CVIK, Eva Daniela, MacGREGOR PELIKÁNOVÁ, Radka. The Dark Side of the General Data Protection Regulation. In: Dvoráková, P.; Baisa, B. (eds.) *Proceedings of the 22nd International Conference Current Trends in Public Sector Research 2018,* January 18-19, 2018. Brno: Masaryk University, 2018. pp. 28-35 of 392. ISSN 2336-1239. ISBN 978-80-210-8923-5.

The Dark Side of the General Data Protection Regulation

CVIK, Eva Daniela[a], MACGREGOR PELIKÁNOVÁ[b]

[a] *Czech University of Life Sciences, Faculty of Economics and Management, Department of Law, Kamýcká 129, 160 00 Prague 6 - Suchdol, Czech Republic, cvik@pef.czu.cz*

[b] *University of West Bohemia, of West Bohemia in Pilsen, Faculty of Law, Department of Business Law, Sady Pětatřicátníků 14, 306 14 Pilsen, Czech Republic, radkamacgregor@yahoo.com*

Abstract

The Regulation (EU) 2016/679 on the protection of personal data (GDPR) was enacted in 2016 and it will apply from 25th May 2018 in the entire EU. The GDPR is a product of an ambitious reform and represents a direct penetration of the EU law into the legal systems of the EU member states. The EU works on the enhancement of awareness about the GDPR and points out its bright side. However, the GDPR has as well its dark side, which will inevitably have a negative impact. It is relevant and useful to identify problematic, controversial and unclear rules and institutions mandatorily brought by the GDPR, and propose recommendations about how to reduce, or even avoid, their negative impacts. These theoretic analyses are projected to the Czech case study focusing on municipalities, which offers fresh primary data and allows a further refining of the proposed recommendations. The GDPR, like Charon, is at the crossing, the capacity and knowledge regarding its application is critical for operating in the EU in 2018. There is no time to procrastinate in getting ready to address its bright and, more importantly, its dark side.

Keywords: Controller v. processor; Data protection officer; GDPR; Transparency.

JEL Classification: D82, K29, M15, O33.

1 Introduction

Within the framework of the ten year strategy Europe 2020, especially digital aspects and the technological potential of European economies [3] and its dynamics between old and new member states [4], the European Commission presented the Data Protection Reform Package. The EU is well aware that, although openness-oriented policies are to be associated with growth [12], human rights and freedoms deserve a serious consideration and protection vis-à-vis predatory, over liberal and advantage taking practices. An integral part of it was a proposal COM(2012)11 for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data which focuses both on the data storing and analyzing as well as the portability of the data, including Internet portability realized via emails or e-address books [2]. This mandatory drive for the unification of rules on the processing of personal data in the EU and its key features induced a noticeable wave of reaction [1],[24],[31]. Nevertheless, in April 2016 the Regulation (EU) 2016/679 on the protection of personal data - General Data Protection Regulation ("GDPR") was enacted with its taking effect planned already for May, 2018 (art.99 GDPR) .The GDPR has a broad reach which affects both public and private subjects, imposes a significant set of duties and principles upon them and threatens them with sanctions. Two of the many controversial features of the GDPR are (i) its general non-clarity and ambiguity and (ii) the compulsory introduction of the data protection officer ("DPO") (Art.37 et foll. GDPR). The municipalities have to understand the GDPR, make an audit of their setting and update it to make it compatible with the GDPR, and appoint and pay for a GDPR expert - the DPO, which will double check it and possibly report any discrepancy. The objective of this paper is threefold. First off, to rather theoretically analyze the clarity of the GDPR provisions, especially for data controllers and processors from the public administration sphere, and the issues linked to the search and appointment of DPOs (O1). Second, to rather practically, based on a micro case study, analyze whether municipalities are prepared for the GDPR (O2). Third, to suggest solutions of possibly identified challenges, namely to recommend what municipalities should do

to address the dark side of the GDRP (O3). The authors take full advantage of this pioneering investigation, interview the competent Association and generally their hands-on experience. Although Czech municipalities will be used for the case study and Czech field observations used, the conclusion linked to the legislative and secondary sources of a non-Czech origin is highly relevant for all subjects of the GDPR, regardless if whether Czechs or not.

