The 14th International Scientific Conference
eLearning and software for Education
Bucharest, April 19-20, 2018
10.12753/2066-026X-18-218

New Data Protection Regulations and Their Impact on Universities

Mihai-Ştefan DINU
"Carol I" National Defence University, Panduri str. No. 68-72, 5th distr., Bucharest, Romania
mihaistdinu@yahoo.co.uk

Abstract: *Contemporary technological progress was possible on the background of rapid internet access, geographical spreading which has facilitating not only the rapid transmission of vast amount of data but also not so honest storage, use and transmission of this big amount of data. Internet access needs credentials, and frequently credentials are linked to personal data that nowadays can be considered priceless. That is why the protection of personal data must be a priority for the universities. Why new data protection regulation? Why students and employee data are so important? Why and how to protect all these big amounts of data? How to implement new data protection regulations in universities? From all these questions, we start to analyze the actual and future legal environment regarding data protection in order to identify the best practical cyber security solutions. The analysis will start from the replacement of Data Protection Directive 95/46/EC and national regulation with the EU General Data Protection Regulation (GDPR). Intention is to identify the way universities will approach data privacy in order to collect, store and transmit data on students or teachers and in what measure the selected approach will affect educational and research processes. Role of human factor have also been considering in the framework of new regulations, with the focus on necessary relations grid around Data Protection Officer. The analysis will go further with the considerations regarding the place of cyber insurance process in the institutional grid, which is involved in the data protection process, on the one hand, and the necessary resources for implementing the new regulations.*

Keywords: *data protection, GDPR, university, research data, cybersecurity, privacy, databases*.

I. INTRODUCTION

We live today in a very interconnected word. Almost every human activity is influenced by the appliances of a rapid development technology. We get informed with the everyday facts of live, we learn and educate, get medical assistance, pay our bills and taxes using the latest technological updates. The internet facilitates all these activities, as the largest multi-areas infrastructure humanity ever knows. It is the infrastructure that holds, transport and many time store an unprecedented amount of data in the history of humanity, leading to the transformation of our society[1]. Predicted forty years ago by Yoneji Masuda who named it *the information society*, is a society in which the major production center is the information utility, developed information networks, data bases and data banks[2]. Data got value and this value gets priceless. According to Masuda, besides its positive issues, the information society develops challenges and threats, a series of social problems: *future shock, terrorism and invasion of privacy*[3], main forces of social change being *citizens' movements and litigations*[4].

Current statistical data confirm Masuda's predictive vision, thus at the end of the 2017 there were approximately 4.15 million internet users (this number being increased in the last two years with approximately 1 million) from an estimated 7.63 billion world populations[5], the percentage of spreading by regions being as depicted in the figure no. 1.

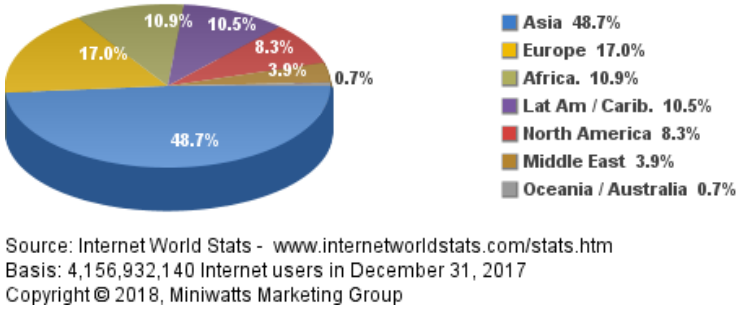

Figure 1. Internet users by world regions, December 2017

With all those previous noted challenges and threats, in spite of the large development of cyber security industry, it became clear that all the data kept, transported and stored within the cyber space, must be furthermore protected.

