THE USV ANNALS OF ECONOMICS AND PUBLIC ADMINISTRATION | VOLUME 20, ISSUE 1(31), 2020

TWO YEARS OF GDPR IN ROMANIA

Professor PhD **Doru TILIUȚE**
„Ștefan cel Mare" University of Suceava, Romania
dtiliute@seap.usv.ro

Abstract:
May 25, 2020 marks two years since the entry into force of the GDPR across the EU. The provisions of the directive were known since the date of publication, in 2016, and the time remaining until the date of the application has been designed for businesses to take the measures necessary to comply with these provisions. To this quite generous interval, a few months were added tacitly, until the end of 2018 when, practically, no fines were applied for non-compliance. However, starting with the first months of 2019, a multitude of fines have been imposed, in all EU countries, on larger or smaller companies for breaches of the GDPR. The aim of this article is to outline a perspective on how the lack of compliance with GDPR in Romania was monitored and sanctioned and to present some conclusions related to the situation of other EU countries.

Key words: GDPR, fines, Romania, EU, compliances

JEL classification: B55, D21, F69

1. INTRODUCTION

In this article we try to make a retrospective of how the GDPR was applied and is still applied in Romania, two years after the entry into force of General Data Protection Regulation 2016/679. It is also analyzed the way in which the National Supervisory Authority for the Processing of Personal Data (ANSPDCP) intervened and sanctioned the non-conformities in applying the GDPR provisions.

2. WHAT ACTUALLY GDPR IS?

Since the purpose of this article is to analyze the way in which ANSPDCP sanctioned the non-compliance of the economic operators with the regulations of the GDPR and the reasons why the fines were applied, we consider that it might be useful a brief presentation of the fundamentals of the elaboration of the Regulation, as well as the principles on which it is based

The GDPR replaces an older directive "Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with a view to the processing of personal data and on the free movement of such data". The development of the new directive took about four years (BURGESS, 2020).

Unlike a regulation, a directive allows each EU member State to adopt and customize its laws according to the needs of its citizens, while a regulation requires its adoption in its entirety, without exceptions or derogations by all EU Member States. In the case of the GDPR, all 27 member States[1] are required to comply.

Regulation GDPR has in its center a primordial element: the individual. Individual data must be protected by appropriate measures. Thus, the GDPR introduces an important principle, the responsibility. By personal data is generally understood that category of information that allows the direct or indirect identification of a living person, from the available data. Some data may be obvious, such as a person's name, geographical location or a clear username, while others might be somewhat less obvious: IP addresses or data stored by cookie variables may be considered personal data.

Within the GDPR there are also some special categories of personal data that are sensitive, requiring a special attention and protection. These personal data include information on racial or

[1] After Brexit in January 31, 2020

ethnical origin, political opinions, religious beliefs, union membership, genetic and biometric data, health information and data on a person's life or sexual orientation.
Although it comes from the EU, the GDPR can also apply to companies located outside the Union, which have activities in the territory of the EU states. An US firm, for example, doing business in the EU, must conform to GDPR regulations if it is a controller[2] of EU citizens.
GDPR introduces six principles that must be respected by any Data Processing Organization as described below:

- Legality, fairness and transparency - process the data legally and correctly towards the data subject and explain to them why you are processing them in a language they can understand, without legal jargon.
- Purpose limitation - do not use the data in any other way than that presented to the natural person;
- Data minimization - don't process more data than you need to;
- Accuracy - keeps the data updated;
- Integrity and privacy - protects data by taking appropriate measures;
- Responsibility - document the processes and be able to demonstrate respect for the above principles

On brief, the principle of legality requires that all operations on data must be legal, meaning that they are based on at least one of the following requirements (The European Parliament and the Council, 2016):

- Consent - the person has validly consented;
- Contract - there is a contract or a contract is to be concluded;
- Legal obligation - there is a legal obligation;
- Vital interest - protect the life or health of the person;
- The public interest;
- Your legitimate interest - as long as it does not conflict with the interest of the natural person

The principle of *Legitimate interest* requires additional caution. It is usually used for situations where there is no consent, it cannot be obtained or it is not desired and there is no other basis for data processing (CCTV surveillance, GPS location monitoring, recruitment, event organization, etc.). In order to be able to use the legitimate interest, it is necessary for the Organization (controller) to document in writing that its interest prevails over the rights and interests of the data subjects.