2 Legislative and Literature Review

Focusing on O1, the legislative review rests on the overview of key provisions of the GDPR, while paying special attention to its general (lack of) clarity and to its special setting of the DPO. The GDPR clearly perceives the processing of the personal data of a natural (!) person as a fundamental right (Preamble (1) and Art.1 GDPR) and related to the Charter of the Fundamental Rights of the EU ("Charter") and to the Treaty on the Functioning of the EU ("TFEU"). The GDPR is conceptually embedded in the EU "constitutional triangle"[17], while endorsing the concept of the single internal market [15]. The European Commission indicates the general endorsement of the GDPR by up to 90% of Europeans and presents a bright picture of the GDPR [9]. The GDPR expands the definition of "personal data" and of "processing" (Art.4) and extends its reach to processing both within and outside the EU (Art.3). The bright picture starts to become darker with the definition of key subjects of the GDPR, "controller" and "processor" (Art.4).

Table 1. Controller and processor under the Art.4 GDPR (Source: Authors)

Function	Definition	Comments
Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; ….	All municipalities are "controllers" under GDPR and thus have to comply with it
Processor	a natural or legal person, public authority, agency or body which processes personal data on behalf of the controller...	Municipalities can become processors.

The GDPR provides a lot of mandatory principles, general and specific duties and requirements, along with references to various codes and other rules. In addition to the lawfulness, the processing is conditioned by a clear consent or other well defined reasons (Art.6)

Table 2. Principles relating to processing of personal data under the Art.5 GDPR (Source: Authors)

Personal data shall be processed
(a) processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
(b) collected for specified, explicit and legitimate purposes (purpose limitation)
(c) adequate, relevant and limited to what is necessary in relation to the purposes (data minimization)
(d) accurate and, where necessary, kept up to date (accuracy)
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (storage limitation)
(f) processed in a manner that ensures appropriate security of the personal data (integrity and confidentiality).
The controller shall be responsible for, and be able to demonstrate compliance with, all of them (accountability).

Neither the GDPR nor the European Commission nor other EU institutions or bodies provide explanations about the exact meaning of these principles. The created uncertainty is further magnified by the extent of the responsibilities of controllers. They include the responsibility of the controller which includes the implementation of appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDRP, including adherence to approved codes of conduct (Art.24). Each controller shall maintain a record of processing activities under its responsibility, including the name and contact details of the controller and the data protection officer, etc. (Art. 30). The controller shall seek the advice of the DPO (Art. 35). The controller shall designate a DPO in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consists

of processing operations which, by virtue of their nature, their scope and/or their purposes, requires regular and systematic monitoring of data subjects on a large scale (Art.37). Municipalities are not only a subject of the GDPR, but in addition must appoint their DPO – either their "own" or a "shared one", either as their employee or as their free-lance outsourcer. The tasks of a DPO are broad and can work for, as well as against, the particular controller.

Table 3. Tasks of the DPO under the Art.39 GDPR (Source: Authors)

The data protection officer shall have at least the following tasks:
(a) to inform and advise the controllers of their obligations pursuant to the GDPR and to other EU law provisions;
(b) to monitor compliance with the GDPR, with other Union or Member State data protection provisions...;
(c) to provide advice where requested as regards the data protection impact assessment and monitor;
(d) to cooperate with the supervisory authority;
(e) to act as the contact point for the supervisory authority on issues relating to processing.

The GDPR explicitly provides remedies, liabilities and penalties for any GDPR breaches (Art.77), such as the right to compensation and liability (Art.82) and imposition of administrative fines of up to 10 000 000 EUR or up to 2% of the total worldwide annual turnover or even up to 20 000 000 EUR or up to 4 % of the worldwide annual turnover (Art.83).