II. GDPR CONTEXT

2.1 Data breach phenomenon

The way data is used within the framework of cyberspace lead, as we mentioned, to evolved cyber security infrastructure, as well as regulations in order to face newly challenges and threats[6] to data, especially to personal data, that kind of data being intimately related to the protection of individual rights and liberties or/and privacy. *Breach Level Index Report*[7] regarding the first half of year 2017 revealed some interesting issues on the data breach occurrence at international level. The methodology[8] used for the report categorized data after number of records, type of data (nuisance, account access, financial access, identity theft, and critical existential data) , source of the breach (lost devices, stolen devices, malicious insider/outsider, state espionage), the nefarious usage of data (ransomware, publication of embarrassing or harmful information[9] , use of financial data in order to get funds or to apply for loans etc) and the industries where braches occurred. According to the report, the incidence of data breach after source and type are depicted in the *Figure no. 2.*

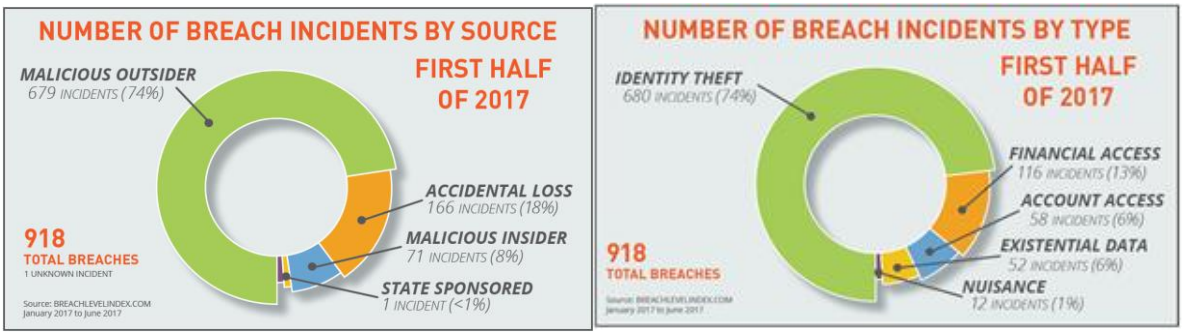

Figure 2. Breach Incidents by Source and by Type, first half of the year 2017

It is easy to observe that by the source the majority of breaches were malicious outsider (74%), and by type the majority of data was identity theft (74%), that type of breach being in direct relation with the identity, therefore with personal data type.

2.2 Legal development of Right to be forgotten

The Right to be Forgotten is founded on the right to privacy and it came into effect in May 2014, when the European Court of Justice ruled that individuals can request that URLs containing "inaccurate, inadequate, irrelevant or excessive" information that appear in queries with name of the requester[10] to be removed.

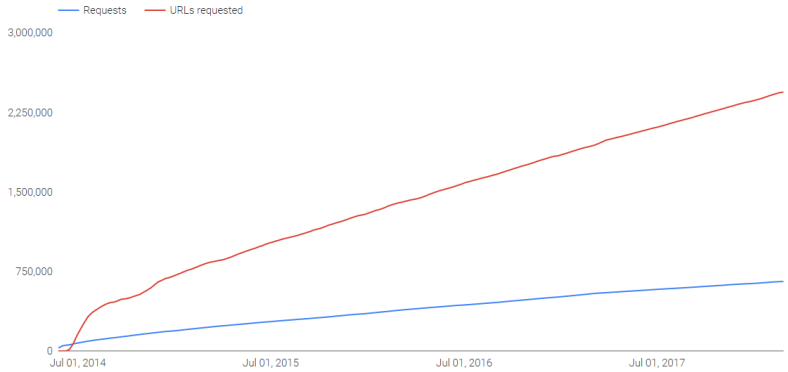

Figure no 3. Number of requests and number o URLs to be removed since july 2014[11]

In almost four years from the coming into effect of that ruling, there were two major trends in removal requests: 33% from 2.4 million of the URLs (*Figure no. 3*) were on social media or directory services that contained personal data, and other major 20% were URLs that contains news or were part of government websites[12]. Most of them requested removal of legal history. The data containing request of removal in the approximately last two years are depicted in the *Figure no.45.*