As the GDPR focuses on respecting the privacy of individuals, it gives them more rights and stronger control over how their data is used.
These rights are presented in table 1:

Table 1. The rights of individuals as derived from GDPR, with their meaning

1	**Right to be Informed**	**the person must be informed, inter alia of what data is being processed, why, for what purposes, to whom it is transmitted and what rights it has**
2	**Right of access by the data subject**	the person has the right to access their personal information processed
3	**Right to rectification**	the person has the right to obtain the rectification of the incomplete and inaccurate information concerning him
4	**Right to erasure**	In some situations, the person has the right to request the deletion of data that are no longer needed
5	**Right to restriction of processing**	Restriction of processing when there is a basis
6	**Right to data portability**	The right of the person to request the porting of the data from one operator to another

[2] The entity which determines the purposes and means of the processing of personal data

7	**Right to object**	The right of the person to oppose processing, when there is a basis
8	**Right to be not subject of an individual decision making taken as a result of automated data processing , including profiling**	The person has the right to human intervention in the case of important decisions concerning him

Source: ANSPDCP, 2020; GDPR Enforcement Tracker, 2020

In addition, the data subject has the right to lodge a complaint at the national supervisory authority and to sue the economic agent.

3. MONITORING THE COMPLIANCE WITH THE GDPR IN ROMANIA

In Romania, the national authority charged with observing the provisions of the GDPR and entitled to apply sanctions is „Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal" (ANPSPDCP), meaning National Supervisory Authority for Personal Data Processing. This authority has been operating since 2005, based on the law no. 102 of May 3/ 2005, by which the Authority was established and its responsibilities were set.

As a consequence of the entry into force of regulation (EU) 2016/679 from May 25, 2018, the organization and the attributions of the authority were modified by the law no. 129/2018, harmonizing them with the new European regulation.

Analyzing the activity of ANSPDCP from the reorganization date, following the entry into force of the regulation, and so far, we find that in 2018 no fines were applied but several organizational actions were carried out: a series of documents and procedures for internal use and for the settlement of complaints were elaborated and approved. Since 2019 many fines have been imposed for violating the principles set out by the GDPR. Among the provisions that were most frequently violated are the right to information, obtaining the explicit acceptance of the person, lack of protection of data collected and processed, which created the possibility of their public disclosure, the use of personal data for other purposes than those for which the subjects were informed. Table 1 presents a selection of cases that lead to penalties applied to economic agents for the infringement of the above principle (ANSPDCP, 2020), (GDPR Enforcement Tracker, 2020). Selection was made from the highest fines that were applied to firms in different fields: hotels, telecommunications providers, banking institutions, transportations and so on. Based on the size of the fined companies and their financial power, the fines are quite modest, the largest being about 150,000 euros and has been applied to a banking institution with global coverage. However, this is the second highest fine in Central and Eastern Europe countries, after that of 200,000 euros applied in Poland (Albu, 2019)[3].

[3] The article refers to another fine of 130.000 Euros, also applied to a financial institution, but afterwards it was overpassed by that of 150.000 we mention.

