establishing internal procedures, applying them and following their implementation presupposes a considerable effort, especially for non-EU entities that process European citizens' personal data.

PwC Canada – through the voice of its privacy director, Mr. Constantine Karbaliotis – conceived a "nightmare letter" that comprised the requests of a data subject after the 25 May 2018[22]. The letter gives a striking image on all the possible requests of an informed data subject under the GDPR, such as:

- access to personal data pursuant to Article 15 of the GDPR;
- 30 days deadline to response – according to Article 12 of the GDPR;
- access to information regarding the collected type of data, data storage;
- request of a copy of the data in readable format;
- access to a list of third party to whom data is revealed to;
- details on the legal grounds for each type of data processing activities and data transfers;
- details regarding the retention period;
- if data from third party sources is being also processed;
- information on automated decision making or profiling – Article 22 of the GDPR;
- if a data breach has ever taken place;
- information on security measures of protecting data (*e.g.* encryption, minimization, anonymization).

The real challenges of the implementation under the GDPR are related to the following rights of the data subjects: access to a copy of the data, data portability, data erasure – the right to be forgotten.

For most undertakings, the right of the data subject to request a readable copy of all the data that they store on the data subject will be a challenge. Data could be stored in different platforms: CRMs excel files on different employees' computers, emails containing email signatures or archives of the emails, online cloud platforms, backups of individual computers or servers in the cloud or even physical archives stored in the other part of the world. If the previous internal procedures of the companies have not included an inventory of the personal data or policies on data storage, retention and circulation, it will be a real challenge to respect the rights to access, portability or erasure.

The right to data portability raises real problems in relation to competition laws and undertakings will be challenged to respect the data subject's right to transfer data to a competitor. The Article 29 Working Party revised its guidelines on the right to data portability on 5 April 2017, giving more light on the elements of data portability, when data portability applies, how general rules governing the exercise of data subjects' rights apply to data portability and how data must be provided in case of portability[23].

However, national competition laws are often not aligned to the GDPR so undertakings might get cought in the middle. In this view, national authorities are also in a race to become GDPR compliant. Starting with human resources related laws and ending with public authorities' policies, the GDPR is being implemented at national levels.

On 14 March 2018, the Romanian Senate published on its website a bill of law in application to the GDPR[24]. According to this bill, the Romanian law shall be more restrictive than the GDPR in certain aspects (*i.e.* Article 3 prohibits the processing of biometric or genetic data other than by public authorities). This bill intends to bring clearance to the processing of the unique identification number under Article 4 and human resources data processing under Article 5. With regards to the "the shaming list" published by the Romanian Fiscal Authority in 2016 mentioned above and to the fine applied in the respective case, please note that this bill of law proposes that fines applicable to public authorities will be no greater than 200,000 RON (approximately 43,000 EUR). We shall follow interestedly the legislative process in order to find out the final version of this piece of legislation.

2.3. Remedies and Sanctions

Rights under data protection law can be exercised by the data subject affected or by a "not-for-profit body, organisation 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"[25]. The GDPR clarifies the requirements regarding claims brought by

[21] Please see https://economie.hotnews.ro/stiri-finante-21000512-fiscul-publicat-lista-persoanelor-fizice-datorii-peste-1-500-lei-peste-187-230-romani-restante-fiscale-care-insumeaza-3-4-miliarde-lei.htm.
[22] Please see https://www.linkedin.com/pulse/nightmare-letter-subject-access-request-under-gdpr-karbaliotis/.
[23] Please see https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf.
[24] Please see https://www.senat.ro/legis/lista.aspx.
[25] Please see Article 80 of the GDPR.

third parties on behalf of data subjects. We also consider that these associations can seek judicial remedies and compensation from controllers and processors, on behalf of multiple data subjects (in collective claims that are similar to class action litigation). It is obvious that in case of minors, they shall be represented by their parents or guardians.

Chapter VIII of the GDPR governs the legal problem of remedies, liability and penalties in case of breach of this regulation. From the analysis of the remedies and sanctions chapter, it appears that the GDPR takes a multi-layered approach for breach of its provisions. Although it sets out the high-level principles and maximum administrative fine amounts, the regulation leaves some latitude to the EU Member States as to how these remedies and sanctions will operate in practice.

According to Article 77 of GDPR, if a data subject considers that the processing of personal data relating to him or her infringes the GDPR, then he or she has the right to lodge a complaint with a supervisory authority, without prejudicing any other administrative or judicial remedy under the GDPR. This complaint can be lodged either where the data controller or data processor has its establishment or in the place of habitual residence of the complainant data subject. The respective supervisory authority shall have to inform the data subject on the progress and the outcome of the complaint, mentioning the possibility of a judicial remedy. We underline that under the "One-Stop-Shop" provided by the GDPR, the supervisory authority to which the complaint is addressed will not necessarily be the authority that is responsible for regulating the relevant controller.

As for the effective judicial remedy against a supervisory authority governed by Article 78 of the GDPR, it is worth mentioning that every natural and legal person shall have the right to bring such a claim if it concerns them[26]. This right shall be exercised where the competent supervisory authority:

a) does not handle a complaint;
b) does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77 mentioned above. These proceedings shall be brought before the courts of the Member State where the supervisory authority is established. If these proceedings were preceded by an opinion or decision of the Board in the consistency mechanism, then the supervisory authority is bound to forward it to the court, the GDPR not stressing a sanction if this obligation is not respected.

Additionally, according to Article 79 of the GDPR, the data subject has the right to bring proceedings against a controller or a processor, before the courts of the Member State where that controller or processor is established, or where the data subjects has his or her habitual residence, "unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers"[27].

We consider that the GDPR provides greater clarity and legal certainty regarding the claims that can be brought by the data subjects than it was regulated through the Data Protection Directive.

Because of the possibility of the data subject to bring proceedings in different Member States (raising the problem that a controller or processor may be subject to legal proceedings in unfamiliar jurisdictions), the GDPR expressly regulates in Article 81 the suspension of proceedings: any competent court other than the first seized one may suspend its proceedings. We emphasize that the claims could be delayed if a national court decides to suspend proceedings pending the outcome of the case in front of the first seized court of law (in another Member State), being also possible that the outcome of the case in the second jurisdiction be influenced by the decision taken in the first seized court of law.

Every data subject who has suffered material or non-material damage, as a result of an infringement of the GDPR, shall be entitled to receive compensation from the controller or processor for the damage suffered. Data controllers and data processors can escape liability if they prove they are not in any way responsible for the event giving rise to the damage invoked by the data subject. Article 82 paragraph (5) of the GDPR expressly provides a "joint and several" liability, meaning that where a controller or processor has paid full compensation for the damage suffered by the data subject, that controller or processor shall be 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. This type of clause is needed for ensuring effective compensation of the data subject.

Unlike the Data Protection Directive which exempted data controllers from liability for harm arising in cases of force majeure, the GDPR contains no such exemption, meaning that the data controllers may bear the risk in force majeure cases.

Even though the concept of administrative fines for breaches of EU data protection law did not change a lot under the GDPR, there are significant changes to both the amount of fines and the factors relevant to determining those fines.

The GDPR also provides that the supervisory authorities are entitled to establish the imposition of administrative fines, on a case by case analysis. Article 83 of the GDPR establishes the criteria for deciding whether to impose an administrative fine and deciding

[26] Since the party against which are brought proceedings is a public authority, then the specificities of the administrative review shall be applicable. In this respect, please see Marta-Claudia Cliza, *Drept administrativ. Partea a II-a*, Editura Pro Universitaria, Bucuresti, 2011, p. 78 and following; Elena Emilia Stefan, *Drept administrativ. Partea a II-a*, Editura Universul Juridic, Bucuresti, 2013, p. 52 and following.

[27] Please see Article 79 paragraph (2) of the GDPR.

on the amount of the administrative fine in each individual case.

Although the GDPR establishes several amounts for the administrative fines, it is expressly mentioned that if "*a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*"[28].

The GDPR fundamentally changes the potential financial consequences of breaching EU data protection law, the level of the potential sanction depending on the breach and ranging from administrative fines of:

1. up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher[29] (for breach of principles such as "by design and by default", non-compliance with the processing related obligations, or failure to appoint a Data Protection Officer). The relevant articles in this respect are:

a) Article 8 (Conditions applicable to a child's consent in relation to information society services);
b) Article 11 (Processing which does not require identification);
c) Article 25 (Data protection by design and by default);
d) Article 26 (Joint controllers);
e) Article 27 (Representatives of controllers or processors not established in the Union);
f) Article 28 (Processor);
g) Article 29 (Processing under the authority of the controller or processor);
h) Article 30 (Records of processing activities);
i) Article 31 (Cooperation with the supervisory authority);
j) Article 32 (Security of processing);
k) Article 33 (Notification of a personal data breach to the supervisory authority);
l) Article 34 (Communication of a personal data breach to the data subject);
m) Article 35 (Data protection impact assessment);
n) Article 36 (Prior consultation);
o) Article 37 (Designation of the data protection officer);
p) Article 38 (Position of the data protection officer);
q) Article 39 (Tasks of the data protection officer);
r) Article 42 (Certification);
s) Article 43 (Certification bodies);

2. 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[30] (for breaches of the principles relating to processing or of the lawful processing requirements, and for breach of data subject rights). The relevant articles in this respect are:

a) Article 5 (Principles relating to processing of personal data);
b) Article 6 (Lawfulness of processing);
c) Article 7 (Conditions for consent);
d) Article 9 (Processing of special categories of personal data);
e) Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject);
f) Article 13 (Information to be provided where personal data are collected from the data subject);
g) Article 14 (Information to be provided where personal data have not been collected from the data subject);
h) Article 15 (Right of access by the data subject);
i) Article 16 (Right to rectification);
j) Article 17 (Right to erasure);
k) Article 18 (Right to restriction of processing);
l) Article 19 (Notification obligation regarding rectification or erasure of personal data or restriction of processing);
m) Article 20 (Right to data portability);
n) Article 21 (Right to object);
o) Article 22 (Automated individual decision making, including profiling);
p) Articles 44 - 49 (Transfers of personal data to third countries or international organisations);
q) Infringements of obligations under Member State law adopted under Chapter IX (Provisions relating to specific processing situations);
r) Non-compliance with access in violation of Articles 58 paragraph (1) and of orders under Article 58 paragraph (2) (powers of the supervisory authorities).

We underline that the administrative sanction regime will require a case by case assessment of the circumstances of each individual infringement, therefore it does not impose liability on a strict liability basis. We consider that the factors that should be taken into account should be the nature, gravity and duration of each infringement, the form of guilt (intention or negligence), the damage mitigation steps already implemented, any technical and organisational measures already implemented, and the manner in which the supervisory authority became aware of the issue.

A Member State is entitled to lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

But what happens in the legal systems which do not provide for administrative fines (*i.e.* Denmark, Estonia)? The GDPR expressly regulates that in such Member States, the fine shall "*be initiated by the competent supervisory authority and imposed by*

[28] Please see Article 83 paragraph (3) of the GDPR.
[29] Please see Article 83 paragraph (4) of the GDPR.
[30] Please see Article 83 paragraphs (5) and (6) of the GDPR.

competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive"[31].

Member States may lay down the rules on other effective, proportionate and dissuasive penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines and shall take all measures to ensure that they are implemented in the national legal system – as a third level of 'penalties'. Taking into consideration certain recitals of the GDPR, these effective, proportionate and dissuasive penalties to be established by the Member States can be interpreted as criminal sanctions for certain violations. We consider that the possible introduction of criminal sanctions for unlawful processing of personal data presents a significant risk for undertakings, depending on how the Member States interpret and apply this power.

For transparency, the Member States are obliged to notify to the European Commission the legal provisions which they adopt by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

3. Concluding Remarks

The aim of this study is to raise awareness and improve knowledge of data protection rules established by the GDPR. It is recommended for legal professionals and non-specialist legal professionals, and other persons working in the field of data protection.

The data protection right developed out of the right to respect for private life, being related to human beings. Natural persons are, therefore, the primary beneficiaries of data protection - personal data covers information pertaining to private life or to professional or public life of a person. Data also relate to persons if the content of the information indirectly reveals data about a person.

With the application of the GDPR from May 2018, its rules will become legally binding, together with the right to protection of personal data which becomes a separate fundamental right. Having in view the new technologies and the digital revolution, GDPR will satisfy the growing need for the robust protection of personal data.

The new data protection rules shall be applied in Member States by the national courts and by the national data protection authorities (the latter being part of the public administration system[32]), which shall be liable for obeying the GDPR[33].

The new maximum fines of the greater of 20,000,000 EUR or four percent of an undertaking's worldwide turnover are devilish and will manage to scare every general manager perception in order to comply with the GDPR.

In any case, for all the actors involved in data protection, the final countdown is near!

References

- Augustin Fuerea, *Dreptul Uniunii Europene*, Universul Juridic Publishing House, Bucharest, 2016
- Marta-Claudia Cliza, *Drept administrativ. Partea a II-a*, Editura Pro Universitaria, Bucuresti, 2011
- Mihaela Augustina Dumitrascu, Roxana Mariana Popescu, Dreptul Uniunii Europene, *Sinteze si aplicatii. Editia a II-a, revazuta si adaugita*, Universul Juridic Publishing House, Bucharest, 2015
- Nicolae Popa, Elena Anghel, Cornelia Ene-Dinu, Laura-Cristiana Spataru-Negura, *Teoria generala a dreptului. Caiet de seminar*, third edition, C.H. Beck Publishing House, Bucharest, 2017
- Roxana-Mariana Popescu, ECJ Case-law on the Concept of "Public Administration" Used in Article 45 Paragraph (4) TFEU, CKS Ebook, "Nicolae Titulescu" University Publishing House, 2017
- Laura-Cristiana Spataru-Negura, *Dreptul Uniunii Europene – o noua tipologie juridica*, Hamangiu Publishing House, Bucharest, 2016
- Elena Emilia Stefan, *Drept administrativ. Partea a II-a*, Editura Universul Juridic, Bucuresti, 2013
- Elena Emilia Ștefan, Răspunderea juridică. Privire specială asupra răspunderii în dreptul administrativ, ProUniversitaria Publishing House, Bucharest, 2013
- European Union Agency for Fundamental Rights, *Handbook on European data protection law, Council of Europe*, 2014, available at https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
- Matheson, *GDPR in Context. Remedies and Sanctions*, available at http://www.matheson.com/images/uploads/documents/GDPR_in_Context_-_Remedies_and_Sanctions.pdf
- White & Case, *GDPR Handbook: Unlocking the EU General Data Protection Regulation. A practical handbook on the EU's new data protection law*, September 2017, available at https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation
- www.9to5mac.com
- www.agpd.es
- www.bbc.com

[31] Please see Article 83 paragraph (9) of the GDPR.

[32] For the European Union public administration concept, please also see Roxana-Mariana Popescu, *ECJ Case-law on the Concept of "Public Administration" Used in Article 45 Paragraph (4) TFEU*, CKS Ebook, "Nicolae Titulescu" University Publishing House, 2017, p. 529.

[33] It is widely acknowledged that nobody can be exempted from liability for the offenses committed in the exercise of public function. For more information, please see Elena Emilia Ștefan, *Răspunderea juridică. Privire specială asupra răspunderii în dreptul administrativ*, ProUniversitaria Publishing House, Bucharest, 2013, p. 317.

- www.dailymail.co.uk
- www.eur-lex.europa.eu
- www.hotnews.ro
- www.iapp.org
- www.linkedin.com
- www.paypal.com
- www.reuters.com
- www.senat.ro
- www.techterms.com
- www.un.org