ACTA UNIVERSITATIS AGRICULTURAE ET SILVICULTURAE MENDELIANAE BRUNENSIS

Volume 66 153 Number 6, 2018

IMPACT OF GDPR SECURITY MEASURES ON THE INTELLECTUAL PROPERTY AND UNFAIR COMPETITION

Radka MacGregor Pelikánová[1], Eva Daniela Cvik[1]

[1]Metropolitan University Prague, Dubečská 900/10, 100 31 Prague 10, Czech Republic

To cite this article: MACGREGOR PELIKÁNOVÁ RADKA, CVIK EVA DANIELA. 2018. Impact of GDPR Security Measures on the Intellectual Property and Unfair Competition. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis,* 66(6): 1535–1542.

To link to this article: https://doi.org/10.11118/actaun201866061535

Abstract

The 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 ("GDPR") created a duty to implement appropriate technical and organizational measures to ensure a level of security to protect natural persons with regard to the processing of personal data. Infringement of this duty is severely punished. These GDPR security measures and their operation should effectively and efficiently reflect intellectual property ("IP") and unfair competition concerns. The theoretic teleological interpretation of the GDPR along with the critical study of the academic literature is complemented by a practical exploratory investigation via a micro-case study based on interviews of a well-balanced group of subjects of this GDRP duty – Czech SMEs. Although the yielded results are rather indicative than generally conclusive, they allow to suggest a partial confirmation of the proposed hypotheses that this GDPR duty will have a significant impact on IP and unfair competition. The semi-conclusions based on the primary and secondary data enlightens the status quo, offers recommendations and brings suggestions for further research.

Keywords: Europe 2020, GDPR, intellectual property, IT, unfair competition, security measures

INTRODUCTION

In 2010, a new ten-year strategy for the EU was launched ("Europe 2020"). Europe 2020 has three priorities, i.e. smart, sustainable and inclusive growth, and focuses on the single internal market (Staníčková, 2017) and in particular on its digital aspects and the technological potential of European economies (Balcerzak, 2016). There are studies analyzing the status quo and future developments of sustainability reporting in Central and Eastern Europe (Horváth *et al.*, 2017). The EU believes that openness-oriented policies are to be associated with growth (Iyke, 2017) but need to be balanced with the need for protection of human rights and freedom. This is reflected by endeavors of the EU under the auspices of Europe 2020, such as the Data Protection Package which brought forth the Regulation (EU) 2016/679 on the protection of personal data – GDPR. Interestingly, no cascade taking effect or time exemptions are previewed, thus the whole GDPR applies as of May 25, 2018, throughout the entire EU, regardless of the standpoint of national laws. One of the many duties brought by the GDPR is implementing appropriate technical and organizational measures to ensure a level of security (Art. 32) to protect natural persons regarding processing of personal data (Art. 1).

This prompts interest in the understanding and appreciation of this duty and its impact. It is far from being established, the legislative wording is not self-explanatory, academics and practitioners quarrel about it and, there is low awareness about it (Tikkinen-Piri *et al*., 2018), similarly to the case of the implementation of IFRS standards to national accounting systems (Jindřichovská and Kubíčková, 2017). The implementation of the mandatory GDPR measures has an impact on the IP and unfair competition and, vice versa, the IP and unfair competition influence the implementation of the mandatory GDPR measures. According to the three set hypotheses, the impact is significant for both IP and the protection against unfair competition and represents a serious challenge for SMEs. The performed theoretical and practical study confirms these hypotheses just partially by Czech SMEs.

MATERIALS AND METHODS

The GDPR is an integral part of the Data Protection Package with a direct impact on the data protection, including processing, in all EU members states and even beyond. It is necessary to study the legislative wording and provided official comments, i.e. the GDPR and glossary and/or explanatory comments to it provided by the European Commission need to be understood while using the EU law interpretation approach par excellence – the teleological approach. The resulting information needs to be critically appreciated, concurrent with studying the current academic literature. The combination of information generated by the legislation and academic secondary sources represents the theoretical part, which is to be complemented by a practical part. After a contextual reflection, the exploratory investigation via a case study was selected. It was performed via interviews of a well-balanced group of respondents – Czech businesses having the legal form of a Limited Liability Company (aka Ltds), employing less than 250 employees and doing business in various fields of industry. Due to the confidentiality and other concerns, only a micro-sample of responding subjects was explored.

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 (Matejka, 2013), as legal theoretic orientation reflects legal science which is argumentative, not axiomatic. The opposition between qualitative and quantitative data and methods should not be overplayed, rather their synergy effects projected in the Meta-Analysis should be taken advantage of (Nevima and Majerová, 2015). The theoretic and practical parts were methodologically dominated by the Meta-Analysis (Silverman, 2013) complemented by critical comments and Socratic questioning (Arreda, 1996). The proposed hypotheses are A) that the GDPR duty to implement appropriate technical and organizational measures to ensure a level of security to protect natural persons with regard to the processing of personal data (Art. 32) will have a significant impact on the IP (H1) and B) on unfair competition (H2) and C) that this impact is a serious challenge for SMEs, namely for the Czech business Ltds with less than 250 employees (H3). These hypotheses were set based on the suggestions generated by the theoretical part, i.e. a legislative and academic analysis, and were confronted by the practical part of the investigation with questionnaires. Only a partial confirmation was achieved and fresh indices were offered by these Czech SMEs. The interaction of semi-conclusions based on the primary and secondary data addresses the hypotheses, provides a picture of the status quo, offers recommendations and brings suggestions for further research.

Legislative and Literature Overview

Despite the permanently blurred distinction between the historical truth and the reality of the EU (Chirita, 2014), it can be stated that the current EU and EU laws are marked by both supranational and intergovernmental features and by normative characteristics linked to the concept of the institutionalized single market with competing interest groups (Damro, 2012). The four freedoms of movement in this single internal market are getting progressively more competitive and more digitalized (MacGregor Pelikánová, 2017), while the EU member state societies, as well as the global society, are both getting more reliant on information systems/information technologies ("IS/IT") and more full of contradictions (Vivant, 2016). Clearly, the EU post-modern, highly competitive society is marked by digitalization (MacGregor Pelikánová, 2012), puzzling complex and dynamic organizations (Piekarczyk, 2016), and an increase in the value of information, especially data with business significance. Personal data, in particular, is recognized as an indispensable commodity and its storing, processing and analyzing can be at the core of the business model of many businesses (Auvermeulen, 2017).

The EU is an international organization sui generis. EU law has features of both international law (primary EU law) and federal law (secondary EU law) and is integrated into national laws in a fierce and penetrative manner (Azolai, 2011). Once the strategy Europe 2020 was brought out, the European Commission launched legislative initiatives targeting the digital market, including the Data Protection Reform Package to harmonize, if not unify the so-far, diversified, national law settings. The drive for Regulations, in addition, or even instead of, previous Directives, such as the e-Privacy Directive (Zuiderveen, 2016), was the resultant demand to overcome various diversities (Balcerzak, 2015 and MacGregor Pelikánová, 2014) negatively impacting the operation of the internal single market.

The decade long evolution (see the German Act from 1970 and the Swedish Data Protection Act from 1973) of data privacy legislation in Europe (Tikkinen-Piri *et al.*, 2018) reached, in the context of IS/IT, a point for a need of unification. The Data Protection Package, as one of the legislative pillars generated by Europe 2020, brought about 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 on the data storing and analyzing as well as the portability of the data (Auwermeulen, 2017). The EU move from the harmonization to the unification of rules on the processing of personal data generated strong academic feed-back (Portmeister, 2017 and Zuiderveen, 2016) and was completed by the enactment of the GDPR in 2016, which impacts data processing as well as processing of other types, such as e-payments (Schlossberger, 2016).

The GDPR is in compliance with the EU "constitutional triangle" – the TEU, TFEU and Charter, while recognizing the critical aspect of the single internal market for the modern European integration (MacGregor *et al.*, 2017). The long list of GDPR mandatory principles and duties includes lawfulness, fair and transparent processing (Art. 5 et foll.), the duty of security processing through the implementation of appropriate technical and organizational measures (Art. 32) and the duty of notification of a personal breach to the supervisory authority (Art. 33) and to the data subject (Art. 34). These duties apply to both public and private subjects processing the personal data of a natural (!) person (Art. 1) and their breach is punished by sanctions in the form of remedies, suspension, compensation and administrative fees up to EUR 10 million or 2% of the total worldwide turnover, or even EUR 20 million or 4% of the total worldwide turnover (Art. 77 et foll.). The European Commission indicates the endorsement of the GDPR by up to 90% of Europeans and presents a bright picture of the GDPR (European Commission, 2017). Do European businesses understand their duty and thus become ready to process data "in a manner that ensures appropriate security of the personal data" (Art. 5)? The teleological approach suggests considering the spirit of this legislation, i.e. the internal single market.

The literature overview shares the same pathway as the legislative overview. Indeed, it recognizes the EU commitment to the doctrine of the four freedoms of movement in the single internal market (Cvik and MacGregor Pelikánová, 2016) in a 21st century digital context (MacGregor Pelikánová, 2012) and the broad reach of the GDPR (Tankard, 2016). So the EU opted for a unified legal regime but academia commented on this exceedingly heavily praised presented drive of the EU via pragmatic and more objective observations. Included would be that personal data breaches in the IS/IT environment are frequent, often have a cross-border nature and rarely are effectively and efficiently sanctioned (Malatras *et al.*, 2017 and Turečková, 2014)), that GDPR offers law consistency in data protection in the entire EU (Zerlang, 2017 and Zuiderveen Borgesius, 2016), which brings both general (Piekarczyk, 2016) and specific threats and issues (Pormeister, 2017) and about which there is not enough awareness (Raab and Szekely, 2017). Regarding the duty to implement appropriate technical and organization measures to ensure a level of security to protect a natural person's personal data, it is important to unify the, so far, very diverse approach and regime of the controlling data protection authorities, labeled by the GDPR as "supervisory authorities" (Raab and Szekely, 2017) so as to reach a unified, effective and efficient application of the GDPR in the EU.

A legislative and literature overview may support a confirmation of the stated three hypotheses. Yet, this needs to be verified by a Czech case study, i.e. the secondary data implications need to be confronted with the fresh direct data.

I: *Questionnaire with replies provided by the 1st respondent*

Questions	Answers
1. Your business field?	Buying-selling cars.
2. Administration of your IS/IT	Outsourced to an external IT firm (in-house expensive)
3. Protection before the GDPR	Just antivirus programs for all PCs.
4. Protection due to the GDPR	Updating antivirus programs and monitoring based on IP licenses.
5. Introductory costs of the new protection	CZK 130 000
6. Brand new protection measure	Nothing
7. Performed penetration test.	Not yet.
8. Exchange of information about the GDPR with other business.	No.
9. Do you expect an unfair competitionimpact of the GDPR?	No, but expect speculative denunciations by competitors to authorities about alleged security incidents.

Source: Prepared by authors based on their micro pilot case study investigation performed in 1/2018.

Czech Case Study

As stated above, the theoretic, legislative and academic findings are to be confronted with the reality of the primary data generated by the pilot case study of the perception of GDPR, specifically of the impact of certain aspects of the GDPR, by both a homogenous and still representative micro-sample of Czech SMEs, i.e. the exploratory investigation was performed through interviews of a well-balanced group of respondents – 5 Czech Ltds with less than 250 employees and operating in various fields of industry. Nine semi-open questions were selected in order to address the set of the three hypotheses.

The answers and information provided by the 1st respondent belong to the mainstream represented by the outsourcing and licensing of IP issues, the readiness to pay "extra" due to the GDPR and a contradiction – not doing a penetration test and being afraid that security incidents and their reporting can have an unfair competition impact.

The answers and information provided by the 2nd respondent belong to the mainstream as in the case of the 1st respondent. A new piece of information is that security incidents and their reporting can cause unfair competition not only because of the punishment by the GDPR, but in addition can harm the good reputation of the business.

Feedback provided by the 3rd respondent belongs to mainstream.

Answers and information provided by the 4th respondent differs significantly due to the essence and technical background of this business. Logically, the 4th respondent does not need outsourcing, as he provides outsourcing services himself. The knowledge and awareness of the 4th respondent is superior and this is reflected by the successful performance of the penetration test, by active involvement of the employees – some of them are even authors of measures to satisfy the GDPR requirements and by the interest in the information and methodology from the Czech Data Protection Office ("CDPO").

Answers and information provided by the 5th respondent belong to the mainstream as in the case of the 1st , 2nd and 3rd respondent. A new piece of information is that the fear is linked directly to the reporting to the named supervisory authority, the CDPO.

II: *Questionnaire with replies provided by the 2nd respondent*

Questions	Answers
1. Your business field?	HR agency – Personal agency.
2. Administration of your IS/IT	Outsourced to an external IT firm for a fixed monthly fee.
3. Protection before the GDPR	Nothing special, passwords to all PCs.
4. Protection due to the GDPR	Employee training, setting security monitoring, services from the external IT firm.
5. Introductory costs of the new protection	CZK 98 000
6. Brand new protection measures	Nothing
7. Performed penetration test.	Not yet.
8. Exchange of information about…	No.
9. Do you expect unfair competition impact of the GDPR?	Trust in an effective and efficient enforcement of the GDPR. Concern about the medialization of (alleged) security incidents and harm to the reputation.

Source: Prepared by authors based on their micro pilot case study investigation performed in 1/2018.

III: *Questionnaire with replies provided by the 3rd respondent*

Questions	Answers
1. Your business field?	Tax advising.
2. Administration of your IS/IT	Outsourced to an external IT firm for a fixed monthly fee.
3. Protection before the GDPR	Passwords + antivirus programs for all PCs.
4. Protection due to the GDPR	Employee training, security monitoring, enhanced passwords, updating antivirus programs, data encryption based on IP licenses.
5. Introductory costs of the new protection	CZK 90 000 (CZK 60 000 updating old + CZK 30 000 for new IP)
6. Brand new protection measure	Ten new IP encryption licenses – Program Area Guard Neo for CZK 30 000.
7. Performed penetration test.	Not yet.
8. Exchange of information about…	No, just sharing trainings and schooling.
9. Do you expect unfair competition…?	No.

Source: Prepared by authors based on their micro pilot case study investigation performed in 1/2018.

RESULTS AND DISCUSSION

The GDRP creates a new framework for the processing of personal data. The general goals are strengthening online privacy rights and boosting European digital economy (Tikkinen-Piri *et al.*, 2018). One of the specific goals is to mandatorily introduce the duty of security processing through the implementation of appropriate technical and organizational measures (Art. 32) and the duty of notification of a personal breach to the supervisory authority (Art. 33) and to the data subject (Art. 34). These duties are explicitly legislated by the GDPR and even academia is open to recognize their potential to generate IP and unfair competition impacts along with possible serious issues for SMEs. These concerns were projected in the three hypotheses, which were tested in the light of the direct inquiry, namely a questionnaire search of a micro-sample of Czech business Ltds SMEs. Although feedback provided by this micro-sample is statistically insignificant, it provides some interesting and so far not reported data and indices.

Generally, the respondents did not seem overly frustrated or afraid of the GDPR. Instead, they provided a prima facia impression of welcoming the GDPR and making ahead of time all necessary adjustments. However, a deeper study of provided feedback, especially to open-questions, darkens this sunny picture. First, basically all respondents, except IT firms, need to, or decided to, outsource in a significant manner and their replies included strong statements such as "we have to outsource a great deal of our GDPR duties, including the data protection officer job" or "we hire an IT firm for all of that and use an external data protection guy." Businesses purchase not only IP licenses, but in addition hire an IT firm for a fixed monthly fee. The liability shifting is obvious and the genuine effectiveness and efficiency of such an approach is questionable. Second, almost all respondents made an introductory expense of about CZK 100 000 to purchase or to update instruments and tools for the coming GDPR. These costs are introductory and need to be assessed in the light of related fees to be paid as well, such as a monthly fixed fee to be paid for outsourcing, license fees, updating expenses, etc. The GDPR protection and consumer-friendliness do not come for free, i.e. businesses need to spend significant amounts and this may translate into a rise in prices charged to consumers. Third, and perhaps more surprisingly, businesses state they are getting ready but they do not test it, i.e. they do not perform the penetration test. For what do they

IV: *Questionnaire with replies provided by the 4th respondent*

Questions	Answers
1. Your business field?	Providing IT services.
2. Administration of your IS/IT	By ourselves.
3. Protection before the GDPR	Instruments created by employees or obtained based on license agreement (e.g., antivirus programs) from 3rd parties.
4. Protection due to the GDPR	Nothing new, existing is sufficient.
5. Introductory costs of the new protection	Almost nil, just some administration costs.
6. Brand new protection measure	Nothing.
7. Performed penetration test.	Yes, all worked out, no changes needed.
8. Exchange of information about …	Yes, we communicate + provide training.
9. Do you expect unfair competition impact of the GDPR?	No, but businesses underestimate penetration tests, risking a third party will intentionally interfere with their networks with unfair competition consequences.

Source: Prepared by authors based on their micro pilot case study investigation performed in 1/2018.

V: *Questionnaire with replies provided by the 5th respondent*

Questions	Answers
1. Your business field?	Real Estate services.
2. Administration of your IS/IT	Outsourced to an external IT firm for a fixed monthly fee.
3. Protection before the GDPR	Bought high quality antivirus program.
4. Protection due to the GDPR	Employees training, security monitoring, enhanced IP licenses, antivirus program.
5. Introductory costs of the new protection	CZK 68 000.
6. Brand new protection measure	No, but waiting for information and methodology from the CDPO.
7. Performed penetration test.	Not yet.
8. Exchange of information about …	Not yet.
9. Do you expect unfair competition impact of the GDPR?	Generally not, but afraid that (alleged) security incidents might be reported by a third party (competitor) to the CDPO.

Source: Prepared by authors based on their micro pilot case study investigation performed in 1/2018.

wait, if they are allegedly ready? Why don't they test how good their IS/IT is? Why don't they want to find problems and fix them before the GDPR takes effect and incidents to be reported happen? Fourth, businesses do not share information and manifestly a big asymmetry of information dominates the current market. Fifth, the unfair competition impact of the GDPR in general is perceived as insignificant. The issue of reporting of security incidents to the supervisory authority, to the CDPO, is a concern for the businesses and almost all detect in it a serious unfair competition potential. Highly interestingly, they do not fear so much that businesses will not implement the measures or not report the incidents, rather they truly are afraid of alleged incidents and related blackmail and false reports by third parties. They are afraid that their competitors will "make up" stories about security incidents and will use these lies as a tool for blackmail, denigration or even a punishment by the GDPR sanctions. Further, under certain conditions, even the disposition with personal data in a breach of the GDPR can be considered to be a security incident. Even natural persons can inform controlling authorities that they suffered damage or that there was a breach of the GDPR by a business. This creates another option for unfair competition practices between businesses. These real concerns have not been discussed by the EU, European Commission and academia and the GDPR does not offer any protection or advice about it. In sum, the stated hypotheses were only partially confirmed. The GDPR duty to implement appropriate technical and organizational measures to ensure a level of security to protect natural persons with regard to the processing of personal data (Art. 32) will have an impact on the IP (H1) and unfair competition (H2). However, based on the completed micro-case study in combination with published academic opinion, it might be suggested that this impact will NOT be significant. This ultimately will lead to a challenge for SMEs, but although this challenge is at least cost-wise not nominal, still businesses state that it is NOT serious, except for the burning issues of the speculations linked to alleged security incidents and their reporting (H3). It will be highly interesting to observe what really happens from May, 2018 and how businesses will perceive it, and how they will adjust to it.

CONCLUSION

The GDPR applies from May 2018 in the EU, including the Czech Republic. Hence even Czech businesses have to implement appropriate technical and organizational measures to ensure a level of security (Art. 32) to protect natural persons with regard to the processing of personal data (Art. 1) and to give notice about personal breaches both to the supervisory authority (Art. 33) and to the data subject (Art. 34). Three hypotheses were set and legislative and academic analysis was confronted by the practical investigation part with questionnaires. Interestingly, only a partial confirmation was achieved.

Although the yielded results are especially due to the micro-case study nature rather indicative than generally conclusive, they allow to suggest a partial confirmation of the proposed hypotheses that this GDPR duty will have a significant impact on IP and unfair competition. Namely, based on the Czech pioneering micro-case study, which should definitely by expanded in the future, the GDPR duty to place appropriate technical and organizational measures to ensure a level of security to protect natural persons in re to processing personal data (Art. 32) will have an impact on the IP (H1) and unfair competition (H2), but this impact arguably appears NOT significant and the SMEs perceive it as a challenge, which is not serious despite more than nominal costs (H3). Namely, it seems that the Czech SMEs are inclined to "outsource" their GDPR duties and say they are ready, but without truly testing it, i.e. not performing the penetration test. They indicate the significance and impact of the "measures duty" as neither significant nor serious, but they spend a significant amount of money for this purpose and they have serious concerns about abuses. These abuses are not about black sheep that are not implementing the GDPR, but instead about competitors trying to portray them as black sheep. Manifestly, we have here an asymmetry of information and perceptions and it will be extremely interesting to observe the results from May 2018, how these and other businesses will perceive it, and how they will adjust to it.

Acknowledgements

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

REFERENCES

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

VAN DER AUWERMEULEN, B. 2017. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law & Security Review*, 33: 57–72.

AZOLAI, L. 2011. *The Force and Forms of European Legal Integration*. EUI Working Papers, 2011/6. Florence: European University Institute.
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.
BALCERZAK, A.P. 2015. Europe 2020 Strategy and Structural Diversity Between Old and New Member States. Application of Zero Unitarization Method for Dynamic Analysis in the Years 2004–2013. *Economics & Sociology,* 8(2), 190–210.
CHIRITA, A.D. 2014. A legal-historical review of the EU competition rules. *International and comparative law quarterly*, 63 (2): 281–316.
CVIK, E. and 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
DAMRO, C. 2012. Market power Europe. *Journal of European Public Policy*, 19(5): 682–699.
EUROPEAN COMMISSION. 2017. Reform of EU data protection rules. *European Commission*. [Online]. Available at : http://ec.europa.eu/justice/data-protection/reform/index_en.htm [Accessed: 2018, August 15].
HORVÁTH, P., PÜTTER, J. M., DAGILIENĖ, L. *et al.* 2017. Status quo and future development of sustainability reporting in Central and Eastern Europe. *Journal of East European management studies (JEEMS)*, 22(2): 221–243.
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.
JINDŘICHOVSKÁ, I. and KUBÍČKOVÁ, D. 2017. The Role and Current Status of IFRS in the Completion of National Accounting Rules – Evidence from the Czech Republic. *Accounting in Europe*, 14(1–2): 56–66.
MACGREGOR PELIKÁNOVÁ, R. 2017. European Myriad of Approaches to Parasitic Commerical Practices. *Oeconomia Copernicana*, 8(2): 167–180.
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.
MACGREGOR PELIKÁNOVÁ, R. 2012. And the best top level domain for European enterprises is... *International And Comparative Law Review*, 12(2): 41–57.
MACGREGOR PELIKÁNOVÁ, R., CÍSAŘOVÁ, J. and 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. *The Lawyer Quarterly,* 7(3): 145–161.
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.
MATEJKA, J. 2013. *Internet jako object práva – Hledání rovnováhy autonomie a soukromí.* Praha: CZ NIC.
NEVIMA, J. and MAJEROVÁ, I. 2015. The Application of two Econometric Models in The ß-Convergence Approach in the Case of Visegrad Four Regions. *Transformations in Business & Economics*, 14(2A): 549–562.
PIEKARCZYK, A. 2016. Contemporary organization and a perspective on integration and development. *Oeconomia Copernicana*, 7(3): 467–483.
PORMEISTER, K. 2017. Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law,* 7(2): 137–146.
RAAB, Ch. And SZEKELY, I. 2017. Data protection authorities and information technology. *Computer Law & Security Review,* 33: 421–433.
SCHLOSSBERGER, O. 2016. Economic and Legal Aspects of Electronic Money. *ACTA VŠFS*, 10(1): 47-65.
SILVERMAN, D. 2013. *Doing Qualitative Research – A Practical Handbook*. 4th Edition. London, UK: SAGE.
STANÍČKOVÁ, M. 2017. Can the implementation of the Europe 2020 Strategy goals be efficient? The challenge for achieving social equality in the European Union. *Equilibrium-Quarterly Journal of Economics and Economic Policy,* 12(3): 383–398.
TANKARD, C. 2016. What the GDPR means for businesses. *Network Security*, 6: 5–8.
TIKKINEN-PIRI, C., ROHUNEN, A. and MARKULA, J. 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1): 134-153.
TUREČKOVÁ, K. 2014. ICT sector in selected countries in Europe. In: *Crafting Global Competitive Economies: 2020 Vision Strategic Planning& Smart Implementation.* Norristown: IBIMA, pp. 1620–1628.
VIVANT, M. 2016. Building a Common Culture IP? *International Revue of Intellectual Property and Competition law*, 47(3), 259–261.
ZERLANG, J. 2017. GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, 6: 8–11.
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.

Contact information

Radka MacGregor Pelikánová: radkamacgregor@yahoo.com
Eva Daniela Cvik: cvikadvokat@gmail.com