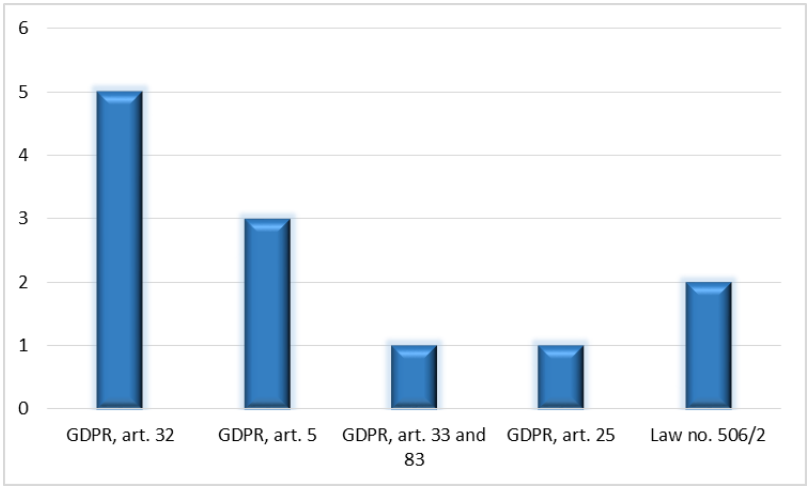

Figure 1. The number of fines applied, grouped by lows and articles from laws
Source: ANSPDCP cited by GDPR Enforcement Tracker

We may notice that the National Authority also applied fines based on other laws in force, which have as their object the processing of personal data, such as the law 506/2004, see items 4 and 7 in Table 2.

Figure 1 represents the number of fines selected in Table 2, grouped by laws and articles from law.

It is easily to notice that the number of fines applied under the GDPR is significantly higher than that imposed under other laws and that the number of those applied under Article 32 is the highest, equal to the sum of the number of fines applied under other articles.

Table 2. A selection of the highest fines applied in Romania since the entry into force of GDPR

No.	Date of application	The entity sanctioned	The reasons	the amount of the fine	legal basis
1.	06/27/2019	UNICREDIT BANK S.A	The bank violated the provisions of art. 25 paragraph (1) of Regulation (EU) 2016/679. The data regarding the CNP and the address of the persons who made payments to UNICREDIT BANK S.A., through online transactions, were disclosed to the beneficiary of the transaction, through the form of the account statement / details. According to art. 5 paragraph 1 letter c) from the GDPR ("Principles related to the processing of personal data"), the operator had the obligation to process data limited to what is necessary in relation to the purposes for which the data are processed.	613,912.00 lei	GDPR art. 25 item (1)
2.	07/02/2019	WORLD TRADE CENTER BUCHAREST S.A	The breach of security of personal data consisted in the fact that a list printed on paper, used to verify the clients who served breakfast and which contained personal data of a number of 46 customers hosted by the hotel unit belonging to WORLD TRADE CENTER BUCHAREST SA, was photographed by unauthorized persons from outside the company, which led to the disclosure in the online environment, by publication, of the personal data of some clients. WORLD TRADE CENTER BUCHAREST S.A. was sanctioned because it did not take measures to ensure that its employees who have access to personal data only process them at his request, according to the law. Also, the operator has not implemented adequate technical and organizational measures to ensure a level of security appropriate to the processing risk, generated in particular, accidentally or illegally, by unauthorized disclosure or unauthorized access to personal data. This allowed unauthorized access to the personal data of a number of 46 clients and the unauthorized disclosure of these data, in the online environment, which led to the damage to the rights to privacy and to the protection of personal data, guaranteed by art. 7 and art. 8 of the Charter of Fundamental Rights of the European Union and art. 16 of the Treaty on the Functioning of the European Union.	71,028.00 lei	GDPR art. 32 item (4) referred to art. 32 item (1) and item (2)
3.	07/05/2019	LEGAL COMPANY & TAX HUB SRL	The sanction was applied for the inadequate implementation of the technical and organizational actions, in order to ensure a level of security corresponding to the processing risk. This led to the unauthorized disclosure and unauthorized access to the personal data of the persons who carried out transactions received from the avocatoo.ro site (name, first name, correspondence address, email, telephone, workplace, details of transactions performed), publicly accessible documents, between December 10, 2018 - February 1, 2019. Those data were accessible through two links on the website.	14,173.50 lei	GDPR art. 32 item (1) and item (2)
4.	08/09/2019	Artmark Holding SRL	The sanction was applied to the operator because it couldn't prove that it obtained the express and unequivocal prior consent for the transmission of commercial messages by e-mail, in violation of the provisions regarding the unsolicited communications provided by art. 13 paragraph (1) letter. q) of Law no. 506/2004 regarding the processing of personal data and the protection of privacy in the electronic communications sector.	10,000.00 lei	Law no. 506/2004 art. 12 item (1)
5.	10/01/2019	Raiffeisen Bank S.A. and Vreau Credit	Two employees of Raiffeisen Bank S.A., using the data from the identity documents of some individuals, transmitted by some employees of "Vreau Credit S.R.L" (I want Credit	150,000 Euro Raiffeisen Bank	GDPR art. 32 item (4) in