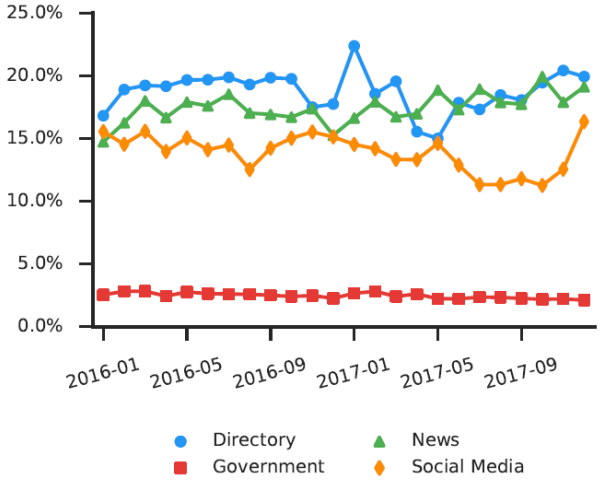

Figure 4. Categories of URLs requested for removal[13]

To be precise in our presentation we must add the type of data contained in the URLs requested for removal which are as follows: personal data, sensitive personal data, professional data, crime history, political affiliation etc (Table no. 1).

Label	Description
Personal information	The requester's personal address, residence, and contact information or images and videos.
Sensitive personal information	The requester's medical status, sexual orientation, creed, ethnicity, or political affiliation.
Professional information	A requester's work address, contact information, or neutral stories about their business activities.
Professional wrongdoing	References to the requester's convictions of a crime, acquittals, or exonerations in a professional role.
Crime	References to the requester's convictions of a crime, acquittals, or exonerations.
Political	Criticism of a requester's political or government activities, or information about their platform.
Self authored	Requester authored the content.
Name not found	No reference to the requester's name found in the content of the URL, though their name may appear in the URL parameters.

Table 1. Categories of data requested for removal[14]

From the previously cited report came out the idea that issues related to privacy in the case of the right to be forgotten bring upfront a controversial legal issue: conflicting interests in the personal

privacy data versus public interest data[15]. as the same report reveals that from 85% request of private individuals, a number of 33,937 URLs request of removal came from politicians and government officials and other 44,213 from non-governmental public figures[16]. These conflicting issues are proposed to be solved, according to the recital (4) from GDPR where is stated that *the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*[17]. Therefore, the principle of proportionality must be taken in the account when it comes about balancing privacy and public interest in afore mentioned cases.

2.3 New regulations on personal data: *EU General Data Protection Regulation (GDPR)*

In this context, on 25 of May 2018, the new regulation on personal data will come into force, based on the ***EU General Data Protection Regulation (GDPR)***, approved by the EU Parliament on 14 April 2016.

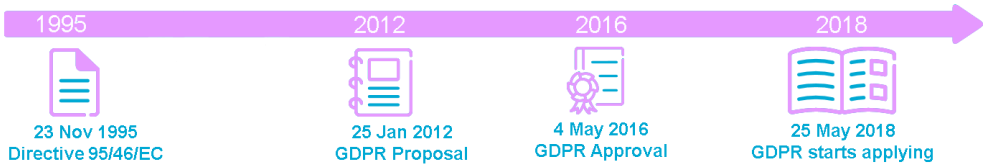

Figure 5. Timeline for GDPR legislative process

Intended to replace the Data Protection Directive 95/46/EC and the Romanian national regulation Law no. 677 of 2001 – *for the protection of individuals with regard to the processing of personal data and the free movement of such data –*, GDPR emergence was possible in order to harmonize data privacy laws in Europe. Its primary objective is to protect and empower all EU citizens in data privacy issues and to transform the manner in which organizations approach data privacy. It does not apply only to EU organizations but all organizations that are processing personal data of the subjects residing in European Union. Along with this increased territorial scope, meaning an extra-territorial applicability, the new regulations bring:

- new sanctions in the form of huge penalties that can be up to 4%of annual global turnover or 20 million euros,
- new conditions for consent, that must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. The consent must be as easy to withdraw, as it is to give it.
- Modifications on data subject rights as breach notification, right to access, right to data erasure (previously known as the right to be forgotten), data portability, privacy by design and data protection officers.

The ***EU General Data Protection Regulation***[18] is structured on 11 chapters that grouped 99 articles, as follows:

1. General provisions (Art. 1 – 4)
2. Principles (Art. 5 – 11)
3. Rights of the data subject (Art. 12 – 23)
4. Controller and Processor (Art. 24 – 43)
5. Transfer of personal data to third countries or international organizations (Art. 44 – 50)
6. Independent supervisory authorities (Art. 51 – 59)
7. Cooperation and consistency (Art. 60 – 76)
8. Remedies, liability and penalties (Art. 77 – 84)
9. Provisions relating to specific processing situations (Art. 85 – 91)
10. Delegated acts and implementing acts (Art. 92 – 93)
11. Final provisions (Art. 94 – 99)

Due to its large applicability, not only territorial but as domains of activity, GDPR will impact every activity that process or collect personal data. Article 4 of the GDPR that stated the role of controllers of data and processors of data, lead us to the conclusion that higher education organizations fall under the rule, and must comply with the new regulation regarding data protection. In order to accomplish legal request, the universities must follow few not easy steps. These are as follows: to

know the data contained in its activities, to assign a data protection officer, to ensure that can give subjects control and rights over their data in order to access information, correct inaccurate information, to opt out of direct marketing campaigns, to prevent data sorting and automated profiling, and to ensure data portability.

III. UNIVERSITIES ACTIVITIES AND ISSUES FALLING UNDER THE GDPR COMPLIANCE

3.1. GDPR's impact on Universities' activities

As mentioned in the beginning of our paper, value of data can be priceless, especially in the case of personal data; a breach in the records containing such type of data could lead to identity theft and a series of crimes that emerge from the use of stolen data. According to the Data Breach Index Report, when it comes to the industries where data breach incidents are occurring, education comes in fourth place, as shown in *table no. 2.*

INDUSTRY	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017
Healthcare	176	170	240	209	237	214	303	229	228
Financial Services	79	86	87	126	155	123	145	97	125
Education	8	28	86	88	102	64	110	58	118
Retail	56	41	82	115	131	109	122	125	112
Government	131	65	113	180	161	137	157	125	89
Technology	55	57	73	67	60	63	119	82	76
Other Industries	152	111	138	137	177	140	130	47	53
Industrial	-	-	-	-	0	0	17	11	35
Entertainment	-	-	-	-	3	2	18	10	32
Hospitality	1	0	0	1	1	0	15	15	19
Non-Profit	-	-	-	-	0	0	10	10	15
Insurance	-	-	-	-	1	1	8	6	10
Social Media	-	-	-	1	1	0	1	0	6
TOTALS	658	558	819	924	1,209	853	1,155	815	918

Source: BREACHLEVELINDEX.COM

Table 2. Data Breach Incidents by Industry in the last five years[19]

Although are placed on the fourth place, the 118 breaches that took place in the first half of 2017 year in the education domain, affected a total of 32 million records, the difference compared with previous monitored period being of 103% and an impressive 4,957%, increased from previously monitored 614,000 records.

In order to fully protect the data contained in their activities, and ensure data subjects rights, universities must assess and review their personal data ecosystem and know with who and which way interact.

In article 4 of GDPR personal data is defined as *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.*

Therefore, the universities personal data ecosystems are composing of the completely identifiable elements of subject data:

- Name and Identification number;
- Any location identifier like postal address or Any online identifier like IP address;
- Sensitive data like religious or political affiliation, sexual orientation etc.

The university personal data ecosystem is of utmost importance due to the outside interactions of such higher education organization. In this regard the universities' personal data ecosystem interacts with various organizations like:

- Health and social insurance;
- Consortium (other universities);

- Local authorities;
- Education or Research Department/Defence Department or other structures from the national security framework;

Besides personal data belonging to students, universities must have in focus another two types of data: *data belonging to parents or legal tutors* and *data belonging to employees* (current employees, new applicants or former employees)

Starting with this empirical mapping of personal data ecosystem, the data protection officer designed by the university board, must develop his assessment and future review towards the possible elements of the ecosystem, like:

- Core management information system and it infrastructure and;
- Curriculum tools and virtual learning environments [20];
- Payment systems, catering management and students or teachers transport;
- Office documents and communication tools;
- Biometric data;
- Mobility programs;

IV. UNIVERSITY RESEARCH IN THE NEW FRAMEWORK OF DATA PROTECTION REGULATION

Another issue of the utmost importance regarding higher education compliance to GDPR is the scientific research developed in the university framework. GDPR does not exactly defines scientific research with the exception of Recital 159 which states that *scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research*. Although, in article 89 GDPR proposes *Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*.

Summarizing, the art. 89 indicate the way to responsibly use personal data before, during and after research. In order to comply with art. 89 recommendations, researchers must follow several steps:

- *privacy by design and privacy by default*, meaning that research design must comply to the principles relating to personal data (article 5): lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability;
- *data protection impact assessment(DPIA),* meaning that researcher must collaborate in realization of DPIA with research support staff, legal and IT staff, in order to identify privacy and security risks associated with ongoing or proposed research projects and to formulate suitable contra measures. In other words, DPIA means consideration of all organizational aspects: legal, technical and infrastructure in order to support a well-documented data management plan;
- *inform*, meaning that participants at research and research partners are fully informed by the purpose of the research, by the risk for the participants and by the implemented contra measures
- *control*, meaning that researcher must be in control and accountable, able to prove his research compliance to the principles regarding the processing of personal data;
- *safety*, meaning that research must be realized with de-identified data (*figure no. 6*), using an encrypt storage device and storing data using encryption on sensitive data;
- *fairness*, meaning that your de-identified data ca be made findable, accessible, interoperable and reusable in an online data repository.

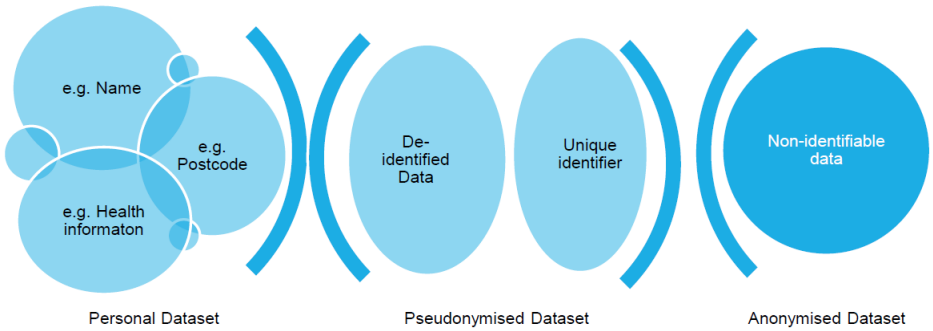

Figure 6. Data de-identification process [21]

However, in scientific research does not apply additionally data obligations if they would imply a disproportionate effort or redundant activities. In this case must be taken in the account the number of data subject, the age of data and the proper safeguards to be adopted, as stated in the Recital 62 and article 14 para.5. A particular focus must be oriented to the non-appliance of the Right to be Forgotten if there is a smallest chance to significantly impair data processing for scientific research purposes, as stated in Recital 65 and article 17 para.3 (d).

V. E-LEARNING ROLE IN GDPR COMPLIANCE

In order to get fully compliant to GDPR, universities must assure that at least the designated data protection officer is well prepared, with legal and technical knowledge, and he can fully understand GDPR. However, the data protection officer cannot contribute to a successful GDPR compliance if the other employees, or departments (Human Resources, Financial, Administrative) does not have staff ready to understand his requests on documents issued by. In order to get results in this segment of staff-readiness for GDPR, the easiest and cost-effective way to train them is to enroll in an e-learning training course regarding GDPR readiness or additional data protection topics.

The main objective of an e-learning training course on GDPR must be that the students to be able to identify personal data and how to control data processing. Lessons must cover issues like:

- How to process a request from data subject and obtain consent from data subjects;
- How to deal with consent withdrawal of data subjects;
- How to recognize and properly respond to suspected data breaches;
- How to realize data protection impact assessment and protect personal data;
- How to collaborate with the Data protection officer.

Covering all these issues, GDPR can be understood and the trained staff can ensure highest compliance level of GDPR. In order to get results in this segment of staff-readiness for GDPR, the easiest and cost-effective way to train them is to enroll in an e-learning training course regarding GDPR readiness or additional data protection topics. As a fact, some of the lessons, especially those related with obtaining/withdrawal consent, response to data breaches in requested time, realization of data protection impact assessment and the collaboration with Data protection officer could be interactively provided by professionals which already assumes the DPO role within their organizational framework.

VI. CONCLUSIONS

The legislative adoption of *EU General Data Protection Regulation*, proves that the EU authorities recognize the new realities on the individual rights and liberties and tries to solve possible conflicts in current legislation. The text of the *Regulation*, even though not explicitly put it, brings together in the effort to protect personal data three parties: management staff, legal staff and technical staff, that fact being obvious in the process of data protection impact assessment. A similar model can be observed in the NATO's Cyber Defence Pledge issued in July 2016, where is proposed and encouraged the cooperation between military, academia and industry.

The study of the Regulation text indicates that the personal data protection within the regulatory framework will be approached by a risk-based manner. In order to accomplish this purpose, must be implemented strict policies and practices not only for the current kept data but also for deleted or destroyed data. It is expected that in time, the implementation of GPDR to lead to a transformation not only in the manner to protect data but also in the manner organizations collaborate and do their business. Focusing on the GDPR impact on universities we must state the fact that the way it was projected, legislative text tends to preserve the balance between the need to effectively protect personal data and implicitly data subject rights, and in the meantime to allow processing of sensitive personal data for scientific research purposes. New Regulation also brings the idea of intensified, intimately cooperation between all parties involved in the internal process of processing data (research staff, human resources staff, IT staff etc.). However, in the research field, GDPR has the merit to impose sharp rules that support research activity when it comes to acquire consent from data subjects. The ethical standards had also been considering, Regulation text referring to them as a part in accomplishing the lawfulness of processing personal data in scientific research.

As a final remark we must add the fact that regarding scientific research a series of topics must be seriously addressed:

- issues regarding the costs in project financing, having in mind that processing data under GPR imply additional cost with necessary investments to reach GDPR compliant;
- issues related to the fact that scientific research could be used as a legal breach that allow less restrictions in personal data restrictions;
- issues regarding publication of research results that should be public available;

Reference Text and Citations

[1] Dănuț Turcu, *Cybernetics and Technological Evolution in the Information Age*, International Scientific Conference" Strategies XXI", vol. 3, Editura UNAp, Bucharest, 2014, pp.77-81

[2] Yoneji Masuda, *The Information Society as Post-Industrial Society*, World Future Society, Washington D.C., 1981, pp. 30-33.

[3] *Ibidem*, p.30

[4] *Ibidem*

[5] Internet World Stats, at www.internetworldstats.com/stats.htm

[6] S Topor, *Cyber criminal and cyber terrorist-two concepts that need to be differently treated*, - International Scientific Conference" Strategies XXI", vol. 3, Editura UNAp, Bucharest, 2016, pp. 181-186

[7] ***, Breach Level Index Report: Poor Internal Security Practices Take a Tool, Findings from the first half of 2017, Gemalto, New York, 2017

[8] Richard Stiennon, *Categorizing Data Breach Severity with a Breach Level Index*, at http://breachlevelindex.com/pdf/Breach-Level-Index-WP.pdf

[9] See cases like WikiLeaks, Snowden etc.

[10] ***, European Commission, *Factsheet on the "right to be forgotten" ruling*, at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, 2016.

[11] https://transparencyreport.google.com/eu-privacy/overview

[12] Theo Bertram et all, *Three Years of the Right to be Forgotten*, at https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view, p 1

[13] *Ibidem*, p. 9

[14] *Ibidem*, p. 5

[15] *Ibidem*, p. 1

[16] *Ibidem*, p. 15

[17] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, p. 3 (L119/3)

[18] ***, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*

[19] ***, Breach Level Index Report: Poor Internal Security Practices Take a Tool, Findings from the first half of 2017, Gemalto, New York, 2017, p. 11

[20] Elena SUSNEA, *Monitoring Student Activities in Social Networking*, The 13th International Scientific Conference eLearning and Software for Education Bucharest, April 27-28, 2017, p.539

[21] ***, *General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR*, The European Research Federation (EFAMRO)&ESOMAR World Research, Amsterdam Brussels, 2017, p.17, at www.esomar.org/uploads/public/government-affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf