doi: 10.36689/uhk/hed/2018-01-055

Conceptual Impact of Selected Aspects of GDPR on Corporate Administration and Business Competition

Radka MacGREGOR PELIKÁNOVÁ, Eva Daniela CVIK

[1]Metropolitan University Prague, Prague, Czech Republic
radkamacgregor@yahoo.com
ruzickovaadvokat@gmail.com

Abstract. The General Data Protection Regulation (GDPR) was enacted in 2016 and will apply to automated processing and filing systems as of 25th May, 2018. However, the general awareness about the GDPR in the EU, and in particular in the Czech Republic, appears rather weak. Therefore, it is highly instructive to identify selected aspects of the GDPR, discuss their impact on businesses and especially their corporate administration, predict challenges and problems, and, most importantly, propose solutions in re how to adjust and comply with the GDPR requirements. This can be achieved based on both a fresh primary investigative data yield from Czech Businesses and comparatively explored secondary data which originated in different EU member states. Indeed, the mandatory and direct application of the GDPR is on its way to inevitably create new duties and will change many features of the corporate administration. However, the expected effective and efficient enforcement of the GDPR might ultimately reshape the current mechanism protection of intellectual property and increase the fairness of business competition.

Keywords: GDPR, Corporate Administration, EU, Competition, Controller and Processor.

1 Introduction

Under the auspices of the ten year strategy Europe 2020, and with the awareness about the need for the development of the technological potential of European economies [3], the European Commission moved to prepare and propose the Data Protection Reform Package. The proclaimed drive for smart, sustainable and inclusive growth, along with the critical importance of digitalization and virtualization, is among the principal engines behind this reform project. Hence, the European Commission presented 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. The concern is laid upon both the data storing and analyzing as well as the portability of the data, which is closely linked to the need of the Internet´s users´ need for transferring data they had been building up, such as in emails or e-address books[23]. Immediately, a part of the professional, as well as the

laic, public, realized that this can become a truly important piece of legislation affecting both the public and private sectors across the EU and having an impact on competition as well as corporate administration. In other words, the European Commission made it clear that mandatory rules on the processing of personal data in the EU are to be unified and set centrally from above. The opening significant wave of reaction and feedback followed. While certain businesses launched into a constructive dialogue and preparation, other businesses opted for ignorance or even fell into the pitfall of misconceptions. The four years long proposal stage ended in 2016 when the General Data Protection Regulation ("GDPR") was enacted with an application provision which surprised many – pursuant to Art.99, the GDPR shall apply from the 25th May, 2018 period. No cascade, selective or other progressive application mechanism was previewed, and the GDPR will basically apply throughout the entire EU, without any exceptions, starting 25th May, 2018. This led to a second wave of reaction and many "steamed-up" critical comments, often coming from the rank of businesses.

Pragmatically, at this point, *Alea iacta est*, the die is cast, and it is futile to make philippics on the (in) appropriateness of this Rubicon crossing. The GDPR is like *Hannibal ante portas,* and it is both wise and necessary to understand both its wording and underlying philosophy and concepts correct existing misunderstandings and draw practical points to be addressed by corporate administrations.

Since the GDPR has a massive reach and definitely belongs among the "more demanding" regulations, imposing duties to a large pool of subjects and threatening them with sanctions, it appears that the current corporate administration built upon today's intellectual property and competition demands, needs adjustments and that mistakes and negligence in this field can create a noticeable competitive disadvantage.

Considering the extent and depth of this material, its sophisticated and multi-disciplinary features and the limitation of available information resources, it is beyond the scope and capacity of this paper to provide a comprehensive and exhaustive list. Instead, this paper approached this subject matter both from theoretically academic and practical business perspectives, while focusing on a general approach to necessary corporate administration issues and possible changes due to selected aspects of the GDPR, and in particular their intellectual property and competition aspects.

2 Literature overview

The literature overview regarding the impact of selected aspects of GDPR on corporate administrations must necessarily start 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, digitalized, context [12]. This commitment represents the overlap of business, law and information systems/information technologies in our global society, which is full of contradictions [Vivant, 2016] and with the permanently blurred distinction between historical truth and reality [6].

Indeed, the post-modern, highly competitive global society is exemplified by digitalization [15], increasingly more complex and dynamic organizations [18], and the value of information, especially data with business significance, regardless whether they are about the business itself or its past, current or potential customers. Indeed, the EU understands that the operation of the single market and the competitiveness of European business is critical, that digitalization is indispensable in the global society [13] and the data is to be used but not abused, i.e. needs to be protected and ideally have the same legal regime across the entire EU. Indeed, data privacy legislation has been evolving with the modern IS/IT on both sides of the Atlantic since 1960s [22], see the German Act from 1970 and the Swedish Data Protection Act from 1973.

3 Sources and methods

Since the GDPR is a regulatory piece of the EU legislation and neither cascade application nor exceptions to its provisions are included, it is a reform, general and fully mandatory legal framework newly defining personal data and the regime of its protection in the EU, and possibly even beyond. This ultimately determines both the sources and methodology to be used in order to explore the impact of selected aspects of GDPR on corporate administrations.

Since this is a multi-disciplinary and multi-jurisdictional topic, an open minded approach needs to be embraced and a myriad of sources need to be explored. This research has to entail the GDPR and its official interpretation instruments, the academic writing and the field search, via interviews involving ultimate addressees of the GDPR, the businesses facing the need to make the necessary corporate administration changes.

This heterogeneity of source determines the selection of methods and the cross-disciplinary and multi-jurisdictional nature points to the processing by Meta-Analysis [21], while using a critical interpretation and application of selected GDPR provisions. This needs to be supported by the holistic perception of national contexts and by case studies. The primary and secondary sources are explored and the yielded knowledge and data are confronted with the expectation of the new real status quo. Since this paper covers legal and economic aspects, it focuses more on qualitative data and methods than quantitative, and includes deductive and inductive aspects of legal thinking [17], as legal theoretic orientation reflects legal science which is argumentative, not axiomatic [11]. Consequently, the dominating qualitative research and data are complemented by the quantitative research and data and their discussion is refreshed by Socratic questioning [1], and glossing.

The cornerstone of the mentioned Meta-Analysis is the performance and exploration of the field case study entailing the interviewing of seven Czech corporations. This pilot and pioneering investigation in the form of a questionnaire involved a representative sample. Namely, seven Czech corporations from various industries (a jam producer, a construction company, personal-human resources agency, etc.) were selected. They all have 250-500 employees, are active in the

private sector and either produce and commercialize goods or provide services and do not processes special categories of personal data (sensitive data). In order to reach the maximum potential from this equilibrated sample, the questionnaire included seven open questions targeting the awareness, preparation, endorsement, impact and predictions regarding the GDPR and its enforcement.

4 Legislative overview

The post-Lisbon EU has both supranational and intergovernmental natures with normative characteristics centered on the concept of the single market with significant institutional features and a competing interest group [10]. EU law, which is neither a typical international law nor a typical federal or state law, is integrated into national laws in a fierce and penetrative manner, i.e. by making use of a national procedural setting to directly incorporate and enforce its norms with the national jurisdiction of the EU member states [2] and the instrument for it, par excellence, is the Regulation. Hence, after launching the strategy Europe 2020 for the smart, sustainable and inclusive growth with a particular focus on the digital market, the focus of the European Commission turned to the Data Protection Reform Package and the preparation and enactment of a Regulation about general data protection became a top priority. The choice of the Regulation, instead of the Directive, was based upon the fundamental treaties of the post-Lisbon EU, TEU and TFEU, while observing the Charter of Fundamental Rights and building upon the already existing e-Privacy Directive [25], and the need to overcome various diversities [4] and [14] hindering the operation of the internal single market with a negative impact on business and even consumers. An overview on legislation based on TEU, TFEU and Charter is given in Table 1.

Table 1. The mapping overview of the legislative background for the GDPR

Legislative Instrument	Provision
TEU Art.6	1. The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.
TFEU Art.16	1. Everyone has the right to protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
Charter of	1. Everyone has the right to the protection of personal data concerning

Fundamental Rights Art.8	themselves. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3.Compliance with these rules shall be subject to control by an independent authority.

Thus, the GDPR sets general rules for the protection of personal data of natural persons and on free movement of this data (Art.1). These rules apply only to personal data as defined by the GDPR (Art.4) and only to subjects identified by the GDPR, i.e. mostly to the so-called controllers (Art.24) and processors (Art.28). So as to enhance compliance, the drafting of private codes of conduct is encouraged (Art.4). In case of a violation of duties set by the GDPR, such as the violation of the set principles (Art.5 et foll.) or of the rights of a data subject (Art.12 et foll.), the GDPR sets a strong monitoring mechanism, including even the internal data processing officers ("DPOs") (Art.37) and the outside public supervisory authority. The remedies, liability and penalty provisions are robust (Art.77 et foll.) and have an administrative, civil, even a potentially criminal nature. Thus, along with the compensation, damages and other private instruments, the administrative fines can reach EUR 20 million or up to 4% of the total worldwide annual turnover (Art.83). Logically, academic, professional and laic discussions about the GDPR focus on what and who exactly is covered by the GDPR, what exactly the GDPR demands and what must be done in order to comply with the GDPR, and if the GDPR is more a threat or an opportunity for businesses. Illustration of the GDPR structure is given in Table 2.

Table 2. Structure of the GDPR

Part	Selected provisions
Preamble (1)-(173)	…..
Chapter I General provisions Art.1-Art.4	Protection of personal data of a natural person (Art.1) All processing by EU subjects even without EU (Art.3) Definitions (Art.4)
Chapter II Principles Art.5-Art.11	Lawfulness of processing (Art.6) Conditions of consent (Art.7) Processing of special categories of personal data (Art.9)
Chapter III Rights of data subject Art.12-Art.23	Transparency (Art.12) Information and Access to personal data (Art.13) Right of access by the data subject (Art.15) Right to rectification (Art.16) Right to erasure (right to be forgotten) (Art.17) Right to data portability (Art.20)
Chapter IV	Responsibility of the controller (Art.24)

Controller and Processor Art.24-Art.43	Processor (Art.28) Controllers and processors cooperation with the supervisory authority (Art.31) Notification of a personal data breach to the supervisory authority (Art.33) Data protection impact assessment (Art.35) Data protection officer (Art.37)
Chapter V	Transfer of personal data to third countries or internal organizations
Chapter VI	Independent Supervisory Authority
Chapter VII	Cooperation and consistency
Chapter VIII	Remedies, liability and penalties
Chapter IX	Provisions regarding specific processing situations
Chapter X	Delegated acts and implementing acts

Regarding the question about "what is covered", one academic stream suggests that the re-definition of personal data and the new categorization of personal data (especially the recognition and special regime for sensitive data), both brought by the GDPR, have clear benefits and increase the transparency of the personal data processing [7]. It is emphasized that the GDPR, by categorizing personal data, prohibits processing of special categories of personal data (Art.9) and provides a set of exemptions, such as a rather comprehensive research exemption to this general prohibition of sensitive data [19]. Further, the GDPR provides for a pseudonymization (Art.5) and understands it as a technique to be combined with additional security measures [5]. However, data that is used to single out a person should be considered personal data and thus GDPR applies to behavioral targeting, i.e. online profiling by using cookies or other methods [25].

The academic press points to the fact that personal data breaches are frequent, often have a cross-border nature and seldom are effectively and efficiently sanctioned [16]. Namely, data protection authorities, labelled by the GDPR as "supervisory authorities," appear to regard the importance of the personal data protection and the approach to it in a rather different manner [20]. The introduction of the GDPR should improve the cooperation of data protection authorities and in general improve and synchronize the entire system [16], e.g. it should lead to a unified rigorous application of the GDPR to behavioral targeting via online profiling, without necessarily always tying this set of data to the particular individual [25].

This needs to be appreciated in the context of the current business setting and conduct, where personal data is an indispensable commodity and for some businesses storing, processing and analyzing personal data, especially about customers, is at the core of their business model [23]. It is suggested that, although the storing and analyzing of personal data under GDPR can be a subject of a conceptual criticism, it seems that the GDPR is on the right track towards the data portability in the EU [23]. Well, it is a right idea, but how should it be materialized? What exactly businesses have, or should, or should not do? These are the burning questions …

5 Results and discussion

Information about the large majority of the world population is collected and processed, often for private business purposes, e.g. Facebook collects information about over 1.5 billion people and Google over 90% of Internet users [25]. The density and intensity of data processing, especially the personal data processing, in the EU is extremely high and logically a harmonized, or even unified, legal regime is a must, and not only for a digital market pursuant to the Europe 2020.

The GDRP, along with other instruments, such as the Charter and ePrivacy Directive, creates a new framework for the processing of personal data. The GDPR aims to meet the current challenges related to the data protection, strengthen online privacy rights and boost European digital economy [22]. The GDPR is a regulation and this is self-explanatory regarding its force. However, provisions about private codes and other indices, even from competent authorities, indicate that the application of the GDPR will not be totally rigidly unified across the EU.

It seems that, so far, explanatory notes and other intrinsic documents provided by the EU, namely the European Commission, do not manage to remove unclearness. Hence, it continues the rather reduced awareness about the exact meaning and extent of the GDPR duties. Academic literature on the topic is rather fragmental and focuses on just a few, often for daily business marginal, aspects and thus general hesitations prevail. Headhunters and education providers react to it by searching for specialists understanding the GDPR and present them to the subject of duties of the GDPR. In the Czech Republic, for example, the recruiter, Hays, offers financial recompense for recommendation of a good client to be an "inhouse lawyer – data privacy" and even a gdpr.cz domain was created to offer GDPR classes for significant fees.

In order to understand better this, as yet, not researched field, a set of interviews was performed with a rather homogenous group of businesses, which will be subject to the GDPR. Namely, seven Czech corporations with 250-500 employees were interviewed based on seven open questions. These corporations were from various industries, but none of them processes special categories of personal data (sensitive data).

Interestingly, this piloting testing supports what has been already intuitively suggested. Boldly, corporations are ready to make administrative and even financial efforts to comply with the GDPR, but they have a hard time to understand what exactly the GDPR expects from them. They are realistic about the impact of the GDPR and recognize that an unfair competition behavior is possible. At the same time, they are optimistic and hope that this will be just temporary and, over time, the GDPR and its requirements will become both clear and fairly enforced. Further, as is often the case, a segment of Czech corporations perceive the GDPR as another futile administrative burden from Brussels. Based on the above provided literature and legislative overview, it can be suggested that this feeling in respect of the GDPR is caused rather by a lack of communication and explanation more than by the intrusive or inherently wrong concepts of the GDPR. Boldly, all point to the one big need – the need for more information ideally provided by a certified, or other official, authority.

Table 3. Summary of the interview of seven Czech corporations regarding the GDPR

Question	
1. Are you ready for GDPR?	All corporations are studying GDPR, arranging for training of competent persons and undergoing an audit regarding what type of data and processing they perform. No corporation is ready at this point, but all work towards being compliant in 2018.
2. Is GDPR needed?	Three corporations perceive the GDPR as needed due to the current partial regulatory vacuum. However, two corporations consider current legislation as sufficient and perceive the GDPR as another unnecessary normative burden from Brussels.
3. Are GDPR duties clear to you?	All corporations perceive the GDPR as unclear and are afraid that they might misunderstand certain provisions and make wrong preparatory steps. They miss certification authorities or other organs able to provide them with explanations.
4. Are theoretically set general conditions of the GDPR a challenge for you?	All corporations like the fact that these general conditions are universal and thus apply to all businesses dealing with certain types of data. All corporations perceive this as fair and indicate that they will use external experts (lawyers, IT specialists) in order to achieve the compliance with the GDPR.
5. What are the biggest issues linked to the GDPR implementation?	All corporations recognize a noticeable administrative burden created by the GDPR and four of them underline that this will cause significant financial expenditures which will reduce the capacity of the given corporation to modernize and develop.
6. Will the GDPR have an impact on the competition?	All corporations fear that the GDPR will have a negative impact on the competition, especially they expect unfair competition behavior by their competitors and (fictive) denunciations about (alleged) breaches of the GDPR to competent authorities. They all are afraid that the GDPR will become an instrument for "dirty" business battles, especially since the GDPR administrative fines are really high.
7. Will the GDPR create a competitive disadvantage for you?	Three corporations do not worry about that and think that even if some corporations will not observe the GDPR or try to manipulate it against their competitors, this will not significantly hurt the competition and its fairness. The corporations think that their competitors will not comply and so might save time, money, effort, etc. However this competitive disadvantage for compliant businesses will be just temporary, because over time the GDPR system will be put truly into the practice and everyone will have to comply.

Knowledge is power and communications are an indispensable necessity in the 21st century. The Europe 2020 fits this line. The above tables demonstrate that the GDPR will have an impact on business conduct and ultimately corporate administration and that the employment of IS/IT, the liability issue and the efficiency and efficacy of the

GDPR enforcement are interrelated and important for businesses. Businesses appear to be aware about the existence of the GDPR, but they do not understand fully its requirements. Some businesses even do not see a raison d'être for the GDPR. Nevertheless, they dare not ignore it and recognize that the GDPR has the potential to change the landscape of business and business conduct in the EU. The most surprising common denominator from all interviews, backed by a further field search, is that businesses are inclined to at least partially "outsource" some or even all duties and requirements generated by the GDPR. Boldly, they prefer hiring external specialists in addition to certain adjustments of their internal corporate administration, i.e. to cooperate with free-lance experts rather than to have a GDPR specialist on staff. This might be a Czech particularity, because Czech corporations acted in a similar manner to the new legal liability of executives, i.e. instead of internal changes and professional liability insurance, they heavily rely on external advisors and so attempt to transfer the liability to them [9].

In addition to the Czech drive to push the "GDPR issue" out, rather than take it in and make internal changes even regarding human resources, Czech businesses expect that there will be black sheep among themselves, ignoring or cheating vis-à-vis GDPR requirements and this will have an unfair competition impact. This further confirms that the GDPR is perceived by businesses as a short-term threat, rather than an opportunity. However, it is possible to observe a trust in the enforcement mechanism and ultimately an effective and efficient application of the GDPR, because businesses believe that in the long term the unfair competition impact might evaporate.

Indeed, these findings match the legislative overview. The GDPR is complex, and businesses are struggling to understand what exactly is newly expected from them, i.e. to what extent and how they should change their corporate, and other, administration to comply with the GDPR. They study and make some changes, but they feel a further need to employ external experts. Hence, there are clear efforts and costs to expend. Over time, these efforts and costs should be less dramatic, and ultimately all competing businesses will have to make them. Nevertheless, before this stage is reached, a myriad of unfair competition behaviors can occur and GDPR complying businesses might have a business disadvantage for a limited period of time. The common tenor expresses the hope that this limited period of time will be not too long and that at the very end the compliance with GDPR by all business will provide a better competition and market environment for all stakeholders, including consumers.

6 Conclusions

The post-Lisbon EU and Europe 2020 are aware that data protection in general, and the related ICT expertise, are extremely important and at the same time ephemeral and moving targets, i.e. there is no ideal state in data protection, instead it is an ongoing learning process [20]. Since the single internal digital market cannot afford a fragmentation in this respect, the European Commission brought the Data Protection Reform Package, including the GDPR.

It cannot be overstated that the GDPR is not a mere directive, it is a regulation going not only for harmonization, but directly for unification and its provisions will generally apply from 2018. Hence, the EU made a strong move towards a mandatory framework regarding protection of personal data of natural persons and on free movement of this data. This ultimately leads to the situation that businesses will easily fit in the category of controllers or processors of personal data and hence will become subjects to many duties.

The results from the pioneering Czech pilot case study support the suggestions already presented in the academic press that the exact content of these duties is generally perceived as unclear and that businesses feel that, despite their efforts, they have a rather weak awareness of the very impact of the GDPR on their management and business conduct, including necessary changes of corporate administration. However, the Czech pilot case study brought forth new indices that businesses feel clearly that the GDPR poses new challenges to businesses. This is complemented by the academic findings that GDPR requirements demand substantial financial and human resources as well as training of a large part of the staff [22]. According to the Czech pilot case study, facing the risk of high fines, at least Czech businesses appear to not only consider internal changes and improvements due to the GDPR, but as well to be inclined to hire external experts from the field of IT and data protection law. Few businesses want to directly hire them and keep them on the exclusive basis, but the majority of businesses seem to be inclined to just use them as free-lance experts and knowing that they can perform similar businesses for other businesses. This seems to be a compromise solution, reducing the liability and requiring manageable costs and minimal efforts, which is critical vis-à-vis the real risk that some businesses, including competitors, will ignore or undermine the GDPR and temporarily could have an unfair competitive advantage. However, there is a belief that the GDPR will be effectively and efficiently enforced, at least in the mid-term and long-term time horizons, so the unfair competitive advantage will be only for a manageable time period. Boldly, the compliant businesses cannot spend too much on GDPR for too long while other businesses would skip these large costs for a long time period. It will be extremely beneficial to compare the indices generated by the Czech pilot case study with other studies, ideally involving similar questions and more respondents, both from the Czech Republic and other EU member states studies. Since currently there is an absence of such studies, the authors are considering performing them in the future and naturally present the outcome in the academic press.

There are no indices that the EU, namely the European Commission, has a clear plan how it will improve the awareness about the GDPR and how aggressively will enforce the compliance. However, the businesses seem to have already made their outsourcing choice while hoping that shortly this will be followed by the remaining businesses. Well, the near future will show whether this strategy and prediction will be met. Nevertheless already three statements are generally accepted. Firstly, the GDPR is a big unknown which is perceived as a challenge and perhaps even a threat by businesses. Secondly, there is clear potential for unfair competition caused by the fact that some businesses will spend time and efforts to comply with the GDPR while other will skip them and cross their fingers. Thirdly, businesses are resolving the

GDPR issues by cooperating with free-lance experts in a hope that this is more safe, cheaper and more flexible than employing them, and once the enforcement will truly kick in, they can adjust their strategy, e.g. to use less external experts and rather make their own staff to be better trained with respect to the GDPR and perhaps to have their own GDPR specialist and/or data protection officer. In sum, the GDPR can after all achieve its goals and also improve the European integration and competition on the single internal market and businesses are open to cooperate actively in this respect, provided one *conditio sine qua non* is met – the GDPR must be effectively and efficiently enforced. If not, then the dark unfair competition might prevail and become another large error of the European integration … an error which the post-Lisbon EU in the Brexit context could hardly afford.

Acknowledgements. This contribution was supported by GA ČR No. 17-11867S „Comparison of the interaction between the law against unfair competition and intellectual property law, and its consequences in the central European context."

References

1. Areeda, Ph.E.: The Socratic Method. Harvard Law Review 109(5), 911-922 (1996).
2. Azolai, L.: The Force and Forms of European Legal Integration, EUI Working Papers, 2011/6, http://cadmus.eui.eu/bitstream/handle/1814/16894/LAW_2011_06.pdf?sequence=1, last accessed 2017/07/01.
3. Balcerzak, A.P.: Technological Potential of European Economy. Proposition of Measurement with Application of Multiple Criteria Decision Analysis. Montenegrin Journal of Economics, 12(3), 7-17 (2016). DOI: 10.14254/1800-5845.2016/12-3/1.
4. Balcerzak, A.P.: 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 (2015).
5. Bologni, L., Bistolfi, C.: Pseudonymization and impacts of Big (personal/anonymous) 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 (2017).
6. Chirita, A.D.: A legal-historical review of the EU competition rules. International and comparative law quarterly 63 (2), 281-316 (2014), DOI: http://dx.doi.org/10.1017/S0020589314000037
7. Cradock, E., Stalla-Bourdillon, S., Millard, D.: 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 (2017).
8. Cvik, E.. MacGregor Pelikánová, R.: 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 (2016a). DOI: http://dx.doi.org/10.1016/j.sbspro.2016.05.472.
9. Cvik, E.D., MacGregor Pelikánová, R.: A comparative study of the legal lability of executives in LLC in the Czech Republic and some of other EU member statests. Scientific Papers of the University of Pardubice, Series D 1/2016, 36, 54-65 (2016b).

10. Damro, C.: Market power Europe. Journal of European Public Policy 19(5), 682-699 (2012).
11. Knapp, V. : Teorie práva. 1. Vyd. Praha, ČR : C. H. Beck. (1995).
12. MacGregor Pelikánová, R.: European Myriad of Approaches to Parasitic Commerical Practices. Oeconomia Copernicana 8(2), 167-180 (2017). Doi: 10.24136/oc.v8i2.11.
13. MacGregor Pelikánová, R.: Selected current aspects and issues of European integration. Ostrava, CZ : Key Publishing (2014a).
14. MacGregor Pelikánová, R.: 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 (2014b).
15. MacGregor Pelikánová, R.: And the best top level domain for European enterprises is ... International And Comparative Law Review 12(2),41-57 (2012).
16. Malatras, A., Sanchez, I., Beslay, L., et al. 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 (2017).
17. Matejka, J.: Internet jako objekt práva – Hledání rovnováhy autonomie a soukromí. Praha, ČR : CZ.NIC. (2013).
18. Piekarczyk, A:. Contemporary organization and a perspective on integration and development. Oeconomia Copernicana 7(3), 467-483 (2016), DOI: 10.12775/OeC.2016.027.
19. Pormeister, K.: Genetic data and the research exemption: is the GDPR going too far? International Data Privacy Law 7(2), 137-146 (2017), DOI: https://doi.org/10.1093/idpl/ipx006
20. Raab, Ch., Szekely, I.: Data protection authorities and information technology. Computer Law & Security Review 33, 421-433 (2017).
21. Silverman, D.: Doing Qualitative Research – A Practical Handbook. 4th Edition, London, UK : SAGE. (2013).
22. Tikkinen-Piri, Ch., Rohunen, A., Markkula, J.: EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review (in press) (2017).
23. Van der Auwermeulen, B.: How to attribute the right to data portability in Europe: A comparative analysis of legislations. Computer Law & Security Review 33, 57-72 (2017).
24. Vivant, M.: Building a Common Culture IP? International Revue of Intellectual Property and Competition law 47(3), 259-261. (2016), DOI: http://dx.doi.org/10.1007/s40319-016-0472-y
25. Zuiderveen Borgesius, F.J.: Singling out people without knowing their names – Behavioural targeting, pseudonymouos data, and the new Data Protection Regulation. Computer Law & Security Review 32, 256-271 (2016).