No.	Date of application	The entity sanctioned	The reasons	the amount of the fine	legal basis
		S.R.L	S.R.L) through the mobile application WhatsApp, they performed queries of the credit bureau system in order to obtain the necessary data in determining the credit eligibility of the respective individuals, through prescoring simulations. In this regard, 1194 simulations were performed, involving 1177 individuals. Also, for 124 individuals, the database of the National Agency for Financial Administration (ANAF) was also consulted. The above mentioned prescoring simulations were performed using the computer application used by Raiffeisen Bank S.A. in the lending activity, and the negative lending decision was communicated by the employees of Raiffeisen Bank S.A. to employees of "Vreau Credit S.R.L", in violation of internal procedures.	20,000 Euro Vreau Credit SRL	conjunction with art. 32 item (1) and item (2) and art. 33 item (1)
6.	09/26/2019	INTELIGO MEDIA SA	ANSPDCP was notified that the Web page for creating a new account on the website avocatnet.ro - belonging to the operator Inteligo Media SA, displays an unchecked box, with a text next to the following content: «I do not want to receive" Personal Update ", the information sent daily, free of charge, by email, by avocatnet.ro ». According to these conditions established by the operator, to the extent that a user omits the checkbox of this box, he is automatically subscribed, respectively his e-mail is recorded automatically in the subscribers' database to this information. Thus, the subscription took place in the lack of a manifestation of will on the part of the users, which clearly indicates the acceptance of the processing for the purpose established by the operator. During the control, the operator could not prove that it obtained the explicit consent, under the conditions provided by art. 7 of the GDPR, for a number of 4357 users whose personal data have been processed.	9,000 Euro	GDPR art. 5 item (1) lit. a) and b), art. 6 item (1) letter a) and art. 7
7.	10/15/2019	Vodafone Romania S.A	The sanction was applied because the operator did not consider the option of a petitioner to no longer receive messages with promotions, contests and any other messages other than those regarding the costs and security of the calls, an option the operator was notified with. Subsequent to his request he was confirmed he had been unsubscribed from the commercial communications sent by the operator, but he received on his e-mail address another unsolicited message from Vodafone Romania S.A., thus violating the provisions of art. 12 paragraph (1) of Law no. 506/2004 regarding unsolicited communications.	10,000 lei	Law no. 506/2004 art. 13 item (1) letter q) in conjunction with cu art. 13 item (5)
8.	11/07/2019	SC CNTAR TAROM SA	The sanction was imposed on the operator due to the fact that it did not implement appropriate technical and organizational measures to ensure that any person acting under his authority and who has access to personal data, not process them except at his request. Related to this aspect, the operator has not taken any adequate measures to ensure a security level corresponding to the risk generated by the unauthorized disclosure or the unauthorized access to personal data transmitted, stored or otherwise processed. This situation led to the unauthorized access of an employee to the booking application and the photographing of a list containing the personal data of 22 TAROM passengers / clients and to the unauthorized disclosure in the online environment of this list.	95,194 lei	GDPR art. 32 item (4) in conjunction with cu art. 32 item (1) and item (2)

No.	Date of application	The entity sanctioned	The reasons	the amount of the fine	legal basis
9.	12/10/2019	Hora Credit IFN S.A.	The sanctions were applied as a result of a complaint alleging that Hora Credit IFN SA transmitted documents containing another person's personal data to the e-mail address. When this error was notified to both the operator and its call center, Hora Credit IFN SA did not remedy this issue, further transmitting messages to the e-mail address. Following the investigation it was found that Hora Credit IFN SA processed the data without proving the application of effective mechanisms for verifying and validating the accuracy of the data collected and processed, respectively, to maintain their confidentiality, according to the principles provided in art. 5 of the GDPR. Also, it was found that the operator did not take sufficient security measures for personal data, according to art. 25 and 32 of the GDPR, to avoid unauthorized and accessible disclosure of personal data to third parties. At the same time, Hora Credit IFN SA did not notify the Supervisory Authority of the security incident that was brought to its notice, according to art. 33 of the GDPR, within 72 hours from the date on which it became aware.	total 14,000 euro	GDPR, art. 33 and 83
10.	12/16/2019	SC Enel Energie S.A.	The operator was sanctioned with two fines, each amounting to 14,334.30 lei, the equivalent of the amount of 3000 EURO for the violation of art. 5 paragraph (1) letter d), art. 6 paragraph (1) letter a) and art. 7 paragraph (1) of the General Regulation on Data Protection, respectively for the violation of the provisions of art. 21 paragraph (1) of the General Regulation on Data Protection. The sanctions were applied following a complaint alleging that S.C Enel Energie S.A. illegally processed the data of the petitioner, not being able to prove his consent for sending notifications to this e-mail address and without respecting the principle of accuracy. In addition, the operator did not take the necessary measures to disable the transmission of notifications, giving the complainant exercised the right of opposition on several occasions.	To fines of 14,334.30 lei each	GDPR, art. 5 item (1) letter d), art. 6 item (1) letter a) and art. 7 item (1)
11.	02/11/2020	Vodafone Romania SA	The sanction was applied because the operator mistakenly processed the personal data of an individual in order of resolving his complaint, which resulted in the operator's response being sent to an incorrect e-mail address afterwards, with insufficient security measures being taken against the illegal processing of the personal data of the respective person. The processing principles provided by art. 5 paragraph (1) letter d) and f) in conjunction with cu. 5 paragraph (2) of the General Regulation on Data Protection have been violated.	3000 euro	art. 5 item (1) letter d) and f) in conjunction with cu art. 5 item (2)
12.	02/13/2020	ONG SOS-Infertilitate	The operator disclosed personal data without the consent of the data subject. The Supervisory Authority asked the Association for more information regarding the aspects notified, but the operator did not respond to the requests of our institution. Following the telephone contact of the operator, the president of the association expressed his option to be sent the request of the Supervisory Authority by e-mail to an address indicated by him.	2000 euro	GDPR, art. 32

4. A LOOK OVER THE FENCE

We cannot have a real or complete picture of Romania's position on the issue of compliance with the GDPR if we do not look at other countries in Europe. For this purpose we have chosen some of the highest fines applied in five different countries in Europe, based on the GDPR articles that brought the highest fines in Romania (GDPR Enforcement Tracker, 2020). The first thing we can notice is a very large discrepancy of fines, in a ratio of at least 1/20 for the same violation of the regulation. For instance, a huge telecommunications company, namely Vodafone Romania SA, was penalized with 3000 euros in Romania, while a much smaller telecommunications company, namely OTE, was fined 200,000 euros in Greece (Helenic Data protection Authority, 2020), both for violating Article 5 of the GDPR. Another telecom provider vas fined 9,500,000 euros in Germany.

Even more surprising is that the Bulgarian Data Protection Supervisor has fined another institution of the Bulgarian state, namely the National Revenue Agency, with a very important amount of money, of 2,600,600 euro (item 2 in Table 3).

Table 3. Top five fines in different countries in EU, applied for violation of art. 5 and 32 in GDPR, articles which determined the highest fines in examples in Table 1

No.	Date of application	The entity sanctioned	The reasons	the amount of the fine	legal basis	
1.	09.12.2019	Telecoms provider (1&1 Telecom GmbH)	Insufficient technical and organizational measures to ensure information security. The Controller is a company offering telecommunication services. A caller could obtain extensive information on personal customer data from the company's customer service department simply by entering a customer's name and date of birth. In this authentication procedure, the BfDI finds a violation of Article 32 GDPR, according to which a company is obliged to take appropriate technical and organizational measures to systematically protect the processing of personal data. Due to the company's cooperation with the data protection authority, the fine imposed was at the lower end of the scale.	9,550,000 euro	GDPR, Art. 32	Germany
2.	28.08.2019	National Revenue Agency	Insufficient technical and organizational measures to ensure information security Leakage of personal data in a hacking attack due to inadequate technical and organizational measures to ensure the protection of information security. It was found that personal data concerning about 6 million persons was illegally accessible.	2,600,600 euro	GDPR, Art. 32	Bulgaria
3.	21.11.2019	Futura Internationale	Insufficient fulfilment of data subjects rights. Futura Internationale was fined for cold calls after several complainants obtained cold calls, despite having declared directly to the caller and by post that this was not wanted. In particular, the decision pointed out that the CNIL's on-site investigation of Futura Internationale revealed, inter alia, that Futura Internationale had received several letters objecting to cold calling, that it had stored excessive information about customers and their health and that Futura Internationale	500,000 euro	GDPR, Art. 5, Art. 6, Art. 13 Art. 14, Art. 21	France

			had not informed individuals about the processing of their personal data or the recording of telephone conversations.			
4.	03.06.2019	IDdesign A / S	The fine was imposed as a result of an inspection carried out in autumn of 2018. IDdesign had processed personal data of approximately 385,000 customers for a longer period than necessary for the purposes for which they were processed. Additionally, the company had not established and documented deadlines for deletion of personal data in their new CRM system. The deadlines set for the old system were not deleted after the deadline for the information had been reached. Also, the controller had not adequately documented its personal data deletion procedures. Please note: Since Danish law does not provide for administrative fines as in the GDPR (unless it is an uncomplicated case and the accused person consented), fines will be imposed by courts.	200,850 euro	GDPR, Art. 5 item (1) e), Art. 5 item (2)	Denmark
5.	07.10.2019	Telecommunication Service Provider	Non-compliance with general data processing principles. A large number of customers were subject to telemarketing calls, although they had declared an opt-out for this. This was ignored due to technical errors.	200,000 euro	GDPR, Art. 5 item (1) c) Art. 25	Greece

On the other hand, Romania has a leading position in second place by number of EU fines, after Spain and closely followed by Germany, Figure 2 (Robinson, 2019).

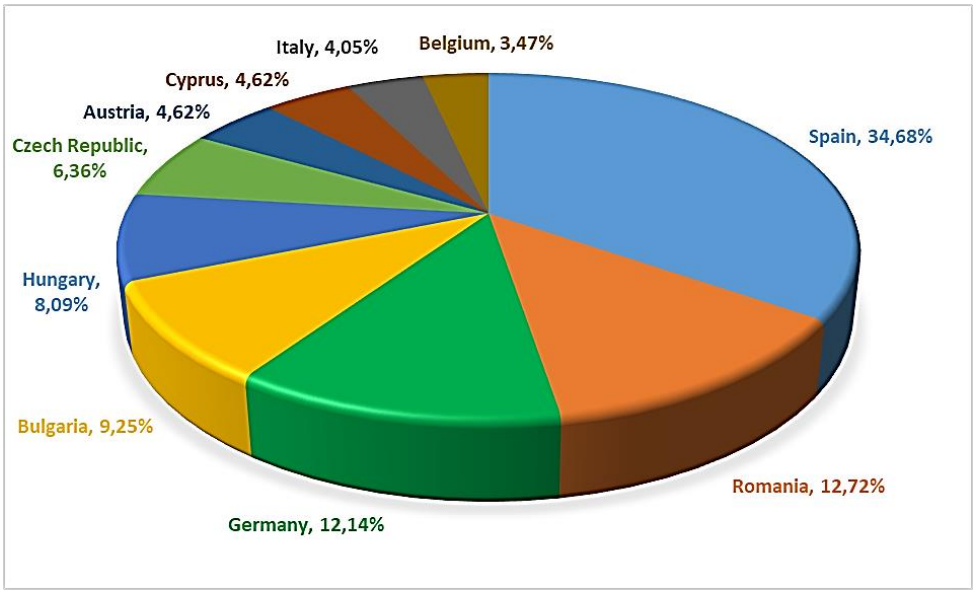

Figure 2. Top ten countries by number of fines
Source: KDnuggets dot com

Meanwhile, in terms of the amount of money collected from fines, Romania does not even fall in the top ten European countries, Figure 3 (Robinson, 2019).
These last two statistical situations confirm the appreciation, somewhat subjective, that we made at the beginning of this section, namely that the value of the fines applied in Romania is small in relation to the size of the sanctioned companies.

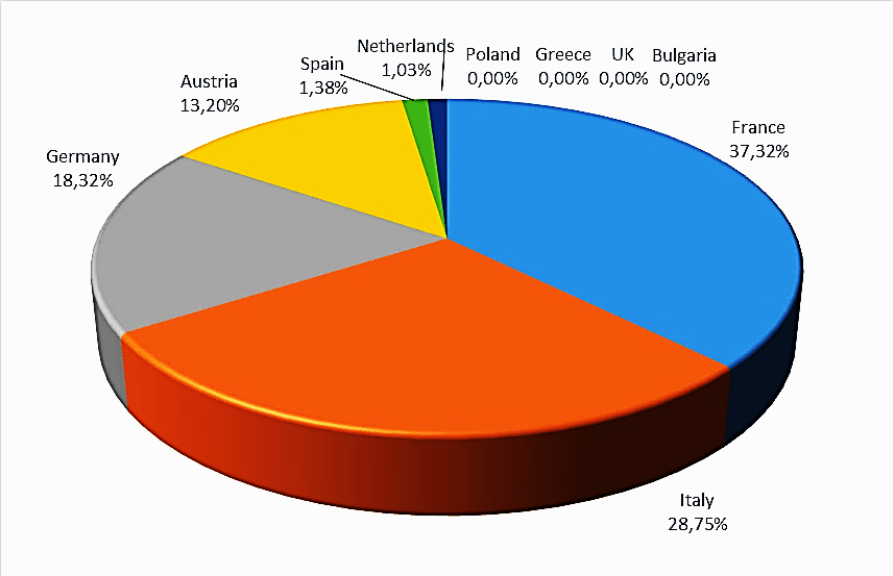

Figure 3. Top ten countries by amount of fines
Source: KDnuggets dot com

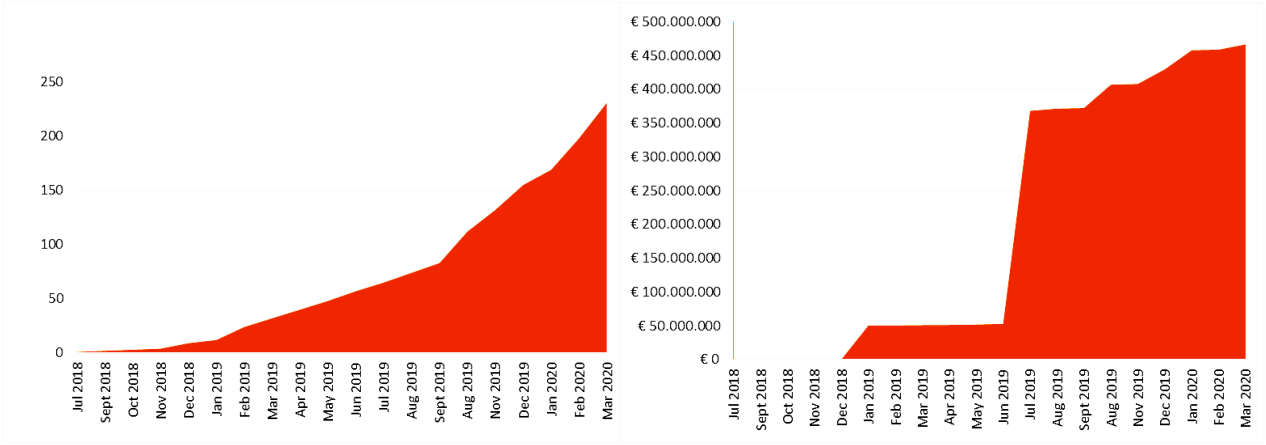

Figure 4. The evolution of the overall number of fines and the overall sum of fines in EU Data
Source: GDPR Enforcement Tracker, 2020

Some countries in EU didn't hesitate to fine, through their national authorities, huge companies with impressive amount of money. Thus, France fined Google Inc. with 50 million euros (Satariano, 2019), UK cached in from Facebook £500,000 (~$643K) fine in Cambridge Analytica scandal (Lomas, 2019), British Airways faced record £183millions fine for data breach, also in UK (BBC News, 2019). In other countries, the National Authorities sanctioned state institutions as in Bulgaria (item 2 in Table 3), or Norway, where the first three highest fines were applied to Bergen Municipality (170,000 euro), Oslo Municipal Education Department (120,000 euro) and Rælingen Municipality (73,000 euro) (GDPR Enforcement Tracker, 2020).

5. CONCLUSIONS

Judging by the number of fines applied in Romania since the entry into force of GDPR, we may be tempted to consider that ANSPDCP is doing its job. Considering the example of other countries in EU, which applies less fines but more consistent, that applies the same measure to private companies and for public institutions as well, we would be entitled to appreciate that there is enough room to improve the activity and make it more efficient.
May be it is time to take a look at the Ministry of Education, where the results of the national competitions are publicly accessible on the ministry's website, with all the identification data of the competitors; to the way in which the collection of personal data is organized upon admission to

schools and universities, to how candidates are informed about their rights, the purpose and duration of the data processing.

REFERENCES

1. Albu, L. (2019, 07 15). *Mediafax.* Retrieved from mediafax.ro: https://www.mediafax.ro/economic/romania-a-doua-cea-mai-mare-amenda-din-europa-centrala-si-de-est-pentru-incalcarea-gdpr-18235720
2. ANSPDCP. (2020, 04 12). *Stiri.* Retrieved from dataprotection.ro: https://www.dataprotection.ro/?page=allnews
3. BBC News. (2019, July 8). *British Airways faces record £183m fine for data breach.* Retrieved from BBC News: https://www.bbc.com/news/business-48905907
4. *GDPR Enforcement Tracker.* (2020, April 1). Retrieved from Enforcementtracker: https://www.enforcementtracker.com/
5. GDPR Enforcement Tracker. (2020, 03 21). *GDPR Enforcement Tracker.* Retrieved from Enforcementtracker: https://www.enforcementtracker.com/
6. *Helenic Data protection Authority.* (2020, March 21). Retrieved from Αρχή: http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=3,241,32,146,79,143,149,112
7. Lomas, N. (2019, October 2019). *Facebook agrees to pay UK data watchdog's Cambridge Analytica fine but settles without admitting liability.* Retrieved from TechCrunch: https://techcrunch.com/2019/10/30/facebook-agrees-to-pay-uk-data-watchdogs-cambridge-analytica-fine-but-settles-without-admitting-liability/
8. Robinson, J. (2019). *Analyzing GDPR Fines – who are largest violators?* Retrieved from KDnuggets: https://www.kdnuggets.com/2020/03/analyzing-gdpr-fines.html
9. Satariano, A. (2019, January 21). *Google Is Fined $57 Million Under Europe's Data Privacy Law.* Retrieved from The New York Times: https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html
10. The European Parliament and the Council. (2016, 4 5). *Regulation (EU) 2016/679 - EUR-Lex - European Union.* Retrieved from EUR-Lex - European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN