# THE GDPR AT THE ORGANIZATIONAL LEVEL: A COMPARATIVE STUDY OF EIGHT EUROPEAN COUNTRIES

***Marek Zanker[1], Vladimír Bureš[2], Anna Cierniak-Emerych[3], Martin Nehéz[4]***

[1] *University of Hradec Králové, Faculty of Informatics and Management, Department of Information Technologies, Czech Republic, ORCID: 0000-0002-2745-4868, marek.zanker@uhk.cz;*
[2] *University of Hradec Králové, Faculty of Informatics and Management, Department of Information Technologies, Czech Republic, ORCID: 0000-0001-7788-7445, vladimir.bures@uhk.cz;*
[3] *Wroclaw University of Economics and Business, Faculty of Business and Management, Department of Labor, Capital and Innovation, Poland, ORCID: 0000-0003-4435-4954, aemerych@wp.pl;*
[4] *Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology, Institute of Information Engineering, Automation, and Mathematics, Slovakia, martin.nehez@stuba.sk.*

***Abstract:*** *The General Data Protection Regulation, also known as the 'gold standard' or the 'Magna Carta' of cyber laws, is a European regulation that deals with rights in the area of privacy and focuses on data collection, storage and data processing. This manuscript presents the results of investigation in the business sphere from eight countries of the European Union. The research focused on awareness of the GDPR, costs associated with the GDPR, number of trainings, how data are secured and subjective evaluation. The questionnaire was used for data collection. The results show that the majority of employees concerned about the GDPR are able to define the GDPR correctly (64%). The correct identification of personal data is in 95% of cases. The vast majority of respondents (94%) assign the right to personal data protection to the GDPR. Most employees are trained in the GDPR once (46%) or twice (45%). Subsequently, the differences between these countries in some areas of the questionnaire survey were examined. For this purpose, Welch ANOVA with post-test Tukey HSD or Kruskal-Wallis test were used. As a result, knowledge about the personal data do not vary significantly between the countries. In the area of rights, the countries are not again statistically different. As for the number of security countries, statistics do not differ significantly. The subjective assessment of the GDPR is different across the countries. The GDPR is rated worst by companies in the Czech Republic and Slovakia. On the contrary, the GDPR is best perceived by companies in France and the United Kingdom.*

***Keywords:*** *General Data Protection Regulation, European countries, personal data, security, privacy, individual rights.*

***JEL Classification:*** *K22, K42.*

***APA Style Citation:*** Zanker, M., Bureš, V., Cierniak-Emerych, A., & Nehéz, M. (2021). The GDPR at the Organizational Level: A Comparative Study of Eight European Countries. *E&M Economics and Management, 24*(2), 207–222. https://doi.org/10.15240/tul/001/2021-2-013

## Introduction

Individuals and corporations alike are aware of the need for data protection. They undergo training and perform exercises where various types data-jeopardizing techniques or cyberattacks are simulated in order to increase the resilience of society and preparedness for crisis situations (National Cyber and Information Security Agency, 2019a).

With the help of the General Data Protection Regulation (GDPR), the European Commission (EC) seeks to draw a line between the personal data security and the free and uncontrolled manipulation of personal data (IT Governance

Privacy Team, 2020). Since its advent, the GDPR has put burden on the shoulders of various institutions which have been struggling to share data. Not surprisingly, it brought a flare-up of frustration (Bovenberg et al., 2020). The intension was good, as the GDPR would ensure and balance the fragile relationship between the data protection and other regulations, such as competition law, consumer protection or intellectual property (De Hert et al., 2018).

The GDPR was introduced in 2018, and it has been regulating the processing by an individual, a company or an organization of the personal data related to individuals in the European Union (EU) since (European Commission, 2019). Citizens have the following rights: 1) Right of access by the data subject; 2) Right to rectification; 3) Right to erasure; 4) Right to restriction of processing; 5) Right to data portability; 6) Right to object (Radley-Gardner et al., 2016). Based on these rights, obligations arise for data processors, such as: 1) The obligation of appointment and Data Protection Officer; 2) Data protection by design and default; 3) Providing proper notification in the case of a data breach (European Commission, 2018).

The view of the GDPR can be divided into two main directions, one from the perspective of customers and one from the point of view of companies. For example, in Norway, companies were contacted with a request for access to data and a request for data transfer (Sørum & Presthus, 2020). They were able to execute these requests and meet set deadlines. However, it was clear from the companies' activities that they did not distinguish between the two requirements. Presthus and Sørum (2018) conducted a survey on knowledge of users' rights related to the GDPR, which revealed that 21% of customers had never heard of the GDPR. However, among respondents who had some idea about the GDPR, the GDPR was generally perceived in a positive way. Nevertheless, they were very skeptical about the implementation in reality at the same time.

The implementation of the GDPR is a big test, especially for small and medium-sized enterprises. Härting et al. (2020) state that access to know-how, the ability to pay the costs associated with the implementation of the GDPR, access to information and the correct adaptation of processes are key to the implementation of the GDPR requirements for small and medium-sized enterprises. Brodin (2019) claims that the input audit represents the main building block for companies, which reveals what, how and to what extent the data are processed. Furthermore, from the point of view of companies, sanctions are important, where fines result from non-compliance with the personal data protection and are set at EUR 20 million or up to 4% of annual total income (European Union, 2016).

According to Gal and Aviv (2020), the GDPR creates two main harmful effects on competition and innovation: from the point of view of competition, it entrenches the market power of those who are already strong; from the point of view of innovation, the GDPR may prevent some data synergies. Another impact of the GDPR in research and innovation was noted by Peloquin et al. (2020), who stated that the GDPR has a negative impact on secondary research uses of data and associated biospecimens.

For some non-European companies, the introduction of the GDPR has meant some reduction in their activities in the EU market. For example, YouTube stopped using third-party advertising services to book purchases after the introduction of the GDPR (Tambou, 2019). Facebook also experienced issues due to non-compliance with the GDPR (Kasse et al., 2018). Li et al. (2019) state that legal proceedings have been initiated against Facebook and Google for 'forced consent'. As the GDPR has the extraterritorial scope, huge fines for companies outside of Europe can be imposed as a consequence. That is why similar acts or countermeasures were created. For instance, California passed its own Consumer Privacy Act, echoing some of the provisions of the GDPR in June 2018 (Gregory Voss & Houser, 2019).

The main motivation for developing this study is associated with the following research gap. Numerous official or academic reports are currently published to figure out the current state of the GDPR implementation after two years (Lachaud, 2020). Issues and weak points of this regulatory effort have been highlighted and explained by recent studies in the ethical, socio-political, legal and policy domains (Marelli et al., 2020). As far as our knowledge extends, there are a few studies directly comparing situations in several countries, including

representatives from the East and the West, as well as both small and big nations. Mostly, studies focusing on the situation in a specific country are published (Tahal & Formánek, 2020; Zahariev & Makshutova, 2020; Sajfert, 2020; Mitrou, 2020; Korpisaari, 2019). Therefore, this paper presents a follow-up of the publications cited in the text, with the aim of expanding the current knowledge about the situation two and a half years after the implementation of the regulation on an international scale and identifying weaknesses and strong points in the implementation of the GDPR in the selected countries. The main objective of this research is to answer two questions, specifically, what the awareness of companies about the GDPR is and what the current state of its implementation is.

The remaining text of this manuscript is structured as follows: The following section presents selected topics associated with the GDPR which are important for this study. Consequently, the applied methodology is described. The next section presents the outcomes of the questionnaire survey and statistical processing of the results. The following section is devoted to the discussion. The last section concludes the paper and offers suggestions for further research and its implementation.

## 1. Theoretical Background

The GDPR can currently be considered the most progressive breakthrough system to implement control mechanisms and regulations on such a large scale (Tchinaryan et al., 2019) and is considered to be the most important innovation in the general EU Data Protection Regulation (De Hert et al., 2018). The regulation applies to all legal persons who do business in the EU or handle the personal data of EU individuals, regardless of where the registered office is located (O'Brien, 2016). However, the GDPR enables a little bit of freedom in the field of automated decision-making, specifically in Article 22. It sets out the measures that should be applied by member states (Malgieri, 2019). Four different approaches to automated decision-making have been identified in national laws implementing the GDPR (Malgieri, 2019):

a) Negative approach – the member state does not allow any specific case of authorized automated decision-making and is applied by most countries (e.g. Italy, Romania, Sweden, Denmark, Poland, Finland, Cyprus, Greece, the Czech Republic, Estonia, Lithuania);
b) Neutral approach – the member state has implemented Article 22 but has not specified any specific measures to protect the rights and freedoms and legitimate interests of the data subjects (e.g. Germany, partly Austria and Belgium);
c) Procedural approach – the member state provides the guarantees referred to in Article 22, which are based in particular on the specific procedures to be followed and followed by the data controllers, such as data examination notifications (e.g. Ireland, the United Kingdom, partly Slovenia);
d) Proactive approach – the member state proposes new specific guarantees in accordance with Article 22 (e.g. France, Hungary).

Despite the sanctions, surveys show that companies do not comply with the GDPR. According to Forrester Research, 80% of companies in Europe and North America did not comply with the GDPR as of May 25, 2018 (Duncan & Zhao, 2018). In 2019, a survey conducted by the EU highlighted the fact that more than half of the 716 small businesses surveyed did not have the knowledge to use the right tools and did not follow the key rules of the GDPR (GDPR.eu, 2019d). In February 2019, Cisco presented the results of a survey which showed that 59% of companies meet the GDPR requirements, 29% expect security during the year and 3% are unable to meet the GDPR requirements at all. Spain appeared to be the most prepared country, while the least prepared countries were Japan, Russia and Turkey (Cisco, 2019). KPMG, a consulting company, came to similar conclusions, presenting at the GDPR conference the results of a survey conducted among 52 major Czech companies and revealing 76 violations. The most common errors detected included incorrectly defined ranges of data that companies process, missing definition of the purpose of data processing, but also the method of obtaining consent from individuals (Vejvodová & Rosůlková, 2019). The monitoring of website visitors and the use of cookies represent another identified violation of the rules. The least number of violations was found in institutions, such as banks and insurance companies, the most, on the contrary, in sports organizations (Vejvodová & Rosůlková, 2019). In the first eight months

after the introduction of the GDPR, a total of 59,430 personal data breaches were reported to the European authorities. Most cases, a total of 15,400, were reported in the Netherlands, the least in Iceland and Estonia, only 25 cases (Vejvodová & Rosůlková, 2019).

Violations are subject to heavy sanctions (European Union, 2016). To date, the highest fine has been imposed on Facebook for breaches of privacy by the US Federal Trade Commission (FTC) (Czech News Agency & iDNES.cz, 2019). Another record fine was imposed by the French CNIL office of the American company, Google, for misinforming users about how their data are used (Vejvodová & Rosůlková, 2019). In Portugal, the hospital in Barreiro received a fine for providing data on patients to unauthorized persons (Vejvodová & Rosůlková, 2019). The Danish taxi service was fined for failing to anonymize or delete its customers' data (GDPR.eu, 2019a).

It is also important to mention the 'privacy paradox' here. On the one hand, legal persons are forced to take measures to protect the personal data of natural persons. At the same time, these natural persons voluntarily share their data and give their headless consent without properly reading the conditions (Botta & Wiedemann, 2019). The reason is simple, reluctance to read extensive texts. According to a European Commission survey from 2015, it was found that only 18% read the conditions, 31% did not read them at all and 49% only partially (Botta & Wiedemann, 2019). Notwithstanding this, companies must comply with their obligations under the GDPR. Modification or introduction of new company processes or audit of the current state is always a burning task for companies, which requires time, knowledge and finances. Small businesses have invested € 1,000–50,000 in technology and consulting services, yet are unsure whether they are in line with the GDPR (GDPR.eu, 2019d). A checklist available on the GDPR.eu website (GDPR.eu, 2019a) can help to identify possible shortcomings. The list is divided into four basic blocks, each of which contains several specific sub-points defining more detailed parameters (GDPR.eu, 2019b):

1. Adherence to the legal framework and transparency;
2. Data security;
3. Accountability and governance;
4. The right to privacy.

At the same time, services based on end-to-end encryption or other personal data security features are often recommended, for which Switzerland, i.e., a neutral territory outside the EU, is often the cradle of origin (GDPR.eu, 2019c). In addition, some providers also offer special features to meet the GDPR, such as Matomo's anonymization (GDPR.eu, 2019c). The recommended providers for individual services are as follows (GDPR.eu, 2019c):

- E-mail communication: ProtonMail, Hushmail, Tutanota, Mailfance;
- VPN: ProtonVPN, AirVPN;
- Analyzes: Open Web Analytics, Matomo;
- Messaging: Signal, WhatsApp, Threema;
- Cloud storage: Tresorit, Sync.com, Boxcryptor;
- Teamwork tool: Wire;
- Annotation tool: Standard Notes, Joplin.

Although public authorities support the correct application of the GDPR by practical examples, model documents and guidelines (National Cyber and Information Security Agency, 2019b), its interpretation is still incomprehensible to companies (Brodin, 2019).

## 2. Research Methodology

### 2.1 Survey

Based on relevant transnational resources (e.g., European Commission, 2020a; European Union, 2016) or national resources (e.g., National Cyber and Information Security Agency, 2019a), we compiled a questionnaire with four sets of questions consisting of a total of 31 questions. The questionnaire was then translated into several world languages (English, French, Bulgarian, Polish, Spanish, German). The questionnaire was designed in a way providing anonymous access and answers while giving respondents support to answer truthfully and comfortably at the same time (Gideon, 2012). The questionnaire was constructed to be as simple and comprehensible as possible. A limited number of response scales were used, i.e., short open answers, dichotomous yes/no and scale rating (Likert's scale). The questionnaires underwent a pilot testing, performed by ten people out of the research group before sending to respondents. The questionnaire was placed in the SURVIO web application (https://www.survio.com/). Using convenience sampling methods, the link to the questionnaire together with basic information was sent by email to representatives of companies in the following countries: Great

Britain (GB), France (F), Bulgaria (BG), Poland (PL), Spain (SP), Germany (DE), Slovakia (SK) and the Czech Republic (CZ). The aim was to obtain respondents equally from the EU-15 countries and from Central and East European countries as the latter demonstrate specifics in the business sector (Svobodová & Hedvičáková, 2015). Consequently, the judgment and snowball sampling methods were used for extension of the sample size. This sampling methods enabled to direct questionnaires at competent employees responsible to the GDPR tasks in particular companies. These individuals were at various levels of seniority or working positions according to their attitude to the GDPR issues in a company, ranging from members of the executive boards to regular employees at the operational level.

The cornerstone of the comparative study was to obtain at least 30 respondents from each country. Out of the total number of 2,456 addressed persons, 603 people opened the questionnaire, of which 307 people completed the submitted questionnaire. Responses were collected during spring of 2020. The basic characteristics of the sample are given in Tab. 1. Only variables Country and Size are statistically analyzed. The variable Industry offers examples of the domains in which companies operates. Due to the uneven distribution with an insufficient size of the sample in some domains, statistical analysis cannot be executed.

## 2.2 Statistical Processing

The results of the questionnaire survey were processed using the Statistical Package for the Social Sciences (SPSS) software in version 26 (IBM, 2020). After obtaining a basic overview, a statistical hypothesis about the equality of the average across companies from individual states for individual types of questions was made. The methodological procedure from IBM SPSS for tests on the similarity of averages was used for the calculations. For Analysis of Variance (ANOVA), it is necessary to meet three basic assumptions: independent observations, normality and homogeneity (SPSS, 2020). The first assumption was met on the basis of data acquisition, i.e., the replies of one company were not conditioned by the replies of another company. Subsequently, homogeneity was tested using the Levene's test. In the case of ordinal data, the Kruskal-Wallis test was used instead of ANOVA, which can be used for ordinal values according to SPSS (2020).

# 3. Research Results

## 3.1 Main Findings

The survey showed that 64.16% (197) of respondents were able to provide a general definition of the GDPR. We asked the respondents about whether certain personal data falls under the protection of the GDPR. The questions were divided into personal data of natural and legal persons. Questions about individuals included first and last name, health, biometrics, camera footage, photographs and sexual orientation, with the percentage of correct answers being 98.04%, 97.72%, 97.72%, 93.48%, 94.46% and 85.34%, respectively. Regarding the data of legal entities, questions were asked focusing on the basic data about the company (ID number, account number and company address), business telephone number, company turnover and annual reports, with the percentage of correct answers being 94.46%, 96.74%, 97.39% and 98.04%, respectively.

Four questions were focused on the area of individual rights: the right to personal data protection, the right to request recorded data, the right to delete personal data and the right to

**Tab. 1: Profile of respondents**

| Indicator | Result |
|---|---|
| Country | BG 9.77% (30); CZ 23.45% (72); DE 10.42% (32); F 11.07% (34); GB 11.73% (36), PL 10.75% (33); SK 12.38% (38); SP 10.42% (32) |
| Size | Micro 11.07% (34); Small 37.13% (114); Medium 32.89% (101); Large 18.89% (58) |
| Industry | Construction, Retail, Education, Financial services, Public administration, Health care, Tourism, Armed forces, Culture, Social services, Logistics and transportation, Estate agency, Food processing |

Source: own

refuse the processing of personal data, with the percentage of correct answers being 94.46%, 50.81%, 58.95% and 64.49%, respectively.

The mode and median number of trainings is equal to one. In total, the respondents stated that employees underwent one training in 140 cases, two or more trainings in 138 cases and none in 29 cases.

The biometric fingerprint security is used by 66.12% of respondents. The use of a numerical code was mentioned by 45.28% of respondents. The graphic character security is used by 28.66% of respondents. Only three respondents stated that none of these types of security had been used.

One third of respondents stated that they did not know what costs the company had spent on the GDPR. The highest frequency is shown by two cost intervals. The first interval is € 1,000–9,999 (69), with e-shops (23), construction companies (21) and industry (11) showing the highest frequencies. The second interval of € 10,000–49,999 (65) has the highest frequency in the construction industry (35). The interval € 1–999 (32) has the highest frequency reported in e-shops (14). Costs in the amount of € 50,000–99,999 (25) were most often reported by construction companies (17), and more than € 100,000 (3) were reported most by industrial companies. Apparently, there are differences even in one type of industry, as we can see on the case of construction industry.

One set of questions focused on the perception of a change in the security of personal data after the introduction of the GDPR. Subjective ratings were used on a scale from 1 to 5, where 1 means worst and 5 means best. In case of the perception of electronic data security, the median was 4, and the mode was 5, which means that overall, the security of electronic data after the introduction of the GDPR is evaluated positively. Similarly, the perception of the security of printed data after the introduction of GDPR had a high value for both median and modus (4 for both indicators). Hence, the security of printed data is perceived positively as well.

The set of questions focused on subjective evaluation of the GDPR applied the scale from 1 to 5, where 1 meant completely disagree, 2 – rather disagree, 3 – status did not change, 4 – rather agree, 5 – agree. The first question focused on the increase in administration after the introduction of the GDPR, and the second question focused on the functionality of the GDPR as an indicator of potential threats. Both questions acquired values of median and modus 4 and 5, and 4 and 4, respectively. Thus, we can presume that the surveyed sample perceives an increase in administration after the introduction of the GDPR, and it is considered as a good indicator of potential threats.

The third question and the fourth were fundamentally different from the others because the respondents were not in a role of a company representative, but they answered for themselves as individuals. The third question was focused on the control of personal data, and the fourth question was focused on the sense of security in relation to the personal data and the GDPR. The median and modus of their answers were 3 and 4, and 3 and 4, respectively. One can conclude that the implementation of the GDPR for respondents did not significantly increase the sense of security in the area of personal data.

## 3.2 Country and the Company Size

The results of statistical testing are presented in Tabs. 2–5. The main hypothesis is set out as follows: the answers of companies to individual areas of questions do not differ based on the country of origin. Hence, an alternative hypothesis claims that for at least one group, the average answers to at least one group of questions differ. The main hypothesis was divided into partial hypotheses according to the four thematic areas in the questionnaire: Personal Data, Law, Type of Security and Subjective Perception of the GDPR.

The first assumption (independent observations) was fulfilled by data acquisition. According to the SPSS methodology, there is no need to test normality if all samples are larger than 25. The last assumption will be tested for each group of questions separately.

Tab. 2 presents the result of the homogeneity test for the division of companies by country. Based on the result for the average for personal data ($p < 0.001$), rights ($p < 0.001$), and security ($p = 0.013$), it can be concluded that the values across the groups are not homogeneous. Therefore, the method for inhomogeneous groups has to be used to evaluate the difference between the groups. Tab. 3 shows the results of the Welch test ANOVA. Based on the results for personal data ($p = 0.077$), rights ($p = 0.418$), and security ($p = 0.052$), it can be stated that

**Tab. 2: Test of the homogeneity of variances (countries)**

| | Levene statistic | | | df2 | | | Sig. | | |
|---|---|---|---|---|---|---|---|---|---|
| Based on | Personal data | Rights | Security | Personal data | Rights | Security | Personal data | Rights | Security |
| Mean | 6.499 | 4.271 | 2.587 | 299 | 299 | 299 | 0.000 | 0.000 | 0.013 |
| Median | 1.913 | 2.227 | 0.841 | 299 | 299 | 299 | 0.067 | 0.032 | 0.554 |
| Median with adjusted df | 1.913 | 2.227 | 0.841 | 183.943 | 209.952 | 277.619 | 0.070 | 0.033 | 0.554 |
| Trimmed mean | 5.016 | 4.140 | 2.219 | 299 | 299 | 299 | 0.000 | 0.000 | 0.033 |

Source: own

Note: df1 excluded from the table (= 7).

**Tab. 3: ANOVA (countries)**

| | | Between groups | Within groups | Total | Welch test |
|---|---|---|---|---|---|
| Sum of squares | Personal data | 9.875 | 220.516 | 230.391 | |
| | Rights | 12.786 | 502.432 | 515.218 | |
| | Security | 4.514 | 109.206 | 113.720 | |
| df | Personal data | 7 | 299 | 306 | |
| | Rights | 7 | 299 | 306 | |
| | Security | 7 | 299 | 306 | |
| Mean square | Personal data | 1.411 | 0.738 | | |
| | Rights | 1.827 | 1.680 | | |
| | Security | 0.645 | 0.365 | | |
| F | Personal data | 1.913 | | | |
| | Rights | 1.087 | | | |
| | Security | 1.766 | | | |
| Sig. | Personal data | 0.067 | | | 0.077 |
| | Rights | 0.371 | | | 0.418 |
| | Security | 0.094 | | | 0.052 |

Source: own

there is no statistically significant difference between the groups. Personal data, rights and security are not treated differently in individual countries.

Tab. 4 reveals the result of the homogeneity test for the division of companies by the company size. Based on the result for the average for the definition of the GDPR ($p = 0.002$), personal data ($p = 0.002$), rights ($p = 0.009$), and security ($p = 0.014$), it can be stated that the values across the groups are not homogeneous. Therefore, the Welch test ANOVA method for inhomogeneous groups has to be used again to evaluate the difference between the groups (see Tab. 5). Based on the results for definition ($p = 0.003$), personal data ($p = 0.173$), rights ($p = 0.003$), and security ($p = 0.174$), it can be concluded that there is no statistically significant difference between the groups for personal data and security. However,

**Tab. 4: Test of the homogeneity of variances (company size)**

| | | Based on mean | Based on median | Based on median and with adjusted df | Based on trimmed mean |
|---|---|---|---|---|---|
| Levene statistic | Definition | 4.946 | 1.348 | 1.348 | 4.946 |
| | Personal data | 5.659 | 2.455 | 2.455 | 4.965 |
| | Rights | 3.893 | 1.720 | 1.720 | 3.917 |
| | Security | 4.337 | 1.327 | 1.327 | 3.598 |
| df2 | Definition | 303 | 303 | 300.799 | 303 |
| | Personal data | 303 | 303 | 223.389 | 303 |
| | Rights | 303 | 303 | 216.412 | 303 |
| | Security | 303 | 303 | 291.728 | 303 |
| Sig. | Definition | 0.002 | 0.259 | 0.259 | 0.002 |
| | Personal data | 0.001 | 0.063 | 0.064 | 0.002 |
| | Rights | 0.009 | 0.163 | 0.164 | 0.009 |
| | Security | 0.005 | 0.266 | 0.266 | 0.014 |

Source: own

Note: df1 excluded from the table (= 3).

**Tab. 5: ANOVA (company size)**

| | | Between groups | Within groups | Total | Welch test |
|---|---|---|---|---|---|
| Sum of squares | Definition | 3.372 | 67.214 | 70.586 | |
| | Personal data | 5.466 | 224.925 | 230.391 | |
| | Rights | 23.939 | 491.279 | 515.218 | |
| | Security | 1.478 | 112.242 | 113.720 | |
| df | Definition | 3 | 303 | 306 | |
| | Personal data | 3 | 303 | 306 | |
| | Rights | 3 | 303 | 306 | |
| | Security | 3 | 303 | 306 | |
| Mean square | Definition | 1.124 | 0.222 | | |
| | Personal data | 1.822 | 0.742 | | |
| | Rights | 7.980 | 1.621 | | |
| | Security | 0.493 | 0.370 | | |
| F | Definition | 5.068 | | | |
| | Personal data | 2.455 | | | |
| | Rights | 4.921 | | | |
| | Security | 1.330 | | | |
| Sig. | Definition | 0.002 | | | 0.003 |
| | Personal data | 0.063 | | | 0.173 |
| | Rights | 0.002 | | | 0.003 |
| | Security | 0.265 | | | 0.174 |

Source: own

for the definition of the GDPR and rights, there is a statistically significant difference between the groups. Personal data and security are not treated differently between the companies based on size. On the other hand, differences exist in case of the definition of the GDPR and rights.

**Personal Data**

Here, respondents were expected to have the same average GDPR-protected personal data scores across the countries. First, the assumption of homogeneity had to be verified, which was tested using the Levene's test. According to the SPSS methodology, the data must meet two assumptions, specifically, independence and the data must be quantitative. Both of these assumptions are fulfilled.

The result of the Levene's test revealed that the data were not homogeneous, therefore the Welch ANOVA test was used. Based on the results, it can be stated that the zero hypothesis is not rejected, i.e., the averages of the responses do not vary across countries.

**Rights**

The assumption of homogeneity was tested using the Levene's test again, and homogeneity was rejected. Based on the previous test results, the difference in averages was tested using the Welch ANOVA, where the hypothesis of the equality of the average success is not rejected ($p = 0.418$).

**The Number of Security Measures Used**

The assumption of homogeneity was tested using the Levene's test, and the hypothesis of homogeneity is rejected ($p = 0.013$). Based on the previous test, the Welch ANOVA was performed, and the hypothesis of the same number of security measures can be confirmed ($p = 0.052$). It can be assumed that there is no difference across the countries in the way that companies secure data.

**Subjective Evaluation of the GDPR**

Due to the ordinal nature of these data, the Kruskal-Wallis test was used. The result of the test reveals that the hypothesis of differences in the perception of the GDPR is rejected ($p < 0.001$). The results show that the GDPR is subjectively perceived most negatively in the Czech Republic and Slovakia, while it is perceived most positively in France and Great Britain.

## 4. Discussion

This section further elaborates and discusses achieved results enriched by the analysis of additional variables. The GDPR influences processes and activities of companies in all investigated industrial segments. Out of the investigated sample, various research domains, such as biomedicine, geographical research or healthcare can serve as examples (Meijering et al., 2020; Donnelly & McDonagh, 2019). For instance, The Court of Justice of the European Union strengthened barriers to transfer and share data, enabling more effective and efficient research of COVID-19 (Bovenberg et al., 2020). Related to research activities, the issue of personal data protection is very important not only from the perspective of enterprises, but also other types of institutions, such as universities. The practice of processing personal data at universities shows that the problem areas for data protection are primarily associated with the recruitment process, publishing exam results, information about the authors of diploma theses, or rankings of the best students. Moreover, universities monitor graduates' careers. Therefore, appropriate documents had to be created to enable obtaining consent from candidates for studies, students and graduates to process their data for the above-mentioned purposes. Similar to the business sector, universities need to appoint a personal data administrator. The basic tasks of the administrator are accounting for compliance with the rules of personal data protection, fulfilling the requests of data subjects, assessing the effects of data processing, or recording data processing activities.

Under some market conditions, the GDPR has unintended and so far, unrecognized effects on competition, efficiency, innovation, and the resultant welfare (Gal & Aviv, 2020). Puljak et al. (2020) found out that there was a dramatic increase in the number of requests to the national GDPR authority in Croatia when the pre- and post-GDPR periods are compared. Furthermore, the GDPR imposes much greater demands on companies to address the rights of individuals who provide data, that is, the Data Subjects (Breen et al., 2020). It can be considered as both the proof that and explanation why companies invest energy, time, financial and other resources heavily in the GDPR implementation. Nevertheless, a third of the respondents in our study stated that they did

not know the amount of the GDPR investment their employer had to make. The remaining two thirds showed the highest frequencies in cost intervals, in the thousands or tens of thousands of Euro (35% and 33% respectively). This finding is in line with the GDPR Survey of May 2019, which states that companies invested the most in the range of € 1,000–9,999 and € 10,000–49,999 (27% and 24% respectively) (GDPR.eu, 2019d). The costs invested are related, for example, to the establishment of a trustee position, which is held by 64% of respondents, although the GDPR legislation imposes this obligation on only 10% of the sample. A similar situation is with the processing of the record of activities, which is mandatory for 18.9% of respondents only. However, the document has been processed by 81.4% of the sample. The factual questions focused on who is protected by the GDPR and who has to follow its rules were answered correctly by 64.17% of respondents.

Inconsistency between the structure of the regulation and the way in which technologies actually operate is an interesting and meaningful topic to investigate (Tatar et al., 2020). Social media platforms, online search engines or targeted advertising services are very often associated with data-driven business models grounded in the large-scale collection, analysis, and monetization of personal data (van der Waerdt, 2020). Respondents are not familiar with details related to End-to-End Encryption (E2EE), as 29% of respondents do not know if the company uses E2EE. Nevertheless, they confirm use of the WhatsApp application as a corporate communication tool. The GDPR Survey of May 2019 came to the same conclusion (GDPR.eu, 2019d). From the sample, 19% of subjects use contacts from purchased databases. As stated by the National Cyber and Information Security Agency on its website, it is highly unlikely that the contacts of a database would give such a specific consent, and a general consent covering more than one area cannot be used (National Cyber and Information Security Agency, 2019b). Direct mailing, i.e., the mass distribution of information to customers, uses 65 sampled persons, 29% of whom do not have a link to unsubscribe from the e-mail distribution. On the contrary, the consent to data processing, which 92% of respondents have before the processing, seems to be a well-defined area. This fact is also confirmed by the GDPR Survey, where respondents gave full or partial consent to the statement that the employer always has the consent of a natural person at 82% (GDPR.eu, 2019d).

While the right to personal data protection, which is integrated in the name, 'General Data Protection' was correctly identified by 94.46% of the subjects. However, the accuracy of replies to other rights is significantly lower, as the right to refuse the processing of personal data, the right to delete personal data and the right to request data processed by a legal entity about a natural person were correctly answered by 64.49%, 58.95% and 50.81%, respectively. If the respondents, i.e., the employees of the company, do not know their rights, one can deduce that the company itself does not have a clear awareness of the rights of natural persons. One of the factors influencing the respondents' knowledge is certainly the training of employees in the field of the GDPR. Training should not be a one-time activity, but a repetitive and regular process reflecting the identified risks and threats in the company. According to our findings, 49.6% of the sampled were trained repeatedly and 50.4% only once. Only 9.4% of respondents were not trained. Higher erudition can help employees be aware of the risks in the work process and the ability to draw attention to them and better defend their rights in private life at the same time. Companies try to protect their data responsibly. In particular, they protect electronic data, where out of 5, the average mark is 4.2 points. Companies use, for example, encryption, anonymization and pseudo-anonymization. Nevertheless, the printed data do not have adequate protection, and the average mark shows a value of 3.6 points. This area is particularly sensitive for micro firms, where the average mark is 3, while large firms show a mark of 4.2. The printing of the documents themselves is also a problematic area. A total of 78.83% of the sampled reported protected printing, i.e., printing under a password (37.79%) or a printer with limited access (41.04%). If printing to the printer is unchecked, employees should at least be instructed that the printed document should only be in the printer for as long as necessary to prevent data misuse. On the contrary, companies have secure access to mobile phones and computers. Only 3 respondents stated that access is not secured. Other respondents use

security mainly through biometric data (on average 25 respondents from each country), numeric code and graphic character. Assigning and removing user access is a much more complex process, and in practice, it often proves to be a painful one for the company that is not completely under control. The claim that employees' approaches are completely under control received an average mark of 3.6 points out of a maximum of 5 points.

Based on its survey, the Association of Privacy Professionals (IAPP) reported that out of 550 respondents, a total of 56% did not comply with the GDPR legislation (Eckert, 2019). Cisco reported that 41% of the 3,200 companies in its 2019 report are not in line with the GDPR (Eckert, 2019). Luxatia International (2019) states that currently, 1 in 3 companies is fully compliant with the GDPR. Based on these facts and the results of the questionnaire survey below, it is possible to confirm outcomes of the previous studies as follows:

- 9.4% of the sampled were not trained in the GDPR;
- 3% of the sampled do not have data security or the data is freely accessible;
- 21.17% of the sample reported uncontrolled printing;
- 1% of the sample does not have secure access to a mobile phone or computer;
- 19% of the sampled use contacts from purchased databases;
- 6% of the sampled persons visibly indicate the recipients of the e-mail during mass mailings;
- 29% of the sample did not have a link to the option to unsubscribe from direct mailing in e-mail;
- allocation and withdrawal of access to employees is not completely under control, the average mark is 3.6 points out of a maximum of 5 points.

Most of these mistakes are easy to eliminate, the problem lies in the ignorance of the company that commits them. However, it is also necessary to highlight the approach of companies to the GDPR, where companies are really trying to meet the requirements of the GDPR, as evidenced by the findings:

- 90.6% of the sampled were trained in the GDPR;
- electronic data security was rated by sampling with a mark of 4.2 out of a maximum of 5 points;
- 81.4% of the sampled have a processed record of activities, therefore they are aware of the data manipulation and potential risks;
- 78.83% of the sample have protected print documents;
- 99% of the respondents stated that they had access to a computer and a mobile phone;
- 37.46% of the sampled have encrypted data on a mobile phone or computer;
- samples use E2EE, anonymization, pseudoanonymization of data;
- sampling using reliable and proven tools and providers of VPN, communication or collaboration tools.

The analysis of data with the country as the selection criterion revealed that the data of the created pairs were undoubtedly interesting but different. It also showed that each country perceived the evaluated area of the GDPR differently. The value indicates the average ranking of the country in the specified areas. The order of countries is as follows: Poland (2.14), France (2.43), Great Britain (2.43), Germany (3.57), the Czech Republic (4.29), Slovakia (4.43), Spain (4.86) and Bulgaria (5). In conclusion, Poland, France, Great Britain and Germany are the most in line with the GDPR in defined areas. The fact that the GDPR has increased the sense of control over the personal data is most felt by the respondents from Great Britain with an average mark of 3.97 out of a maximum of 5.

The contribution of the GDPR in the area of ensuring safety and protection is felt most by those from the United Kingdom (3.97) and Germany (3.94), while the least by the respondents from Slovakia (2.5) and the Czech Republic (2.74). Sobers (2020) reports that 62% of the United Kingdom customers feel more secure when sharing data after the introduction of the GDPR. These results thus confirm the findings described above.

The last part of the study concerned the subjective perspective on the GDPR by respondents. In this area, it was revealed that respondents' opinions were the same in two points, where their grades of 4 and 5 exceeded 50%: GDPR had increased the administration in employment and the GDPR had pointed out the threats and risks of data leakage and misuse. The increase in administration is evidenced by a score of 4 or 5 in 67% of the respondents, while 7.8% said that the GDPR did not increase their administration. The average grade found

is 3.8 points out of a maximum of 5. The fact that the GDPR pointed out threats and risks of data leakage and misuse was rated with a mark of 4 or 5 by 53.4% of those sampled. The average reported mark is 3.78. The subjects achieved different results in the area of increasing the feeling of control over personal data (49% of respondents stated grades 4 or 5, with average 3.3 points and a negative answer for 11% of respondents) and increasing the feeling of security and protection (again 49% of respondents rated the answer with a grade of 4 or 5, and the average grade is 3.3 points, while a negative answer was provided by 15% of respondents). These results confirm the findings of Luxatia International (2019), which states that 45% of EU citizens are still dissatisfied with the protection of personal data.

The GDPR should not be perceived negatively as a law associated with increased administration. The perception of respondents may be related to the insufficient knowledge of legislation and the effort to have consent to everything rather than to make a mistake. On the contrary, the GDPR was a well-meaning data protection law designed to open companies' eyes and show the ways in which data can be misused. An example of poor presentation and information about the GDPR to the public is the Czech Republic, where this law was associated with the increased administration and resulting obligations for the company from the very beginning. In particular, it was a scarecrow for companies doing business in the field of e-shopping. With the coming months, the GDPR has quietly disappeared from the media, and it is only mentioned in the case of sanctions imposed on companies.

## Conclusion

Smart grids, cities, cars and other consequences of the introduction of technologies, such as the Internet of Things, have brought convenience to our lives; and they have also made it faster. These services are connected with emergence of information asymmetries (Mikulecký et al., 2011). Data-driven companies put together significantly more personal data than customers know or can reasonably oversee. Moreover, these companies reach a level of technical understanding for how this data is processed, which is beyond understandability of single consumers (van de Waerdt, 2020). Therefore, there is a need for more rigorous data protection (Abdulghani et al., 2019). The GDPR, also known as the 'gold standard' or the 'Magna Carta' of cyber laws (Andrew & Baker, 2019; Gal & Aviv, 2020), is undoubtedly the law that has its justification. In fact, there are two perspectives confirmed by this study which bring tension among companies: 1) the main objective emphasizes that processing of personal data ought to serve humankind, however 2) the right to personal data protection cannot principally be absolute and must be managed with respect to its function in society and the balance against other fundamental rights has to be ensured and guaranteed (Bovenberg et al., 2020). Despite the occasional negative attitudes, most of us are aware of the need to protect our privacy, and therefore our data, to have an overview of who manipulates the data and how. By birth, a person enters a spiral of electronic data and leaves behind a digital footprint. It is difficult to imagine that people can have full control over the data related to their lives. Digital footprints have also been used in political campaigns, such as in the 2012 US presidential election (Bach et al., 2019).

The aim of this study was to find answers to the following questions: *What is the awareness of companies about the GDPR and what is the current state of its implementation?* These questions are complex and a certain level of ambiguity can be anticipated. As for the former, there is a relatively high level of awareness of the GDPR. The vast majority of companies' representatives do not have a problem to identify the right to personal data protection. However, there are segments, such as the right to refuse the processing of personal data or delete personal data which almost a half of companies do not cover in their GDPR definition. As for the latter, there are aspects which are almost fully implemented (e.g., secured access to work mobile phones and computers), or weakly implemented (e.g., manipulation with printed materials). Other details related to both questions can be found in the Discussion section. Within this study, mistakes of business entities were found in several areas. Examples include errors in the use of data from purchased databases, missing Identity Data Management, insufficient protection of printed documents or insufficient training of employees. The GDPR brings protection to all data, and it must be reiterated that companies have well-secured electronic data, but printed data are neglected. The

research is based on clear recommendations. Companies must regularly train employees in the GDPR, monitor and evaluate threats and risks related to data protection, apply corrective measures and control them or focus on the protection of printed data and control the printing itself. Moreover, if companies are members of various associations or clusters, the evaluation requirements need to be modified according to their roles and competencies (Bureš et al., 2012).

Threats and risks associated with the data misuse should be assessed not only by legal entities but also by individuals, and risks need to be minimized. The aim is therefore to protect data and to have prepared sanctions for those who misuse the data, which the GDPR undoubtedly brings. However, it can already be predicted that the GDPR is only the 'first swallow' in the field of data protection, as the European Commission is already working on the EU's digital strategy, which includes cyber security infrastructure. Moreover, digital education is considered and included. In addition to this strategy, it presented a 'white paper' that defines targets for the credible use of artificial intelligence. The vision is to enable people to maximize the benefits of artificial intelligence without worrying about their data and privacy (European Commission, 2020b). In the future, therefore, we can expect other laws ensuring the protection of personal data, but their effectiveness will be demonstrated by the practice itself. This fact will create space for further follow-up studies to describe the development of this issue over time.

Apparently, there are limitations associated with this study. First of all, the formulation of the research questions is vague and generic. Thus, acquired answers can be considered as too descriptive. However, their specifications open pathways for further research focused on specific GDPR-related issues. Therefore, it enables an application of other criteria for analysis as this study deals only with country and company size. Second, while internal validity does not represent an issue, the external validity of the research is at the low level due to the selection of non-probabilistic sampling methods. Third, although the GDPR definition is strict and exact, different countries can differ in attitudes and legal procedures. Therefore, outcomes of the comparison of particular countries are rather indicative. Fourth, although the outcomes do not reveal significant differences in case of Great Britain, the results can be partially influenced by Brexit. According to the current legal system of Great Britain, this country does not have to follow the GDPR rules. However, the Great Britain's version of the GDPR is compatible with the European Union version.

***Acknowledgment:*** *The research has been partially supported by the Faculty of Informatics and Management UHK specific research project 2107 Integration of Departmental Research Activities and Students' Research Activities Support.*

## References

Abdulghani, H. A., Nijdam, N. A., Collen, A., & Konstantas, D. (2019). A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. *Symmetry, 11*(6)*,* 774. https://doi.org/10.3390/sym11060774

Andrew, J., & Baker, M. (2019). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics, 168*(3), 1–14. https://doi.org/10.1007/s10551-019-04239-z

Bach, R. L., Kern, C., Amaya, A., Keusch, F., Kreuter, F., Hecht, J., & Heinemann, J. (2019). Predicting Voting Behavior Using Digital Trace Data. *Social Science Computer Review*. https://doi.org/10.1177/0894439319882896

Botta, M., & Wiedemann, K. (2019). The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey. *The Antitrust Bulletin, 64*(3)*,* 428–446. https://doi.org/10.1177/0003603X19863590

Bovenberg, J., Peloquin, D., Bierer, B., Barnes, M., & Knoppers, B. M. (2020). How to fix the GDPR's frustration of global biomedical research: Sharing of data for research beyond the EU must improve. *Science, 370*(6512)*,* 40–42. https://doi.org/10.1126/science.abd2499

Breen, S., Ouazzane, K., & Patel, P. (2020). GDPR: Is your consent valid? *Business Information Review, 37*(1), 19–24. https://doi.org/10.1177/0266382120903254

Brodin, M. (2019). A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research, 4*(2), 243–264. https://doi.org/10.1007/s41125-019-00042-z

Bureš, V., Jašíková, V., Otčenášková, T., Kolerová, K., Zubr, V., & Marešová, P. (2012). A Comprehensive View on Evaluation of Cluster Initiatives. In J. Politis (Ed.), *Proceedings of the 8th European Conference on Management Leadership and Governance (ECMLG).* (pp. 74–79). Pafos, Cyprus. Reading: Academic Conferences International.

Cisco. (2019, February 11). *Požadavky GDPR dnes splňuje 59% podniků, odhaluje průzkum Cisco [The Cisco research reveals: The GDPR requirements are met in 59% of companies only].* https://www.cisco.com/c/cs_cz/about/news/2019/20190211.html

Czech News Agency & iDNES.cz. (2019, July 12). *Rekordní pokuta. Facebook zaplatí pět miliard dolarů za porušení soukromí [Record fine. Facebook will pay $ 5 billion for privacy violations].* https://www.idnes.cz/ekonomika/zahranicni/facebook-pokuta-poruseni-ochrana-soukromi-miliard-usa.A190712_221657_eko-zahranicni_pmk

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review, 34*(2), 193–203. https://doi.org/10.1016/j.clsr.2017.10.003

Donnelly, M., & McDonagh, M. (2019). Health Research, Consent and the GDPR Exemption. *European Journal of Health Law, 26*(2), 97–119. https://doi.org/10.1163/15718093-12262427

Duncan, B., & Zhao, Y. (2018). Risk Management for Cloud Compliance with the EU General Data Protection Regulation. In *2018 International Conference on High Performance Computing Simulation (HPCS),* Orleans, France (pp. 664–671). https://doi.org/10.1109/HPCS.2018.00109

Eckert, N. (2019, April 30). *What Are the Real Costs of GDPR Compliance?* GDPR.365. https://www.gdpr365.com/what-are-the-real-costs-of-gdpr-compliance/

European Commission. (2018). *The GDPR: New opportunities, new obligations: what every business needs to know about the EU General Data Protection Regulation* (Report). Luxembourg: Publications Office of the European Union. Retrieved from https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf

European Commission. (2019). *What does the General Data Protection Regulation (GDPR) govern?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

European Commission. (2020a). *EU data protection rules.* https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

European Commission. (2020b). *White Paper on Artificial Intelligence a European approach to excellence and trust* (Report). Brussels: European Commission. Retrieved from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Union. (2016). Regulation (EU) 2016/679 of The European Parliament and of the Council. *Official Journal of the European Union.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Gal, M. S., & Aviv, O. (2020). The Competitive Effects of the GDPR. *Journal of Competition Law & Economics, 16*(3), 349–391. https://doi.org/10.1093/joclec/nhaa012

GDPR.eu. (2019a). *Data anonymization and GDPR compliance: The case of Taxa 4×35.* https://gdpr.eu/data-anonymization-taxa-4x35/

GDPR.eu. (2019b). *GDPR checklist for data controllers.* https://gdpr.eu/checklist/

GDPR.eu. (2019c). *GDPR-compliant services for businesses.* https://gdpr.eu/compliant-services/

GDPR.eu. (2019d, May). *GDPR Small Business Survey: Insights from European small business leaders one year into the General Data Protection Regulation* (Report). Brussels: GDPR.eu. Retrieved from https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf

Gideon, L. (Ed.). (2012). *Handbook of Survey Methodology for the Sciences.* New York, NY: Springer-Verlag. https://doi.org/10.1007/978-1-4614-3876-2

Gregory Voss, W., & Houser, K. A. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal, 56*(2), 287–344. https://doi.org/10.1111/ablj.12139

Härting, R. C., Kaim, R., & Ruch, D. (2020). Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models – An Empirical Study with a Quantitative Design. In G. Jezic, J. Chen-Burger, M. Kusek, R. Sperka, R. Howlett, & L. Jain (Eds.), *Agents and Multi-Agent Systems:*