The literature review regarding the general (un)clarity of the GDPR and the special issue of the DPO begins, similarly to the legislative review, with a re-confirmation of the EU commitment to the doctrine of the famous four freedoms of movement on the single internal market [8] in the 21st century e-context [16],[20] and the very broad reach of the GDPR [27]. This commitment mirrors the interaction of public administration, business, law and information systems/information technologies in our global society, which is full of contradictions [31], of confusion between historical truth and reality [6], and of increasingly more complex and dynamic organization settings and proceedings [23] where the ultimate value is the information [18]. Since the electronization and resulting administration, processing and transferring of data should not lead to abuses and not impair the smooth operation of the single internal market, the EU decided to go for a unified legal regime inspired by the development of data privacy legislation on both sides of the Atlantic since the 1960s [28]. The EU's overly positive tenor is matched by the pragmatic voice of academia, which recognizes the anticipated benefit of law consistency in data protection in the entire EU [31],[32], but immediately adds that the GDPR poses new challenges in general [21],[25] as well as vis-à-vis special aspects [5],[7] to its subjects, including such public law entities as municipalities. It is suggested that they are not sufficiently aware about the exact demands of the GDPR, including the DPO, are not ready for it [28] and that the compliance will cost financially, as well as in time and effort, more than what is expected. It is illustrative to conduct and analyze a micro case study based on questionnaires completed by Czech municipalities (O1 and O2) and to imply new recommendations (O3).

3 Materials and Methods

The GDPR is a reforming regulatory piece of the EU legislation with a direct imminent application which expands the understanding and regulation of the processing of data of natural persons, and not only in the EU. This unequivocally determines both the materials and methods to be employed in the context of the three objectives – the ambiguity of the GDPR and its demands (O1) along with the un-readiness of the ultimate addresses – Czech municipalities – for the GDPR and compliance with it (O2), and recommendations about how to address this dark side of the GDPR (O3). The materials and methods further reflect that this is a multi-disciplinary topic requiring a truly open minded, pragmatic and not always conventional approach. Therefore, materials from heterogeneous sources must be researched and analyzed, namely (i) primary fresh data, obtained by questionnaire-generated research performed within the framework of the Czech micro case study focusing on selected Czech municipalities and their

perception of the GDPR supported by the informal interview with the Czech association of towns and villages ("Association"), (ii) secondary data generated especially by fresh (ideally from the last two years) academic writings and (iii) direct legislative data – a direct citation and exploration of the text of the GDPR itself. This diversity of materials needs to be explored and assessed by a set of methods and leading the van should be Meta-Analysis [26] complemented by critical comments and Socratic questioning [1]. Since the topic has strong legal aspects, the research and analysis are more qualitative than quantitative, and includes deductive and inductive aspects of legal thinking [22], as legal theoretic orientation reflects legal science which is argumentative, not axiomatic [13]. However, the opposition between qualitative and quantitative data and methods should not be exaggerated, since the available resources allow for addressing many of the research questions and issues related to the GDPR by combining and contrasting them [26]. The drive for an objective and neutral assessment and profiling must occur on both levels, qualitative and quantitative, and the employment of conventional methodology is challenging and "mathematization" is not to performed in a rigid manner [19].

The principal data novelty of this contribution consists in the pioneering investigation in the form of a questionnaire search performed vis-à-vis five Czech municipalities from central Bohemia. These five municipalities, homogenous as to their inhabitant types and heterogenous as to their resources, were interrogated based on a questionnaire including the following seven questions reflecting O1 and O2 and inducing ideas for assessment and improvements, i.e. for the ultimate recommendations for the GDPR compliance. In order to yield the most from this rather homogenous sample, the questionnaire included seven open questions targeting the awareness, preparation, realization of the GDPR compliance and its costs. In sum, these questions reflected the three objectives – how are you getting ready for the GDPR? (Q1), are you going to be ready in May 2018? (Q2), what expense do you expect? (Q3), how are you going to finance it? (Q4), do you understand your GDPR duties? (Q5), who will be your DPO? (Q6) and do you know how ready are other municipalities? (Q7).

Table 4. Questionnaire –7 questions given to 5 interrogated municipalities (Source: Authors)

Questions	
Q1	How are you getting ready for the GDPR – where are you right now with your compliance?
Q2	Are you going to be ready in May 2018, i.e. will you manage to become GDPR compliant by May 2018?
Q3	Do you have your GDPR financial calculations, i.e. what (initial) expense do you expect?
Q4	How are you going to finance the (initial) expense for the GDPR compliance?
Q5	Is the setting of your GDPR duties clear to you, i.e. do you understand your GDPR duties?
Q6	How will you resolve the DPO personnel issue, i.e. who will be your DPO (employee, free-lance, shared)?
Q7	Do you know how ready (far in their preparation) for the GDPR are other municipalities?

This legislative and secondary data is further explored via primary data generated by this original and pioneering investigation. The information is explored and the yielded knowledge and data are confronted in a holistic manner, while focusing on the Czech micro case study and recommendations implied by it, while considering also legislative and secondary sources.

4 Results and Discussion

The above presented legislative and literature review reveals that the GDPR is a new piece of strict legislation [2] which is much wider than the well-known concept of personally identifiable information under US privacy law [5],[10] and will be interpreted based on the teleological approach, i.e. its meaning is far from being either insignificant or obvious [11]. The only certainties are that the GDPR brings many new requirements to a broad pool of subjects [7], including municipalities, and that any breach is to be strictly sanctioned from May of 2018. It is necessary that each (potential) subject, e.g. municipality, performs an audit, analyzes the current status quo and needed changes in order to comply with the GDPR and implements these changes. This will entail both initial expenses and efforts as well as ongoing expenses and efforts

[14], see e.g. the payment and co-operation with the DPO [21]. To reveal more about the perspectives of ultimate addressees of these requirements and duties of the GDPR, a balanced set of five Czech municipalities were interrogated. Three of them are parts of the capital, Prague, one of them is a village near Prague and one of them is a town near Prague.

Table 5. Questionnaire – 5 interrogated municipalities from central Bohemia (Source: Authors)

Municipality	Surface in km²	Revenues/Expenditures in thousand CZK	Employees
M1 – in Prague	5,53	139 060/976 485	395
M2 – in Prague	24,22	814 826/750 706	358
M3 – in Prague	9,79	451 889/ 554 541	258
M4 – village	2,18	1 845/ 1 845	6
M5 – town	3432	175 46/ 196 305	61

All municipalities provided detailed answers with comments to all questions in (Table 6).

Table 6. Questionnaire – Answers to 7 questions provided by 5 interrogated municipalities (Source: Authors)

Quest.	M1	M2	M3	M4	M5
Q1 readiness	Employees´training, external audit	Employees´training, plans to order audit	Employees´training, external audit	So far nothing	Employees´training
Q2 timing	Hopes to manage	Hopes to manage	Believes to manage	Believes to..	Hopes to manage
Q3 expen.	No idea	Few millions CZK	No idea	No idea	No idea
Q4 financing	Extraordinary budget expense	Municipal budget	Municipal budget	Municipal budget	Municipal budget
Q5 clarity	Not really	Not really	Not at all	Not really	Needs exter. advice
Q6 DPO	Outsourcing, i.e. free-lance DPO	Dont know, wait for recommendation	New employee	Probably outsourcing	Probably outsourcing
Q7 others	Probably as we are	As we are, need for coordination	As we are, we exchange info	Has certain awareness	Info from the Association

