*Anamarija Mladinić**
*Zdravko Vukić***
*Ante Rončević****

Original scientific paper
UDKUDK 334.7(497.5):342.738
DOI: https://doi.org/10.25234/pv/23972
Paper received on 22 November 2022
Paper accepted on 29 June 2023

GDPR COMPLIANCE CHALLENGES IN CROATIAN MICRO, SMALL AND MEDIUM SIZED ENTERPRISES

Summary: *The General Data Protection Regulation (EU) 2016/679 which applies uniformly since 25th May 2018 in the European Economic Area (EEA) requires small and medium enterprises (SMEs) to respect the right to personal data protection of their clients, customers, and employees. The GDPR is designed to strengthen the data protection rights of all individuals within the EEA ensuring more effective protection for consumers and increased privacy considerations for businesses. However, even after more than four years of its entry into full application, the implementation of the GDPR is still an issue for Croatian SMEs, who, unlike the larger companies, very often lack the human and financial resources to comply with the data protection legal framework. This paper covers theoretical considerations and results of an online survey conducted with 345 SMEs in the Republic of Croatia with the aim to gain insights into their GDPR compliance hurdles. The results of the study have shown that the level of understanding of obligations arising from the GDPR among Croatian SMEs is rather low and that compliance with the data protection legal framework is not at a satisfactory level.*

Keywords: *compliance, Croatian SMEs, data protection authorities, General Data Protection Regulation (GDPR), personal data protection*

* Anamarija Mladinić, the Head of the Department for EU, International Cooperation and Legal Affairs, Croatian Personal Data Protection Agency, Selska cesta 136, 10000 Zagreb. E-mail address: anamarija.mladinic@azop. hr. ORCID: https://orcid.org/0009-0009-2597-7348.

** Zdravko Vukić, univ. mag. oec., director of the Croatian Personal Data Protection Agency, Selska cesta 136, 10000 Zagreb. E-mail address: zdravko.vukic@azop.hr. ORCID: https://orcid.org/0009-0003-9942-7791.

*** Ante Rončević, PhD, Full Professor, University North, Trg dr. Žarka Dolinara 1, 48000 Koprivnica. E-mail address: aroncevic@unin.hr. ORCID: https://orcid.org/0000-0003-2527-9506.

1. INTRODUCTION

The General Data Protection Regulation (EU) 2016/679 applies uniformly since 25th May 2018 in the European Economic Area (EEA), which encompasses the territory of the Member States of the European Union (EU) as well as Iceland, Liechtenstein and Norway[1]. On the same date, in the Republic of Croatia entered into force Act on the Implementation of the GDPR which ensures the implementation of the GDPR and sets out additional rules on the processing of personal data in specific circumstances, such as processing of personal data in connection with video surveillance, processing of biometric and genetic data, processing of children's personal data in relation to information society services and processing of personal data for statistical purposes.[2] The GDPR lays down rules on the protection of natural persons regarding the processing of personal data with the main goal to protect the fundamental rights of individuals: the right to protection of personal data in a data-driven world where personal data are being processed every second. In the increasingly digitalised economy based on the exploitation and monetization of data, personal data needs to be effectively protected as part of a human-centric approach to the opportunities and challenges of emerging technologies such as Artificial Intelligence, 5G and the Internet of Things, biometrics, blockchain etc. Furthermore, there are many situations where the processing of personal data is not transparent, and individuals are not even aware that their data is being used. Another very important goal of the GDPR is to enable free and lawful data flows in European Economic Area, but also to ensure the equal protection of personal data when the personal data of European citizens are transferred and stored in third countries. Although the GDPR is a European Union regulation, non-EU organizations that collect, process and store the personal data of the individuals living in the European Economic Area are also required to comply with the GDPR. However, even after more than 5 years since the GDPR became applicable in the EEA, the implementation of the GDPR is still an issue, especially for SMEs, who, unlike the larger companies, very often lack human and financial resources to comply with the data protection legal framework. More than 99% of the enterprises in Croatia, as well as in the EU are small and medium enterprises[3], which makes them the backbone of the European economy. At the same time, they represent the largest group of data controllers/processors who collect and process a large amount of personal data. European Commission acknowledges that GDPR is challenging, especially for SMEs, therefore financially supports the activities of data protection authorities aimed at underpinning SMEs in their efforts to comply with the GDPR. Furthermore, the European Commission encourages data protection authorities to develop practical tools, especially digital tools that can be replicated in other Member States, practical guidance written in plain language, templates and forms to help low-risk SMEs meet their obligations.[4] Moreover, it is important to outline that effective protection of personal data is an economic

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 16 June 2022 (HR).

2 Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/2018) (HR).

3 'What is SME?' (*European Commission*, 8 September 2020) <https://ec.europa.eu/growth/smes/sme-definition_en> accessed 6 June 2022.

4 European Commission's COMMUNICATION (COM/2020/264) Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 16 June 2022 (EN).

necessity – without consumers' trust in the way their data is being processed there can be no sustainable growth of the European data-driven economy. A single data legal framework enables data to flow freely and lawfully within the EEA and across sectors for the benefit of businesses. In order to bolster the competitiveness of European SMEs, it is crucial that synergies between trade and data protection legal frameworks enable safe international data flows.[5] A key challenge is to create a regulatory environment that maintains the balance between the protection of individuals' fundamental rights and freedoms, fostering innovation, and addressing the potential negative consequences of technological advancements.

2. THEORETICAL FRAMEWORK

While most data protection provisions aimed at the data protection of individuals in Croatia are found in the GDPR and the Act on the Implementation of the GDPR, there are many other laws and bylaws which prescribe specific rules for the processing of individuals' personal data (i.e. Labour Law, Credit Institution Act, Act on prevention of money laundering and funding on terrorism, Electronic Communications Act, Accounting Act, Consumer Protection Law, Family Act, Rulebook on the e-visitor system etc.) Article 5 of GDPR defines basic principles relating to the processing of personal data: personal data shall be processed lawfully, fairly and in a transparent manner, adequate, relevant and limited to what is necessary for the purpose, on the basis of correct data, protected against loss, destruction or damage and providing for the integrity and confidentiality of such data.[6] In addition, personal data may only be stored in a form that permits the identification of the data subjects for as long as this is necessary. According to the principle of accountability, every SME needs to be able to demonstrate compliance with the GDPR requirements. Fundamental requirements on the security of processing personal data are provided in Articles 5, 12, 25 and 32 of GDPR.[7] The GDPR requires SMEs to apply appropriate technical and organizational measures to adequately protect the personal data of individuals and to mitigate the risks to the rights and freedoms of individuals. In a data-driven world, there are numerous and complex ways in which personal data are being processed. As a result, compliance with the data protection principles needs to be supplemented with risk analysis and the management of risks.

2.1. RISK-BASED APPROACH

The risk assessment is the responsibility of SMEs as data controllers and should include factors such as the number of individuals whose data are being processed and likely adverse

5 European Commission's COMMUNICATION (COM/2020/264) Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 16 June 2022 (EN).

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 16 June 2022 (HR).

7 'The Standard Data Protection Model: A method for Data Protection advising and controlling on the basis of uniform protection goals' (AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 17 April 2020) <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf> accessed 23 May 2022.

effects on the individuals' rights and freedoms arising from the personal data processing activities. In other words, the risk level is assessed by combining the likelihood or probability (of the risk to materialize) and the severity (of the consequences due to the materialization of the risk).[8] From a data protection perspective, certain business sectors are considered to be riskier than others, for example, health care services; solvency and creditworthiness; creation and use of profiles (profiling); political, trade union, and religious activities; telecommunications services; insurance; banking and financial companies; social services activities; advertising; large-scale CCTV).[9] A risk-based approach was explored by Peter Hustinx,[10] the European Data Protection Supervisor in the period from 2004 to 2014. It means that compliance efforts should be primarily directed at areas where protection is most needed, due to sensitivity of data or processing operations. In other words, GDPR compliance for a SME with higher-risk processing activities (i.e. polyclinic) is more complex than compliance for an SME with lower-risk processing activities (i.e. beauty salon). Therefore, more detailed obligations should apply where the risk is higher and less burdensome obligations where the risk is lower.[11] Moreover, a risk-based approach allows SMEs a certain level of flexibility to customize technical and organizational solutions to their specific needs to reach compliance with data protection requirements. GDPR does not set out specific technical and organisational measures to comply with the law yet requires that the SMEs understand the data processing activities they undertake, among others, to understand the purposes, scope, lawful basis and risks arising from such processing activities. The necessary level of data security is determined by the following factors: the security features available in the market for any particular type of processing, the costs, and the risks of processing the data for the fundamental rights and freedoms of individuals.[12] A lot of criticism of the GDPR is directed to the increased financial burden for SMEs in relation to aligning business processes with the GDPR requirements, for example, conducting data protection impact assessment. A direct reply to such criticism may be found in Article 40 of GDPR, where it is stated that codes of conduct should contribute to the proper application of the GDPR, taking into account the specific needs of SMEs.[13] Codes of conduct constitute self-regulatory instruments and need to be submitted for approval to the national data protection authority (in Croatia to the Croatian Personal Data Protection Agency). However, to date, there is no significant relevant code of conduct in the Republic of Croatia. To conclude, there is no *one- size fits all* solution, meaning that technical and organisational measures to ensure the maximum level of personal data protection are not going to be the same for a polyclinic and a beauty salon. However, whatever the level of risk involved in

8 Martin Brodin 'A Framework for GDPR Compliance for Small and Medium-Sized Enterprises' (2019) 4 European Journal for Security Research 243.

9 Lina Jasmontaitė-Zaniewicz, Alessandra Calvi, Renata Nagy and David Barnard-Wills, *The GDPR made simple (r) for SMEs* (ASP editions – Academic and Scientific Publishers 2021).

10 Peter Hustinx 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (European Data Protection Supervisor, 15 September 2014) <https://edps.europa.eu/sites/default/files/publication/14-09-15_article_eui_en.pdf> accessed 23 May 2022.

11 Brendan Quinn *Data Protection Implementation Guide: A legal, Risk and Technology Framework for the GDPR* (Kluwer Law International 2021).

12 'Handbook on European data protection law' (*European Union Agency for Fundamental Rights and Council of Europe,* 25 May 2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 23 May 2022.

13 Paul de Hert and Vagelis Papakonstantinou, "The new General Data Protection Regulation: still a sound system for the protection of individuals?" (2016) 32 Computer Law and Security Review 179.

the processing of personal data, all SMEs who are processing individuals' personal data should always respect data protection principles, data subjects' rights, and general provisions of the GDPR. Moreover, the processing must never be performed secretly, and individuals should always be informed about the potential risks.

2.2. DATA BREACHES

In the case of a personal data breach, the data controller needs to notify the personal data breach to the supervisory authority (in Croatia: Croatian Personal Data Protection Agency) and inform about the breach individuals concerned unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. SMEs acting as data controllers should put in place a policy to address data breaches. This policy should include procedures for documenting every data breach and fulfilling the requirements outlined in Articles 33 and 34 of the GDPR, which involve notifying the relevant supervisory authority and affected individuals. Furthermore, it is important to highlight that SMEs should take all necessary measures to prevent future data breaches from occurring again. In 2018, the Croatian Data Protection Authority received 49 data breach notifications, which increased to 73 in 2019, further rising to 107 in 2020, and reaching 108 in 2021. However, there was a slight decrease in 2022 with 97 data breach notifications reported. At the EU level, there has been a notable shift in the trend of data breach notifications. After experiencing four consecutive years of growth, the annual aggregate number of data breach notifications has seen a decline for the first time in 2022. Since 28 January 2022, data protection authorities in the European Economic Area have received notifications of approximately 109,000 personal data breaches, demonstrating a decrease compared to the total of around 120,000 reported in 2021.[14] This trend indicates that organizations might be avoiding reporting breaches, potentially influenced by concerns relating to investigations, enforcement actions, fines, and compensation claims that could arise as consequences.

2.3. FINES FOR FAILING TO COMPLY WITH THE GDPR

The GDPR provides data protection authorities with various options in the event of non-compliance with data protection rules, including issuing warnings, reprimands, temporary or permanent bans on processing, and fines of up to €20 million or 4 % of the business's total annual worldwide turnover.[15] Even though the basic principles relating to the processing of personal data and data subject rights were already defined in the Law on Personal Data

14 'DLA Piper GDPR Fines and Data Breach Survey: January 2023' *(DLA Piper,* 25 January 2023*)* <https://www.dlapiper.com/en-ae/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023> accessed 18 June 2022.

15 'What if my company/organisation fails to comply with the data protection rules?' (*European Commission*, 25 May 2018) <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organis ations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rul esen> accessed 18 June 2022.

Protection from 2012,[16] the GDPR came as a major shake-up for Croatian SMEs and data controllers in general. The main reason for rather law interest to comply with the Law is the fact that the Croatian data protection authority (Croatian Personal Data Protection Agency) did not have the power to impose administrative fines prior to the advent of the GDPR.[17] In 2017 the Croatian Personal Data Protection Agency received 850 requests for legal advice in relation to compliance with the data protection legal framework. In the period from May 25th, 2018 to 31st December 2018 the Agency had a dramatic increase in the number of requests, compared to the pre-GDPR period. In the first half of 2018, the Agency received 859 requests and in the second half of 2018 this number increase to 2605 queries from SMEs and data controllers from all sectors.[18] This sudden interest in compliance with the data protection legal framework was primarily caused by the spread of disinformation in the Croatian media, stating that every organization that fails to comply with the GDPR will be liable to pay fines amounting to up to 20 million EUR. In the period 2019–2021,[19] the number of queries received by SMEs is significantly lower, and the reasons could be found in: the COVID-19 crisis, educational activities organized by the Croatian Personal Data Protection Agency where SMEs were receiving answers to their questions, and finally the perception of SMEs that they are "below the radar" of data protection authorities and that imposition of fines is a concern of big companies.[20] Nevertheless, there have been instances where fines have been imposed on SMEs found to be in violation of data protection regulations. For example, the Belgian data protection authority issued a 15,000 EUR fine to an SME for not complying with information obligations arising from the GDPR when using cookies; the French data protection authority issued a 20,000 EUR fine to a translation company for continuously recording its employees at their workstations,[21] and the Croatian data protection authority issued 25,000 EUR fine to the IT company failing to undertake the appropriate organisational and technical measures to protect personal data. In the case of the fine issued by the Croatian Personal Data Protection Agency, a data controller was a big company from the telecommunication sector, which contracted a data processor (IT company) to maintain its web services. The data controller reported a personal data breach to the Agency alleging that a hacker group gained access to their server by exploiting a publicly available vulnerability of a web application from 2019, used by the data processor. On that occasion, the personal data of 28,000 users were compromised. Based on the analysis of the gathered documentation and contracts between the data controller and processor, the Agency concluded that the IT company was obligated to adhere to the website containing publicly available vulnerabilities known as "OWASP Top 10", and that the company failed to update the

16 Zakon o zaštiti osobnih podataka (no longer in force) (NN 106/2012) (HR).

17 'About the Croatian Personal Data Protection Agency' (*Croatian Personal Data Protection Agency*, 2 December 2018) <https://azop.hr/about-the-agency/> accessed 18 June 2022.

18 Livia Puljak, Anamarija Mladinić, Ron Iphofen and Zvonimir Koporc, 'Before and after enforcement of GDPR: Personal data protection requests received by Croatian Personal Data Protection Agency from academic and research institutions' (2020) 30 (3) Biochemia Medica 363.

19 'Godišnja izvješća o radu' (*Croatian Personal Data Protection Agency*, 8 November 2021) <https://azop.hr/godisnja-izvjesca-o-radu/> accessed 18 June 2022.

20 Leanne Cochrane, Lina Jasmontaite-Zaniewicz and David Barnard-Wills, 'Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-size Enterprises' (2020) 6 (3) European Data Protection Law Review 352.

21 Leanne Cochrane, Lina Jasmontaite-Zaniewicz and David Barnard-Wills, 'Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-size Enterprises' (2020) 6 (3) European Data Protection Law Review 352.

web application to the 2020 version. The Agency imposed an administrative fine for violating the provisions of Article 32 GDPR to the IT company acting as a data processor.[22]

3. DESCRIPTION OF THE PROBLEM

Compliance with the data protection legal framework not only involves understanding the GDPR provisions but rather all the national legislation that applies to the specific country and business sector. SMEs are under a lot of burden to understand all the relevant laws and monitor all the case law and changes in the legislation. Due to the general nature of the GDPR (*lex generalis*) it is important but complex to distinguish proper relationship with specific law (*lex specialis*) and struck the right balance. Moreover, as GDPR is a principle and risk-based regulation, its provisions are open to various different interpretations, for that reason often criticised for being unclear and causing legal uncertainty.[23] The European Commission encourages data protection authorities to provide practical guidance, templates, and digital tools tailor-made to the specific needs of SMEs. Furthermore, the European Data Protection Board (EDPB) is aware of the importance of developing further tools to help SMEs "implement appropriately the GDPR and to alleviate as much as possible their administrative burden. In any case, the risk-based approach promoted by the legislator in the text should be maintained, as risks for data subjects do not depend on the size of the controllers."[24] It can be assumed that the implementation process and level of GDPR compliance differ significantly from country to country. For example, with more than 50 years[25] of fostering a data protection culture, Germany already had a rather high level of data protection before the GDPR.[26] However, this doesn't mean that German SMEs are not facing challenges while complying with the GDPR. Härting et al. identified that the following six constructs have negative impacts on the implementation of the GDPR in the already existing business models of the German SMEs: missing "Know-how", high "Expenditure of time", big "Uncertainties", high "Costs", insufficient "Provision of information" and difficult "Process Adaptations". The research identified important influencing aspects of the implementation of GDRR in SMEs and identified areas in which SMEs need support in complying with the GDPR.[27] Another research conducted with the SMEs from Portugal

22 'Izdane nove upravne novčane kazne' (*Croatian Personal Data Protection Agency*, 5 July 2021) <https://azop.hr/izdane-nove-upravne-novcane-kazne> accessed 16 June 2022.

23 Leanne Cochrane, Lina Jasmontaite-Zaniewicz and David Barnard-Wills, 'Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-size Enterprises' (2020) 6 (3) European Data Protection Law Review 352.

24 'Contribution of the EDPB to the evaluation of the GDPR under Article 97' (*European Data Protection Board*, 18 February 2020) <https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en> accessed 25 May 2022.

25 Anne-Marie Zell, 'Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field German Law ' (2014) 15 (3) German Law Journal 461.

26 Ralf-Christian Härting, Raphael Kaim and Dennis Ruch, 'Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models—An Empirical Study with a Quantitative Design' (2020) Agents and Multi-Agent Systems: Technologies and Applications 14th KES International Conference 295.

27 Ralf-Christian Härting, Raphael Kaim and Dennis Ruch, 'Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models—An Empirical Study with a Quantitative Design' (2020) Agents and Multi-Agent Systems: Technologies and Applications 14th KES International Conference 295

has shown a lack of knowledge on their obligations regarding aspects of labour law and duties to implement security mechanisms on the personal data they store and process, data subject rights, and the need of concluding contracts with data processors.[28] A comparative study conducted in 8 European countries: Great Britain, France, Bulgaria, Poland, Spain, Germany, Slovakia, and the Czech Republic tried to find answers on what is the awareness of companies about GDPR and what is the current state of its implementation. The results have shown 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. Furthermore, the results of the study have shown that enterprises from Poland, France, Great Britain, and Germany are the most in line with the GDPR in defined areas.[29] Under the EU-funded project STAR II, research was conducted by project partners in collaboration with SMEs and SME associations, with the majority of respondents originating from Denmark and Hungary. According to the report on the SME experience of the GDPR, the major challenges they face under the GDPR include the significant time commitment required to prepare for the GDPR, vague and non-specific terminology used in the GDPR, determining the necessary documentation, establishing deletion and retention policies, implementing data minimization practices, deciding on the appropriate level of implementation and what qualifies as "sufficient", among various others.[30] In 2021 the Information Commissioner's Office conducted baseline market research to help improve its understanding of small and medium-sized businesses in the United Kingdom. The results have shown that three in five SMEs have some familiarity with data protection/ GDPR. Amongst those who have heard of it, fewer than half agree that they understand its implications for their business. One out of every three SMEs acknowledges the significance of data protection and GDPR for their business. However, a considerable number of SMEs in Great Britain view data protection/GDPR as unnecessary bureaucracy and only do the minimum necessary.[31] The literature does not provide any research on the experiences of Croatian SMEs regarding the implementation of the GDPR. However, a study conducted on 233 SMEs in the Republic of Croatia aimed to identify the most common methods and tactics of digital marketing and their noncompliance with the GDPR.[32]

4. METHODOLOGY OF RESEARCH

This paper covers theoretical considerations and results of an online survey conducted with 345 SMEs in the Republic of Croatia with the goal to examine the level of awareness of personal data protection of the Croatian SMEs and to identify their compliance issues and

28 Maria de Conceição Freitas and Miguel Mira da Silva, 'GDPR Compliance in SMEs: There is much to be done' (2018) 3(4) Journal of Information Systems Engineering & Management 30.

29 Marek Zanker, Vladimir Bureš V, Anna Cierniak-Emerych and Martin Nehéz, 'The GDPR at the Organizational Level: A Comparative Study of Eight European Countries ' (2021) E&M Economics and Management 24(2) 207.

30 David Barnard-Wills et al 'Report on the SME experience of the GDPR' <https://star-project-2.eu/wp-content/uploads/2021/02/STARII-D-2.2-Report-on-the-SME-experience-of-the-GDPR.pdf> accessed 18 March 2023.

31 'SME research' (*Information Commissioner's Office, SME research,* April 2021) <https://ico.org.uk/media/ about-the-ico/documents/4024787/ico-sme-research-2021.pdf> accessed 18 March 2023.

32 Natalija Parlov, Željko Sičaja and Tihomir Katulić, 'GDPR – Impact of General Data Protection Regulation on Digital Marketing', Annals of Disaster Risk Sciences (2018) 2 (1) 105.

needs. The survey was carried out as a part of the EU-funded project ARC – Awareness Raising Campaign. EU-funded project "Awareness Raising Campaign for SMEs (ARC)".[33] The goal of the survey was to identify the challenges that SMEs in Croatia face while trying to comply with the GDPR and accordingly address their needs by developing practical educational materials and activities which will help SMEs to tackle those challenges. The survey was conducted through the digital platform "Qualtrics" in the Croatian language in the period from 25th May 2020 to 10th September 2021, in cooperation with the ARC project partners and the Croatian Chamber of Economy who contacted 36 983 SMEs via email and invited them to participate in the anonymous study. After the initial invitation, the participants received four more invitations to complete the survey. The COVID-19 crisis could be an explanation for the low engagement of SMEs in the survey, and another explanation could be a lack of interest in GDPR compliance. In almost all sectors, the crisis has pushed digitalization in SMEs and led them to rely almost completely on digital tools and new processing activities of personal data. The SMEs were trying to identify, assess and mitigate privacy risks for specific products, services, and data processing activities. In this study, the authors have used the following scientific methods: cross-sectional and cross-tabulation analysis, synthesis, classification, description, and compilation. The aim of this paper is to answer the following research questions:

To what extent do small and medium-sized enterprises (SMEs) in the Republic of Croatia comprehend their obligations under the General Data Protection Regulation (GDPR)?

To what extent do small and medium-sized enterprises (SMEs) in Croatia currently comply with the requirements of the General Data Protection Regulation (GDPR)?

Do Croatian SMEs need specific tools, such as customized guidelines and templates, to support them in achieving compliance with the General Data Protection Regulation (GDPR)?

4.1. STRUCTURE OF THE SURVEY

For the purpose of the study, the authors have created a survey comprised of 83 questions divided into 10 sections: "Awareness", "Engagement with customers", "Transparency", "Security", "Accountability", "Legal Basis", "Jurisdictional Information", "Monitoring property and people", "Breaches", "Covid 19 crisis" and "General Statistical Information". To develop the survey, the authors utilized various resources developed by data protection authorities and European Data Protection Board[34] as guidelines, including a self-assessment checklist created by data protection experts from the Information Commissioner's Office,[35] the regulatory body for data protection in the United Kingdom. Additionally, the authors referred to guidelines

33 'Objectives of ARC project' (*Awareness Campaign for SMEs*, 20 September 2020) <https://arc-rec-project.eu/objectives/> accessed 18 June 2022.

34 'Guidelines, Recommendations, Best Practices' (*European Data Protection Board*) <https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en> accessed 18 March 2023.

35 'How well do you comply with data protection law: an assessment for small business owners and sole traders' *(Information Commissioner's Office,* April 2019*)* <https://ico.org.uk/for-organisations/sme-web-hub/checklists/assessment-for-small-business-owners-and-sole-traders/> accessed 18 March 2023.

and self-assessment checklists developed by the Irish Data Protection Commission,[36] and to a tool designed by experts from the Spanish Data Protection Authority, aimed to support companies that carry out low-risk data processing in their compliance with the GDPR.[37] In all sections, except for the "Awareness" and "General Statistical Information" sections, SMEs were provided with the choice to select one of the following responses: "Yes", "No", "Not applicable", "I don't know", or to refrain from answering the question. A four-point scale was utilized, intentionally excluding a "neutral" option, in order to encourage respondents to express a clear opinion. In the "Awareness" section, comprising 10 questions, SMEs were given the options of "Yes", "Some", "Little", and "None" to determine their level of awareness regarding various aspects. These questions aimed to assess their awareness of personal data processing, comprehension of the significance of GDPR compliance, and understanding of the roles of both the data controller and data processor. In the section "Engagement with customers", SMEs were asked to respond to 8 questions in relation to purposes and means of the processing of personal data (i.e for direct marketing, processing of personal data through website and cookies, via e-mail) and whether SMEs have internal policies in place for the protection of the personal data available to staff and customers. In the "Transparency" section SMEs were asked 7 questions important for the authors to determine whether SMEs ensure fair and transparent processing in respect of individuals concerned (customers/clients/staff) and their right to obtain confirmation and communication of personal data concerning them which are being processed. In the "Security" section SMEs were asked 8 questions with the goal to establish whether they have undertaken adequate technical and organisational measures to protect the personal data of individuals. In the "Accountability" section SMEs were asked 12 questions in order to determine whether they are able to demonstrate compliance with the GDPR, in accordance with the accountability principle. This means that they need to have in place documented processes and procedures aiming at tackling data protection. Some of the tools that could help SMEs to demonstrate accountability are: to put in place a procedure to deal with access requests from individuals as well as to put in place procedures to enable individuals to exercise their rights arising from the GDPR, to make privacy policy publicly available to customers/clients (according to the Article 13 and 14 of the GDPR), to keep records of processing activities, to conduct Data Protection Impact Assessment, to appoint Data Protection Officer on the basis of professional qualities and expert knowledge of data protection law and practices and the ability to fulfill the tasks from the Article 39 GDPR. In the section "Legal Basis and Jurisdictional Information", SMEs were asked 7 questions in relation to the identification of an adequate legal basis for the processing of personal data under Article 6 (1) GDPR. In the section "Monitoring property and people", SMEs were asked 8 questions in relation to the processing of personal data through video devices, GPS technologies and processing of biometric data. In the section "Breaches", SMEs were asked 7 questions regarding data breaches. GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmit-

36 'Guidance for SMEs' *(Data Protection Commission Ireland*, July 2019*)* <https://www.dataprotection.ie/en/dpc-guidance/guidance-smes> accessed 18 March 2023.

37 'Facilita RGPD' *(Spanish Personal Data Protection Agency*, May 2019*)* <https://www.aepd.es/en/guides-and-tools/tools/facilita-rgpd> accessed 18 March 2023.

ted, stored or otherwise processed."[38] In the section "Covid 19", SMEs were asked 10 questions about the processing of personal data in the context of the COVID-19 crisis (staff working remotely, processing of health data, erasure of personal data when it is no longer needed for the purpose of which was collected). In the section "General Statistical Information", SMEs were asked about the number of staff, the area of work (sector), the role that the respondent occupies in the enterprise, and gender. The final question provided respondents with an open-text box, allowing them the opportunity to share their thoughts and comments regarding any compliance issues they encountered.

5. RESEARCH RESULTS

The online survey has been carried out on 345 SMEs in Croatia with the goal to identify the level of awareness of personal data protection and hurdles of the Croatian SMEs in relation to compliance with the data protection legal framework. Out of 36 983 invited SMEs, only 345 SMEs participated in the survey. According to the report of the Center for Development Policy for SMEs from 2021, in 2020 there were 138.618 SMEs operating in the Republic of Croatia, with the vast majority of these (124.348) being micro-sized enterprises that employ between zero and nine people.[39]

5.1. GENERAL STATISTICAL INFORMATION

Table 1. Primary business sector of the survey respondents

Manufacturing	9.86 %	34	Entertainment/Art/Recreation	0.58 %	2
Medical/Health care/Social care	2.61 %	9	Energy	0.00 %	0
Pharmaceuticals	2.03 %	7	Tourism/Hospitality	1.74 %	6
Financial/Insurance	6.67 %	23	Agriculture/Forestry/Fishing	8.12 %	28
Transport	1.74 %	6	Media	0.87 %	3
Educational	2.90 %	10	Marketing	1.16 %	4
Charitable	0.00 %	0	Retail	2.03 %	7
Technological	7.83 %	27	Protection of people and property	13.91 %	48
Research	6.38 %	22	Other, please specify	24.35 %	84
Construction	6.09 %	21	No answer	0.29 %	1
Telco	0.87 %	3			

38 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 16 June 2022 (HR).

39 'Izvješće o malim i srednjim poduzećima u Hrvatskoj – 2021. Mala i srednja poduzeća u Hrvatskoj u uvjetima pandemije bolesti COVID-19' (*Center for Development Policy of SMEs*, 30 June 2022) <https://www.cepor.hr/w -Content/uploads/2015/03/CEPOR-Mala-i-srednja-poduze%C4%87a-u-HR-u-vrijeme-pandemije-COVID-19. pdf> accessed September 2022.

55.65 % of the survey participants work in an organisation with up to 10 employees, 41.45 % are directors and 57.97 % of the respondents identified themselves as female. More than 13 % of SMEs come from the protection of people and property sector, more than 9 % from the manufacturing sector, more than 7 % from the IT sector, more than 6 % from the financial sector, and more than 20 % haven't specified from which sector they are coming from. A very low response rate comes from SMEs from marketing (1.16 %), media (0.87 %), retail (2.03 %), and tourism sectors (1.74 %) which collect and process a large amount of personal data. The reason for a lack of interest could be found in the crisis caused by the COVID-19 outbreak that impacted significantly these four sectors. The largest number of the participants in the survey come from the private security sector (13.91 %) and the manufacturing industry (9.86 %). The high interest of the SMEs from these sectors in participating in the survey could also be explained by the impact of the COVID-19 crisis, which caused significant changes in the business practices of these two sectors, for example, introducing new processing activities such as processing of personal through thermal cameras, measuring the body temperature of employees and accelerated digitization of business processes. On the other hand, the low level of interest to participate in the survey of SMEs from the marketing, health, and tourism sectors, was not in line with the expectations of the authors, having in mind a significant number of questions received from these sectors during GDPR workshops organized within ARC project. The reason for the low interest of the SMEs from the abovementioned sectors most probably is related to the impact of the COVID-19 pandemic. More precisely, the COVID-19 crisis affected utterly the SMEs from marketing, health, and tourism sectors. Therefore, it is reasonable to conclude that in the period of conducting a survey, their focus was on finding ways to respond to the COVID-19 crisis and continue trading.

5.2. AWARENESS

68.12 % of SMEs answered that they process personal data and only 37.68 % feel well-informed about their obligations under the GDPR. Out of 37.68 % of SMEs who feel well informed about their obligations under the GDPR, more than 78 % identified themselves as female.

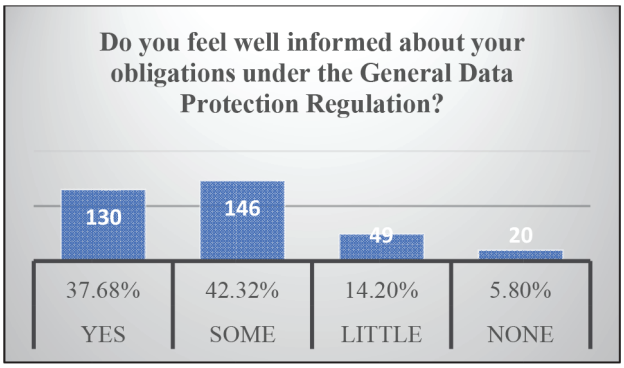

Chart 1. Awareness on obligations arising from the GDPR

Source: authors

Only 29.28 % of SMEs are confident that their staff has a satisfactory level of knowledge to operate in accordance with their obligations under the GDPR.

Chart 2. Awareness of GDPR obligations of employees

Source: authors

Although a significant percentage of SMEs are aware that their staff is not enough educated about data protection topics, only 37.68 % organized proper data protection training. Out of 37.68 % of those who organized data protection training for their staff, 75,29 % are confident that their staff has sufficient information to operate in accordance with the obligations under GDPR. 36.23 % of SMEs stated that they have reviewed their processing activities and only 34.78 % have changed their processing activities in response to this review. 55.94 % of SMEs consider compliance with the GDPR important for their business success, and only 13.91 % don't consider it important at all. Out of those who consider GDPR compliance important, 72.8 % identified themselves as female. Although according to Article 28 of GDPR data controllers and data processors have an obligation to enter into a legally binding contract governing the processing of personal data when a data controller engages a processor to process personal data on its behalf, only 41.74 % of respondents who use subcontractors has data processing agreements in place.

5.3. ENGAGEMENT WITH CUSTOMERS

42.57 % of SMEs use cookies to track customer engagement and their behavior and 48.55 % of them use direct marketing (online or postal) to engage with customers. 68.12 % of the survey participants stated that they have in place policies for the protection of the personal data that arise from engagement with customers. 63.08 % of SMEs responded that their staff is aware of these policies.

5.4. TRANSPARENCY

73.04 % of respondents stated that they inform customers about the data they are collecting about them and why they need them. 45.80 % stated that they have in place a retention

policy governing the deletion of data. Around 83 % of SMEs do not hold any special categories of data. 45.80 % stated that they have in place a retention policy governing the deletion of data. Around 83 % of SMEs do not hold any special categories of data.

5.5. SECURITY

When it comes to information security, 95.36 % of respondents stated that they use firewalls, passwords, and antivirus software to protect their computer systems. 74.13 % of respondents have controls in place to govern who on their staff can access personal data records. Only around 38 % of respondents use encryption software for their computers.

5.6. ACCOUNTABILITY

52.75 % of respondents publish privacy policies on their websites and only around 34 % of them know whether they are in obligation to keep records of their processing activities. Only 35.07 % of survey participants keep records of processing activities. 20.87 % of survey participants conducted a data protection impact assessment, and only 16.23 % of respondents halted project plans in response to data protection concerns. Only around 50 % of respondents have processes in place to deal with access requests from individuals and around 43 % have appointed data protection officers.

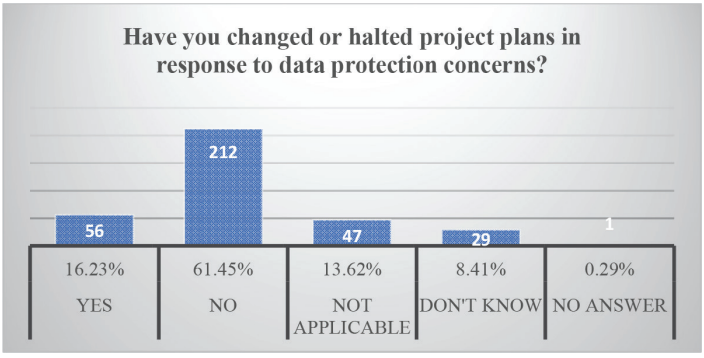

Chart 3. Response to data protection concerns
Source:authors

5.7. LEGAL BASIS AND JURISDICTIONAL INFORMATION

70.43 % of respondents stated that they have identified the legal basis they are relying on for the processing of personal data. Only around 20 % stated that they process children's

personal data and around 12 % stated that they transfer personal data outside the European Economic Area (EEA). 11.30 % of SMEs stated that they use cloud-based services whose servers are outside the EEA.

5.8. MONITORING PROPERTY AND PEOPLE

Only around 38 % of respondents use CCTV to monitor property and people. Around 66 % of those who operate CCTV have put in place an internal policy that regulates access to CCTV footage. Only 58 % of SMEs who use GPS technologies to monitor staff have internal policies to govern the use of monitoring technologies.

5.9. BREACHES

Only 34.78 % of respondents have in place a policy to deal with personal data breaches (e.g. loss or theft of data, employee error). Only 4.93 % of respondents stated that their enterprise experienced a data breach, 2.78 % of them notified the Croatian Personal Data Protection Agency and 4.01 % of them informed individuals about the data breach.

5.10. COVID

60.29 % of SMEs participating in the survey had staff working remotely due to COVID-19 crisis and only 36.52 % of them adjusted their data protection policies to respond to remote working needs.

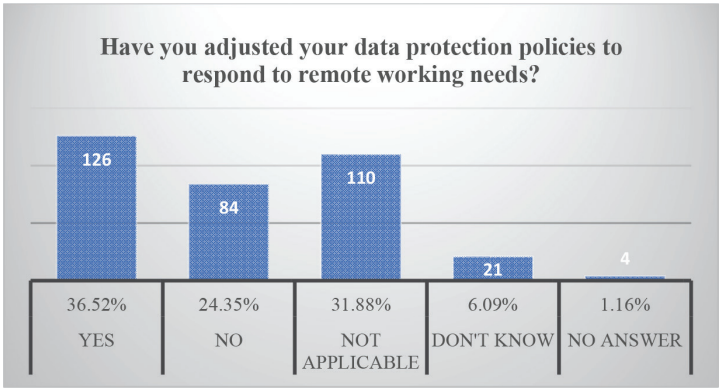

Chart 4: Processing of personal data during the COVID-19 crisis

Source: authors

Less than half of survey participants (39.71 %) have a plan for how to delete the information once it stops being necessary for the purposes for which was collected.

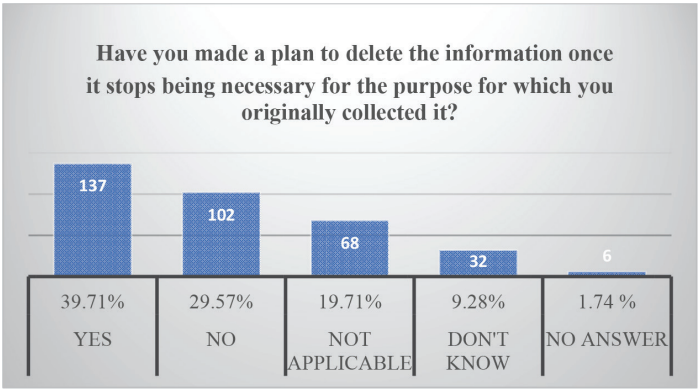

Chart 5: Deletion of personal data when they are no longer needed in the context of processing of personal data during COVID-19 crisis

Source: authors

In the last question, only 19 % of survey participants responded that they wanted to be contacted by the members of the project team to discuss their experiences in relation to GDPR compliance. In addition, all survey participants were provided with an open-ended question format, allowing them the opportunity to freely express their thoughts and discuss the challenges they faced during the implementation of the GDPR. Out of 52 comments, in 26 of them, SMEs stated that GDPR is an unnecessary administrative and financial burden for SMEs and that they don't see and benefit from it. Several SMEs expressed the need for increased assistance and guidance regarding the practical implementation of the GDPR, emphasizing its complexity and intricacy as a regulation.

6. DISCUSSION

The findings from the study reveal that a significant number of Croatian SMEs continue to face challenges in achieving GDPR compliance. Firstly, it is noteworthy that slightly over 37 % of respondents express feeling adequately informed about their obligations under the GDPR. Interestingly, among this group, more than 78 % identify themselves as female. The notably low response rate may be attributed to the survey being conducted during the coronavirus outbreak, which has caused disruptions in the global economy, particularly affecting SMEs. Additionally, this could be due to a lack of awareness regarding the importance of personal data protection and a general disinterest in GDPR compliance among these SMEs. The survey was intentionally structured to serve as a valuable self-assessment checklist for SMEs. It empowers them to identify their specific obligations under the GDPR and pinpoint areas where improvements are necessary to attain a higher level of GDPR compliance. Furthermore, SMEs had access to experts from the ARC team who were available to provide guidance on addressing their compliance challenges. However, the survey results indicate that more than

80 % of Croatian SMEs expressed their preference not to be contacted by the ARC team of researchers to share their experiences, questions, or concerns regarding data protection. Several reasons could contribute to this response. One potential reason is the fear of drawing negative attention from data protection authorities. Businesses may be concerned that engaging with researchers or sharing their experiences could result in scrutiny from the Croatian data protection authority and potential enforcement actions. This fear might stem from worries about non-compliance with data protection regulations or a lack of confidence in their current data protection practices. If businesses do not fully understand the significance of data protection or the requirements imposed by the GDPR, they may not see the value in participating in research initiatives or seeking guidance from experts. Although it was difficult to attract their attention to discretionary issues during the COVID-19 crisis, such as surveys, the Croatian SMEs were very interested to participate in the GDPR training activities organized within the ARC project,[40] during which a very low level of understanding of the GDPR provisions was demonstrated. In many cases, SMEs don't have the ability to demonstrate an adequate level of compliance and fail to comply with the GDPR due to misunderstandings of the data protection legal framework, jeopardizing in this way individuals' rights and freedoms and risking fines for data breaches.[41] Furthermore, less than 50 % of respondents stated that they have in place a data retention policy. It is of utmost importance to highlight that the GDPR has established the erasure of personal data as a fundamental requirement for all organizations. As digital processes become more prevalent and the COVID-19 crisis accelerates the adoption of new technologies, the scope of personal data processing has expanded to include various types of data that were not previously considered high-risk, such as voice recordings, metadata, data stored on social media and in emails, location tracking, etc.[42] Given these circumstances, it is crucial for SMEs to put in place data retention and erasure policies that encompass all record types, irrespective of their format. This is essential to uphold compliance with the principles of data minimization and storage limitation. Furthermore, a significant number of SMEs heavily rely on data processors; however, only slightly over 40 % of them have established data processing agreements in place. In addition, Croatian SMEs are facing challenges in complying with the transparency principle, particularly in terms of informing individuals about the processing of their personal data, as only slightly over 50 % of them have published privacy policies on their official websites. Moreover, the research results indicate that SMEs would greatly benefit from additional practical guidance and templates relating to various internal policies, including data breaches, data retention, and deletion, data subject access requests, internal policies governing the use of monitoring technologies (e.g., GPS tracking of employees), guidance on maintaining records of processing activities, developing meaningful privacy policies, and training strategies for staff members on data protection matters. However, there are also positive findings. When it comes to information security, more than 95 % of respondents stated that they utilize firewalls, passwords, and antivirus software to safeguard their computer systems. Additionally, over 70 % of SMEs claim to have identified a lawful basis for the pro-

40 'Radionice za mikro, male i srednje poduzetnike' (*Awareness Campaign for SMEs*, 20 September 2020) <https://arc-rec-project.eu/dogadanja/ > accessed 18 June 2022.

41 Luis M Pedroso, Virgínia Araújo, Manuel Perez Cota and João Paulo Magalhães, 'How can GDPR fines help SMEs ensuring the privacy and protection of processed personal data' (2021) 16th Iberian Conference on Information Systems and Technologies (CISTI) 1.

42 Brendan Quinn, Data Protection Implementation Guide: A legal, Risk and Technology Framework for the GDPR (Kluwer Law International 2021).

cessing of personal data. At the time of conducting the survey, there was no publicly available guidance in the Croatian language written in plain language and adapted to the needs of SMEs that would alleviate the administrative burden. Despite the European Data Protection Board publishing numerous guidelines addressing various data protection topics for data controllers and processors, these guidelines often appear overwhelming to average SMEs who lack expertise in legal and IT matters. Based on the results of the survey, partners in the ARC project have developed 20 guidance on topics that were identified as most relevant for the Croatian SMEs: data protection basics, data protection principles, data protection lawful bases, keeping records of processing activities, data transfers, data protection impact assessment, technical and organisational measures, CCTV, direct marketing, privacy policy, data security, phishing, data subject rights, data breaches, right to access to personal data, cookies, 2 self-assessment questionnaires and templates for legitimate interest assessment, data protection impact assessment, consent, privacy policy, records of processing activities and template for the contract between the data controller and processor.[43] In the period from 6th October 2020 until 5th July 2022, Croatian Personal Data Protection Agency conducted 30 GDPR workshops for 2552 SMEs. The GDPR workshops were organized as a part of ARC project activities, during which SMEs had the opportunity to ask their compliance questions and were given concrete support in their efforts to align their business processes with the GDPR.

7. CONCLUSION

The study has confirmed the previously identified issues and needs of SMEs regarding the implementation of the GDPR while also uncovering new ones. The findings of the study indicate that a considerable number of Croatian SMEs who participated in the survey lack a fundamental understanding of their obligations under the GDPR. It can be inferred that Croatian SMEs still encounter challenges in identifying the personal data they possess, determining its storage location, establishing appropriate retention periods, and ensuring secure data disposal when it is no longer necessary. Considering these findings, it is evident that the level of GDPR compliance among Croatian SMEs is unsatisfactory. However, this study is subject to several limitations. Firstly, there is a non-response bias, as only 0.93 % of the invited SMEs participated in the study, which may impact the generalizability of the findings. Secondly, the study relies on self-report data, introducing the possibility of response bias and relying on the honesty of the respondents. Additionally, a significant limitation of this study is the formulation of vague research questions, leading to acquired answers that are overly descriptive, and lacking depth and specificity. Future research can build upon the results of this study by focusing on specific sectors to explore the compliance of Croatian SMEs with the GDPR. Sectors such as tourism, financial, insurance, and marketing are traditionally characterized by processing a significant amount of personal data. Therefore, future research should investigate GDPR compliance within these sectors to gain insights into their specific challenges and practices. Moreover, it would be highly advantageous to delve into the exploration and development of diverse models for effectively implementing the (GDPR) across various industries. When organizations implement

43 'Objectives of ARC project' (*Awareness Campaign for SMEs*, 20 September 2020) <https://arc-rec-project.eu/objectives/> accessed 18 June 2022.

the GDPR, they should consider its implementation in light of their business objectives. Additionally, the model employed for GDPR implementation ought to encompass considerations of technological advancements, environmental influences, information management, supply chain management, and globalization, given that these factors exhibit variations across industries.[44] By addressing these research directions, future studies can contribute to a deeper understanding of GDPR compliance in specific sectors and provide insights into effective models for implementing the GDPR across various industries. Another intriguing finding is that among those who consider GDPR compliance important, 72.8 % identified themselves as female. This highlights the potential significance of exploring gender differences in the approach to GDPR compliance. Further investigation into how gender may influence attitudes, behaviors, and perceptions regarding GDPR compliance would be a valuable area of study. Based on our analysis, it can be inferred that the GDPR imposes significant compliance burdens on Croatian SMEs, who are often constrained by limited human and financial resources. Therefore, they require additional support from the data protection authority to enhance and reinforce their compliance efforts. One of the biggest mistakes SMEs make is considering GDPR compliance as just another box-ticking exercise when it is, in fact, a dynamic and ongoing process. During the lifetime of the processing activity, processing can change in many ways, and so can the risk profile. In order to keep in line with the principles of data protection such as data minimization, storage limitation, and the principle of accountability, SMEs need to conduct regular data flow audits in order to be able to identify the personal data they collect and process, understand the sources of such data and how the data is processed and who is accountable for the processing. While the primary objective of the GDPR is to enhance and safeguard individuals' data protection rights, certain provisions of the regulation also address the issue of concentrated market power held by major tech companies, commonly referred to as "gatekeepers", who process and monetize substantial volumes of personal data. Many SMEs argue that GDPR hinders innovation and restricts their ability to compete against larger companies.[45] In order to avoid strengthening the dominant market positions of large companies, further guidance and support for SMEs are needed to help them to overcome the overwhelming compliance burden. Moreover, as individuals become increasingly aware of their data protection and privacy rights, the necessity to build a "culture of data privacy" will become imperative for every organisation that processes personal data in the coming years. Achieving full GDPR compliance means that an organization has reached a high level of data protection which boosts the trustworthiness in the eyes of customers and could become a key competitive differentiator.

BIBLIOGRAPHY

1. Brodin M, 'A Framework for GDPR Compliance for Small and Medium-Sized Enterprises' (2019) 4 European Journal for Security Research 243
2. de Hert P and Papakonstantinou V, 'The new General Data Protection Regulation: still a sound system for the protection of individuals?' (2016) 32 Computer Law and Security Review 179

44 Tzanko Tzolov, 'One Model For Implementation GDPR Based On ISO Standards' (2018) International Conference on Information Technologies (InfoTech) 1.

45 Crispin Niebel, 'The impact of the General Data Protection Regulation on innovation and the global political economy' (2021) 40 Computer Law & Security Review.

3. Cochrane L, Jasmontaite-Zaniewicz L and Barnard-Wills D, 'Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-size Enterprises' (2020) 6 (3) European Data Protection Law Review 352
4. Zell M, 'Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field German Law ' (2014) 15 (3) German Law Journal 461
5. Härting RC, Kaim R and 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' (2022) Agents and Multi-Agent Systems: Technologies and Applications 14th KES International Conference 295
6. Zanker M, Bureš V, Cierniak-Emerych, A, Nehéz M, 'The GDPR at the Organizational Level: A Comparative Study of Eight European Countries ' (2021) E&M Economics and Management 24(2) 207
7. Parlov N, Sičaja Ž, Katulić T, 'GDPR –Impact of General Data Protection Regulation on Digital Marketing', Annals of Disaster Risk Sciences (2018) 2 (1) 105
8. Freitas M. C. and Mira da Silva 'GDPR Compliance in SMEs: There is much to be done' (2018) 3(4) Journal of Information Systems Engineering & Management 30
9. Puljak L, Mladinić A, Iphofen R and Koporc Z, 'Before and after enforcement of GDPR: Personal data protection requests received by Croatian Personal Data Protection Agency from academic and research institutions' (2020) 30 (3) Biochemia Medica 363
10. Pedroso LM, Araújo VM, Cota MP and Paulo Magalhães J, 'How can GDPR fines help SMEs ensuring the privacy and protection of processed personal data' (2021) 16th Iberian Conference on Information Systems and Technologies (CISTI) 1
11. Niebel C, 'The impact of the general data protection regulation on innovation and the global political economy' (2021) 40 Computer Law & Security Review
12. Jasmontaitė-Zaniewicz L, Calvi A, Nagy R and Barnard-Wills D, *The GDPR made simple(r) for SMEs* (ASP editions - Academic and Scientific Publishers 2021)
13. Quinn B, *Data Protection Implementation Guide: A legal, Risk and Technology Framework for the GDPR* (Kluwer Law International 2021)
14. Tzolov T, 'One Model For Implementation GDPR Based On ISO Standards' (2018) International Conference on Information Technologies (InfoTech) 1