*Technologies and Applications 2020: Smart Innovation, Systems and Technologies* (Vol. 186, pp. 295–303). Singapore: Springer. https://doi.org/10.1007/978-981-15-5764-4_27

IBM. (2020). *SPSS Statistics – Overview.* https://www.ibm.com/products/spss-statistics

IT Governance Privacy Team. (2020). *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4th ed.)*. Ely: IT Governance Publishing. https://doi.org/10.2307/j.ctv17f12pc

Kasse, J. P., Xu, L., deVrieze, P., & Bai, Y. (2018). The Need for Compliance Verification in Collaborative Business Processes. In L. Camarinha-Matos, H. Afsarmanesh, & Y. Rezgui (Eds.), *Collaborative Networks of Cognitive Systems. PRO-VE 2018. IFIP Advances in Information and Communication Technology* (Vol. 534, pp. 217–229). Cham: Springer. https://doi.org/10.1007/978-3-319-99127-6_19

Korpisaari, P. (2019). GDPR Implementation Series · Finland: A Brief Overview of the GDPR Implementation. *European Data Protection Law Review, 5*(2), 232–237. https://doi.org/10.21552/edpl/2019/2/13

Lachaud, E. (2020). What GDPR tells about certification. *Computer Law and Security Review, 38,* 105457. https://doi.org/10.1016/j.clsr.2020.105457

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management, 22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Luxatia International. (2019). *GDPR Statistics from the First Year (Infographic)*. https://www.luxatiainternational.com/article/gdpr-statistics-from-the-first-year-infographic

Malgieri, G. (2019). Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations. *Computer Law & Security Review, 35*(5), 105327. https://doi.org/10.1016/j.clsr.2019.05.002

Marelli, L., Lievevrouw, E., & Van Hoyweghen, I. (2020). Fit for purpose? The GDPR and the governance of European digital health. *Policy Studies, 41*(5), 447–467. https://doi.org/10.1080/01442872.2020.1724929

Meijering, L., Osborne, T., Hoorn, E., & Montagner, C. (2020). How the GDPR can contribute to improving geographical research. *Geoforum, 117,* 291–295. https://doi.org/10.1016/j.geoforum.2020.05.013

Mikulecký, P., Olševičová, K., Bureš, V., & Mls, K. (2011). Possibilities of Ambient Intelligence and Smart Environments in Educational Institutions. In N. Y. Chong, & F. Matrogiovanni (Eds.), *Handbook of Research on Ambient Intelligence and Smart Environments: Trends and Perspectives* (pp. 620–639). Hersey, PA: IGI Global.

Mitrou, L. (2020). GDPR implementation series: Greece: The new data protection framework. *European Data Protection Law Review, 6*(1), 107–113. https://doi.org/10.21552/edpl/2020/1/14

National Cyber and Information Security Agency. (2019a, June 21). *České energetické firmy čelily cvičným kybernetickým útokům [Czech energy companies faced training cyber attacks].* https://nukib.cz/cs/infoservis/aktuality/1350-ceske-energeticke-firmy-celily-cvicnym-kybernetickym-utokum/

National Cyber and Information Security Agency. (2019b). *GDPR (obecné nařízení) [GDPR: General Regulation].* https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

O'Brien, R. (2016). Privacy and security: The new European data protection regulation and it's data breach notification requirements. *Business Information Review, 33*(2), 81–84. https://doi.org/10.1177/0266382116650297

Peloquin, D., DiMaio, M., Bierer, B., & Barnes, M. (2020). Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics, 28*(6), 697–705. https://doi.org/10.1038/s41431-020-0596-x

Presthus, W., & Sørum, H. (2018). Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. *Computer Science Procedure, 138,* 603–611. https://doi.org/10.1016/j.procs.2018.10.081

Puljak, L., Mladinić, A., Iphofen, R., & Koporc, Z. (2020). Before and after enforcement of GDPR: Personal data protection requests received by Croatian Personal Data Protection Agency from academic and research institutions. *Biochemia Medica, 30*(3), 030201. https://doi.org/10.11613/BM.2020.030201

Radley-Gardner, O., Beale, H., & Zimmermann, R. (Eds.). (2016). *Fundamental Texts on European Private Law.* Oxford: Hart Publishing. https://doi.org/10.5040/9781782258674

Sajfert, J. (2020). Croatia: Minimum Service for the Implementation, Big Service to the Public

Sector. *European Data Protection Law Review, 6*(2), 281–288. https://doi.org/10.21552/edpl/2020/2/14

Sobers, R. (2020, June 17). *A Year in the Life of the GDPR: Must-Know Stats and Takeaways.* Varonis. https://www.varonis.com/blog/gdpr-effect-review/

Sørum, H., & Presthus, W. (2020). Dude, where's my data? The GDPR in practice, from a consumer's point of view. *Information Technology & People,* (ahead-of-print). https://doi.org/10.1108/ITP-08-2019-0433

SPSS. (2020). *SPSS One-Way ANOVA Tutorial*. https://www.spss-tutorials.com/spss-one-way-anova/

Svobodová, L., & Hedvičkáková, M. (2015). Doing Business in the Countries of Visegrad Group. *Procedia Economics and Finance, 34,* 453–460. http://doi.org/10.1016/S2212-5671(15)01654-8

Tahal, R., & Formánek, T. (2020). Reflection of GDPR by the Czech Population. *Management and Marketing. Challenges for the Knowledge Society, 15*(1), 78–94. https://doi.org/10.2478/mmcks-2020-0005

Tambou, O. (2019). France · Lessons from the First Post-GDPR Fines of the CNIL against Google LLC. *European Data Protection Law Review, 5*(1), 80–84. https://doi.org/10.21552/edpl/2019/1/13

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review, 38,* 105454. https://doi.org/10.1016/j.clsr.2020.105454

Tchinaryan, E. O., Lavrentieva, M. S., Kuchenin, E. S., & Neznamova, A. A. (2019). Digital Technologies of the European Union in Personal Data Protection. *International Journal of Innovative Technology and Exploring Engineering, 8*(12), 3600–3604. https://doi.org/10.35940/ijitee.L3798.1081219

van de Waerdt, P. J. (2020). Information asymmetries: Recognizing the limits of the GDPR on the data-driven market. *Computer Law and Security Review, 38,* 105436. https://doi.org/10.1016/j.clsr.2020.105436

Vejvodová, A., & Rosůlková, J. (2019). *Absurdní rok s GDPR [An absurd year with GDPR].* National Cyber and Information Security Agency. https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=46962

Zahariev, M., & Makshutova, R. (2020). GDPR implementation series · Bulgaria. *European Data Protection Law Review, 6*(3), 424–432. https://doi.org/10.21552/edpl/2020/3/12