These self-assessments reveal reduced awareness and problematic readiness. Additional comments and explanations provided by municipalities support it even further. The common tenor of the municipalities point out the dark side of the GDPR, or more precisely dark sides and paradoxes. Each municipality genuinely wants to be compliant with the GDPR, but no municipality truly understands what to do and what duties and requirements apply to it. Each municipality is ready to pay the necessary initial and even further costs, but no municipality knows roughly how much it will be. Each municipality plans on paying the expense from its budget, but does not have any special revenues or resources to offset it. This is a big issue, especially for municipalities with small budgets where "each CZK matters" and some of them even sadly stated that because of the GDPR no planned actions, investments and popular projects will be realized. The GDPR will take money desperately needed for critical municipal services. The DPO function is for all of them a clear stable and ongoing expense without bringing any noticeable benefit for the municipality. Some of them will hire an external (i) expert, either a law firm or other firm providing legal and data protection services, or (ii) create a new job and hire their own "DPO". Although all municipalities have some awareness about the (un)readiness and struggles of other municipalities, they all would appreciate more information, ideally up-to-date. This call for information and advice is further magnified by the readiness of certain municipalities to use a public procurement call and select an outside expert firm and hire it for the GDRP audit and assistance for the setting of the initial GDPR compliance. These voices calling for guidelines and counselling are a true phenomenon and the Czech municipal association, i.e. Association granted an informal interview and within it stated that approximately 15 500 public service entities will have to comply with the GDPR (6 300 municipalities, 5 100 maternal schools, 4 100 elementary schools) and that the Association expects a "sharing" of the DPO, i.e. the Association thinks that approximately 20 entities will agree about hiring the same external, free-lance DPO. There is no hard data, this is mere speculation. Nonetheless, it is worth

consideration, especially since the Association, in co-operation with human resource experts, came to a preliminary suggestion that each DPO will need to be paid approximately CZK 55 000 CZK brut per month, i.e. CZK 30 000 net per month. If this speculative prediction of the Association is met, then 775 DPOs are needed for the indicated public service entities and if each is going to "cost" CZK 55 000 per month, then the combined annual cost will reach 775 * CZK 55 000 * 12 = CZK 515 500 000 CZ. The investigation of municipalities indicates (at least at this point) a much weaker readiness to "share" a DPO and suggests that many more than 775 DPOs will be needed. Recently, the authors have been contacted several times via group emails by head-hunters offering a DPO job, or at least a bonus for a recommendation for a law and data protection expert ready to take a DPO job. The authors saw several offers to attend DPO and/or GDPR training for approximately CZK 10 000 per day. The GDPR, awareness about it, and the DPO function, have become an integral part of business in the EU.

5 Conclusion

The GDPR and the implementation of its requirements is neither obvious nor easy nor cheap [7],[11],[14],[27]. The performed case study, along with questionnaires, informal interviews and field observations, provides a rather grim picture. First, Czech municipalities have a low awareness about the exact content of the GDPR regime, and this even despite their efforts, and struggle with several features, such as the DPO. Second, these municipalities are not yet prepared for the GDPR and even do not know how they could be. However, they all pragmatically came to the same conclusion as already partially presented in the foreign academic press, i.e. that the compliance with the GDPR demands substantial financial and human resources, training of employees and guidance [28]. Hence, some of them have already allocated resources in their budgets for future years for "GDPR". From an accounting point of view, the GDPR is a clear expense for municipalities which often financially struggle and desperately attempt to have a balanced, and not a deficit budget. This prompts conclusions about the dark side of the GDPR and the perception of the GDPR as another bureaucratic, red-tape and expensive instrument from above [17],[19]. Well, the GDPR might have very bright aspects, especially from the above and long-term perspectives, and become a great opportunity [30],[31] and a leverage for the smart, sustainable and inclusive growth so vigorously called for by Europe 2020. However, many of its subjects, such as controllers and processors from the public sphere, perceive, and will perceive, its dark side [29]. The compliance with something unclear, complex and demanding is expensive and, at the same time, there is not enough time remaining and the price for non compliance is harsh, strict and heavy. These subjects, including Czech municipalities, understand that they have to "bite the bullet" and, in addition to financial resources, make other efforts. As already suggested, timely preparation is absolutely pivotal with respect to the GDPR [14],[24],[27]. Recommendations can be presented in this deplorable context. First, the EU should listen to bottom-up voices, provide a clear guidance [15], [23], e.g. via an Internet platform with clear advice in all languages of the EU member states [16],[20], and offer a leniency period and support. Second, each EU member state should engage in an open dialogue with subjects of the GDPR, provide resources (financial, informational, educational and other) to help them to reach compliance as soon as possible and send feedback and suggestions even to the EU. Third, Associations and other institutes should pool resources, and, via their www pages or other Internet platforms, offer conventional as well as on-line tutoring and advising [27]. Next, the public service entities would definitely benefit by a public procurement and central "sharing" of DPOs, perhaps based on annual renewal contracts allowing cancelling this type of service when these entities feel ready to perform "DPO in house". Lastly, each subject of the GDPR should genuinely work on increasing its awareness and information sharing with other subjects and implement the acquired knowledge in order to boost the GDPR compliance without any delay. The EU and EU member states should appreciate it and include it in their leniency programs. Europe 2020 and the GDPR should be here to serve

and help Europeans, not to punish them by bureaucratic demands! After all, the EU wants to increase its legitimacy and for this it needs smart and light (and not) dark sides of the GDPR!

6 References

[1] ARREDA, P.E. 1996. The Socratic Method. *Harvard Law Review*, 109(5): 911-922.

[2] AUWERMEULEN Van der, B. 2017. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law & Security Review*; 33, 57-72.

[3] BALCERZAK, A.P. 2016. Technological Potential of European Economy. Proposition of Measurement with Application of Multiple Criteria Decision Analysis. *Montenegrin Journal of Economics*, 12(3):7-17. DOI: 10.14254/1800-5845.2016/12-3/1

[4] BALCERZAK, A.P. 2015. Europe 2020 Strategy and Structural Diversity Between Old and New Memember States. Application of Zero Unitarization Method for Dynamic Analysis in the Years 2004-2013. *Economics & Sociology*, 8(2): 190-210.

[5] BOLOGNO, L., BISTOLFI, C. 2017. Pseudonymization and impacts of Big Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review,* 33, 171-181.

[6] CHIRITA, A.D. 2014. A legal-historical review of the EU competition rules. *International and comparative law quarterly,* 63 (2), 281-316 , DOI: 10.1017/S0020589314000037

[7] CRADOCK, E., STALLA-BOURDILLON, S., MILLARD, D. 2017. Nobody puts data in a corner? Why a new approach to categorizing personal data is required for the obligation to inform. *Computer Law & Security Review*, 33, 142-158.

[8] CVIK, E., MacGREGOR PELIKÁNOVÁ, R. 2016. Implementation of Directive 2014/17/EU and its Impact on EU and Member States Markets, from not only a Czech Perspectives. In: Kapounek, S., Krutilova V. (Eds.) 19th International Conference Enterprise and Competitive Environment (ECE) Brno. *Procedia Social and Behavioral Sciences*, 220, 85-94. DOI: 10.1016/j.sbspro.2016.05.472

[9] EUROPEAN COMMISSION, 2017. [online] *Reform of EU data protection rules.* Available on http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[10] GODDARD, M. 2017. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research,* 59(6), 703-705, DOI: 10.2501/IJMR-2017-050

[11] HERT de, P., PAPAKONSTANTINOU, V. 2016. The new General Data Protection Regulation: Still and sound system for the protection of individuals? *Computer Law & Security Review*, 32(2): 179-194. DOI: 10.1016/j.clsr.2016.02.006

[12] IYKE, B.N. 2017. Does Trade Openness Matter for Economic Growth in the CEE Countries? *Review of Economic Perspectives – Národohospodářský obzor*, 17(1): 3-24. DOI: 10.1515/revecp-2017-0001

[13] KNAPP, V. 1995. *Teorie práva*. 1 vyd. Praha, CZ : C.H.Beck.

[14] KRYSTLIK, J. 2017. With GDPR, preparation is everything. *Computer Fraud & Security,* 6, 5-8. DOI: 10.1016/S1361-3723(17)30050-7

[15] MacGREGOR PELIKÁNOVÁ, R., CÍSAŘOVÁ, J., BENEŠ, M. 2017. The misleading perception of the purpose of the protection against misleading advertising by the EU law and its impact on the Czech Republic. *Lawyer Quarterly,* 7(3): 145-161

[16] MacGREGOR PELIKÁNOVÁ, R. 2017. European Myriad of Approaches to Parasitic Commerical Practices. *Oeconomia Copernicana,* 8(2), 167-180. DOI: 10.24136/oc.v8i2.11

[17] MacGREGOR PELIKÁNOVÁ, R. 2014. *Selected current aspects and issues of European integration.* Ostrava, CZ : Key Publishing.

[18] MacGREGOR PELIKÁNOVÁ, R. 2014. The (DIS)harmony of opinions regarding domain names in the Czech Republic. *Scientific Papers of the University of Pardubice, Series D: Faculty of Economics and Administration*, 21(32): 73-84

[19] MacGREGOR PELIKÁNOVÁ, R., 2013. Internet My Dearest, What Type of European Integration Is The Clearest*? Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, 61(7): 2475-2481.

[20] MacGREGOR PELIKÁNOVÁ, R. 2012. And the best top level domain for European enterprises is ... *International And Comparative Law Review,* 12(2): 41-57.

[21] MALATRAS, A., SANCHEZ, I., Beslay, L., et al. 2017. Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review,* 33, 458-469.

[22] MATEJKA, J. 2013. *Internet jako object práva – Hledání rovnováhy autonomie a soukromí*. Praha, CZ : CZ NIC.

[23] PIEKARCZYK, A. 2016. Contemporary organization and a perspective on integration and development. *Oeconomia Copernicana*, 7(3), 467-483. DOI: 10.12775/OeC.2016.027

[24] PORMEISTER, K. 2017. Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law*, 7(2), 137-146. DOI: 10.1093/idpl/ipx006

[25] RAAB, Ch., SZEKELY, I. 2017. Data protection authorities and information technology. *Computer Law & Security Review*, 33, 421-433.

[26] SILVERMAN, D. 2013. *Doing Qualitative Research – A Practical Handbook*. 4th Edition, London, UK : SAGE.

[27] TANKARD, C. 2016. What the GDPR means for businesses. *Network Security*, 6, 5-8. DOI: 10.1016/S1353-4858(16)30056-3

[28] TIKKINEN-PIRI, Ch., ROHUNEN, A., MARKULA, J. 2017. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review* (in press). DOI: 10.1016/j.clsr.2017.05.015

[29] TUREČKOVÁ, K., NEVIMA, J. 2016. The Perils of Drawing from European Funds in Public Education. In: *Proceedings of the 11th International Scientific Conference Public Administration 2016*. Pardubice: University of Pardubice, Faculty of Economics and Administration, pp. 273-282. ISBN 978-80-7560-040-0.

[30] VIVANT, M. 2016. Building a Common Culture IP? *International Revue of Intellectual Property and Competition law,* 47(3), 259-261. DOI: 10.1007/s40319-016-0472-y

[31] ZERLANG, J. 2017. GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, 6, 8-11. DOI: 10.1016/S1353-4858(17)30060-0

[32] ZUIDERVEEN BORGESIUS, F.J 2016. Singling out people without knowing their names – Behavioural targeting, pseudonymouos data, and the new Data Protection Regulation. *Computer Law & Security Review*, 32, 256-271.