REGULATIONS AND DOCUMENTS

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 16 June 2022 (HR)
2. Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/2018) (HR)
3. Zakon o zaštiti osobnih podataka (no longer in force) (NN 106/2012) (HR)
4. European Commission's COMMUNICATION (COM/2020/264) Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264 > accessed 16 June 2022 (EN)

INTERNET RESOURCES

1. 'Godišnja izvješća o radu' (*Croatian Personal Data Protection Agency,* 8 November 2021) <https://azop.hr/godisnja-izvjesca-o-radu/> accessed 18 June 2022
2. 'Izvješće o malim i srednjim poduzećima u Hrvatskoj – 2021. Mala i srednja poduzeća u hrvatskoj u uvjetima pandemije bolesti covid-19' (*Center for Development Policy of SMEs*, 30 June 2022) <https://www.cepor.hr/wp-content/uploads/2015/03/CEPOR-Mala-i-srednja-poduze%C4%87a-u-HR-u-vrijeme-pandemije-COVID-19.pdf> accessed September 2022
3. 'Izdane nove upravne novčane kazne' (*Croatian Personal Data Protection Agency,* 5 July 2021) <https://azop.hr/izdane-nove-upravne-novcane-kazne> accessed 16 June 2022
4. 'Radionice za mikro, male i srednje poduzetnike' *(Awareness Campaign for SMEs,* 20 September 2020*)* <https://arc-rec-project.eu/dogadanja/> accessed 18 June 2022
5. 'About the Croatian Personal Data Protection Agency' (*Croatian Personal Data Protection Agency, 2 December 2018*) <https://azop.hr/about-the-agency/> accessed 18 June 2022
6. 'Contribution of the EDPB to the evaluation of the GDPR under Article 97' (*European Data Protection Board,* 18 February 2020) <https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en> accessed 25 May 2022
7. 'Handbook on European data protection law' (*European Union Agency for Fundamental Rights and Council of Europe,* 25 May 2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 23 May 2022
8. 'What is SME?' (European Commission, 8 September 2020) <https://ec.europa.eu/growth/smes/sme-definition_en> accessed 6 June 2022
9. Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (*European Data Protection Supervisor,* 15 September 2014) <https://edps.europa.eu/sites/default/files/publication/14-09-15_article_eui_en.pdf> accessed 23 May 2022
10. 'The Standard Data Protection Model: A method for Data Protection advising and controlling on the basis of uniform protection goals' (*AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder,* 17 April 2020*)* <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf> accessed 23 May 2022
11. 'DLA Piper GDPR Fines and Data Breach Survey: January 2023' (*DLA Piper*, 25 January 2023) <https://www.dlapiper.com/en-ae/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023> accessed 18 June 2022
12. 'What if my company/organisation fails to comply with the data protection rules?' (*European Commission,* 25 May 2018) <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/ what-if-my-companyorganisation-fails-comply-data-protection-rules_en> accessed 18 June 2022
13. Barnard-Wills D, Cochrane L, Mattur K, Waterford F, Marchetti F, 'Report on the SME experience of the GDPR' <https://star-project-2.eu/wp-content/uploads/2021/02/STARII-D-2.2-Report-on-the-SME-experience-of-the-GDPR.pdf>accessed 18 March 2023
14. 'SME research' (*Information Commissioner's Office, SME research,* April 2021) https://ico.org.uk/media/about-the-ico/documents/4024787/ico-sme-research-2021.pdf accessed 18 March 2023
15. 'Guidelines, Recommendations, Best Practices' (*European Data Protection Board*) <https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en> accessed 18 March 2023

16. 'How well do you comply with data protection law: an assessment for small business owners and sole traders' *(Information Commissioner's Office,* April 2019*)* <https://ico.org.uk/for-organisations/sme-web-hub/checklists/assessment-for-small-business-owners-and-sole-traders/> accessed 18 March 2023
17. 'Guidance for SMEs' *(Data Protection Commission Ireland,* July 2019*)* <https://www.dataprotection.ie/en/dpc-guidance/guidance-smes> accessed 18 March 2023
18. 'Facilita RGPD' *(Spanish Personal Data Protection Agency,* May 2019*)* <https://www.aepd.es/en/guides-and-tools/tools/facilita-rgpd> accessed 18 March 2023
19. 'Guidelines, Recommendations, Best Practices' (*European Data Protection Board,* 10 October 2022) <https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en> accessed 20 October 2022
20. 'Objectives of ARC project' *(Awareness Campaign for SMEs,* 20 September 2020*)* <https://arc-rec-project.eu/objectives/> accessed 18 June 2022

*Anamarija Mladinić**
*Zdravko Vukić***
*Ante Rončević****

IZAZOVI S KOJIMA SE SUOČAVAJU MALI I SREDNJI PODUZETNICI PRI IMPLEMENTACIJI OPĆE UREDBE O ZAŠTITI PODATAKA

Sažetak

Opća uredba o zaštiti podataka (EU) 2016/679 koja se jedinstveno primjenjuje od 25. svibnja 2018. u Europskom gospodarskom prostoru (EGP) zahtijeva od malih i srednjih poduzeća da poštuju pravo na zaštitu osobnih podataka svojih klijenata, kupaca i zaposlenika. Opća uredba o zaštiti podataka osmišljena je kako bi ojačala pravo na zaštitu podataka svih pojedinaca unutar EGP-a, a ujedno olakšala prekogranični protok osobnih podataka i potaknula razvoj digitalne ekonomije. Opća uredba o zaštiti podataka u punoj je primjeni više od četiri godine, ali i dalje predstavlja problem za hrvatska mala i srednja poduzeća, kojima za razliku od većih tvrtki, vrlo često nedostaju ljudski i financijski resursi za usklađivanje s pravnim okvirom zaštite podataka. Ovaj rad obuhvaća teorijska razmatranja i rezultate *online* ankete provedene među 345 malih i srednjih poduzeća u Republici Hrvatskoj sa svrhom dobivanja uvida u izazove s kojima se suočavaju pri usklađivanju s Općom uredbom o zaštiti podataka. Rezultati istraživanja pokazali su da razumijevanje obveza koje proizlaze iz Opće uredbe o zaštiti podataka i usklađenost s pravnim okvirom zaštite podataka među hrvatskim malim i srednjim poduzećima nije na zadovoljavajućoj razini.

Ključne riječi: *usklađenost, hrvatski mali i srednji poduzetnici, nadzorna tijela za zaštitu podataka, Opća uredba o zaštiti podataka, zaštita osobnih podataka*

* Anamarija Mladinić, načelnica sektora za EU, međunarodnu suradnju i pravne poslove, Agencija za zaštitu osobnih podataka Republike Hrvatske, Selska cesta 136, 10 000 Zagreb. E-adresa: anamarija.mladinic@azop.hr. ORCID: https://orcid.org/0009-0009-2597-7348.

** Zdravko Vukić, univ. mag. oec., ravnatelj Agencije za zaštitu osobnih podataka Republike Hrvatske, Selska cesta 136, 10 000 Zagreb. E-adresa: zdravko.vukic@azop.hr. ORCID: https://orcid.org/0009-0003-9942-7791.

*** Dr. sc. Ante Rončević, redoviti profesor Sveučilišta Sjever, Trg dr. Žarka Dolinara 1, 48000 Koprivnica. E-adresa: aroncevic@unin.hr. ORCID: https://orcid.org/0000-0003-2527-9506.