REVIEW ARTICLE ADRS
Ann. Disaster Risk Sci. 2018, 2, 105-116

GDPR – IMPACT OF GENERAL DATA PROTECTION REGULATION ON DIGITAL MARKETING

Natalija Parlov[1], Željko Sičaja[2], Tihomir Katulić[3]

[1]Parlov Digital Intelligence Ltd; Apicura Business Intelligence Ltd

[2]Republic of Croatia, Ministry of Interior

[3]University of Zagreb, Faculty of Law

Abstract

Due to the rapid development of technology, in the last ten years digital marketing has given rise to sophisticated automated models for successfully affecting the behaviour of consumers whose fundamental rights, such as the right to privacy and the right to the protection of personal data, have often been violated because of the discrepancy between the regulations and the actual use of personal data.

The possibility of targeting has been brought to an enviable level – a precise targeting of an identified individual and his or her personal data, as well as their complete demographic, sociographic and psychographic profile – thus opening the doors to the possibility of making precise predictive analyses and the placement of behavioural strategies by combining various digital channels in creating communication messages of inducement to purchase and continuous monitoring of an individual and their habits.

On the other side, information security is a term which all parties in the marketing world involved in the provision of technological services directed towards automated use for marketing purposes, i.e. third-party-side tools with the goal of collecting data, shy away from.

The goal of the *General Data Protection Regulation* is the protection of personal data, primarily the right to privacy in the digital age. The Regulation will strongly influence the current modalities of using digital marketing.

This study was carried out by the authors on 233 small and medium entrepreneurs in the Republic of Croatia on the use of marketing modalities and tools to collect data about target individuals. It has shown that through digital marketing, the companies collect not only the information about their consumers' preferences, but their *a priori* goal is the concrete identification of an individual for the purpose of reducing the costs of marketing activities, directing customized communication to a target individual and creating a quick return on a marketing investment by raising sales – at the same time without any special sensitivity regarding the protection of the individual's rights and their personal data.

The aim of the paper is the identification of the most frequent methods and tactics of digital marketing and their non-compliance with the *General Data Protection Regulation* which comes into force at the end of May this year.

Keywords: GDPR, *General Data Protection Regulation*, personal data, digital marketing, consumer protection

Address for correspondence: Natalija Parlov, Parlov Digital Intelligence Ltd; Apicura Business Intelligence Ltd, Zagreb, Croatia, e-mail: una@parlov.hr

1. INTRODUCTION

The new European General Data Protection Regulation, GDPR, has been adopted in order to strengthen the rights of data subjects and enhance the obligations and responsibilities of those who collect, process and store personal data. With its provisions, the GDPR has also defined and harmonised rules for personal data protection, as well as sanctions for breaches of the regulations in all member states.

The development of modern technologies has enabled the collection of information from any field in a matter of seconds. The collection and processing of different information and data in everyday business has never been more necessary and desirable. Information and data have become a form of business capital (Nikolić, Sičaja, & Parlov, 2018).

A large part of GDPR provisions is inter-

twined with the sector of information security. For years experts from this sector have been trying to point to the obsolescence of the personal data protection regulations. Thanks to the GDPR, even the information security sector will now have to take into account the personal data component in the design and planning of new projects. This will certainly have a positive effect on the market in this sector because new jobs will be created and clients who order services from this market will be able to define their needs more clearly and precisely.

The adoption of this regulation has therefore brought about a positive shock in the information security sector because businesses expect that information security experts will help them and prepare them for the beginning of the application of the GDPR.

Marketing strategies in the digital media, with a special focus on social networks, include strategic communication plans with clearly differentiated channels of message distribution which also include the micro-level distinction in defining communication goals and modalities, i.e. the distinction of communication based on the specific social network on which a message will be placed. The same message is transferred through seemingly similar channels, but sometimes in an entirely different way, depending on the target group of users of a certain social network (Parlov & Sičaja, 2017).

A steady trend of investment growth can be clearly observed by virtue of the characteristics of contemporary media. Digital marketing strategies include a choice of the appropriate means of digital marketing through one of the available digital channels (Chaffey and Smith, 2008). Some of the characteristics are adjustability, freedom of choice, user control, cost reduction, and most importantly, interactivity. Digital marketing relies on Internet technology and the unique characteristics of the digital environment, but the characteristic pointed out by all authors as the crucial one is the possibility of interaction with the potential buyer (Parlov, Perkov, & Sičaja, 2017). Interactivity affects performance quality, motivation, the sense of fun, cognitive abilities, learning, normativity and sociability. McMillan (2002) notes that interactivity affects one's attitude towards websites, the relevance of topics on a website, the rate of return to a website, referring others to a website and buying from a website. Interactivity also has an effect on the better processing of information about a web offer and about the product itself (Sicilia, Ruiz, & Munuera, 2005).

Professional literature states that interactivity lies in the process or characteristics of a communication medium. Based on the definition, Masi and Levi (according to Heeter, 1989) carried out a study of the presence of interactive characteristics on websites, such as e-mail links, comment forms, search forms, registration forms, on-line ordering, games, surveys, etc. (Heeter, 1989). All researchers operationalised their studies under the assumption that the interactivity of communication grows with the number of web communication characteristics. The characteristics themselves can be divided into those that enable bidirectionality and those that enable control.

2. AIM AND METHODOLOGY

The aim of this paper is to identify the most common methods and tactics of digital marketing and their non-conformity with the General Data Protection Regulation, whose application starts at the end of May 2018. The methodology used is quantitative and deductive analysis, as well as discourse analysis with a sampling and interpretation of the traceability of the results.

3. WHY THE GENERAL REGULATION?

The General Data Protection Regulation is the new European general regulation which lays down the rules for personal data pro-

tection and attitude towards the protection of the individual in terms of using the individual's personal data in a specific business process. Furthermore, this regulation protects the individual's fundamental rights and freedoms, especially the right to the protection of personal data. With the application of the GDPR, a great change in the approach to the protection of personal data will take place through technological changes in the IT and information security sector, as well as through the organization of business within a company and the training of employees (Nikolić, Sičaja, & Parlov, 2018).

The Regulation was adopted with the goal of a consistent protection of individuals in the entire EU area and in order to harmonise the criteria and the degree of personal data protection. There have also been changes in the exchange and free movement of personal data on the internal market because the Regulation represents an effort to equalize the regulation and practice of personal data protection in the EU member states and it indirectly enables greater legal security for business operators, including microenterprises, small and medium-sized enterprises. Thanks to the GDPR, individuals in all member states now have the same degree of rights and obligations, and the regulation also clearly defines the responsibilities of controllers and processors. Furthermore, the provisions of the Regulation also define the appropriate monitoring of the processing of personal data, equivalent sanctions in all member states and the cooperation between the supervisory authorities of member states (GDPR Regulation EU 2016/679)

The GDPR has also defined the protection of the individual on the technological level which should be compliant with GDPR's principles in the processing of personal data. This primarily refers to the processing of personal data by automated means, but also manual processing, if the personal data are stored in another form in the storage system.

"The principles of data protection should apply to any information concerning an identified or identifiable natural person" (GDPR Regulation EU 2016/679). Pseudonymised personal data are included here, since the holder of personal data can be identified with an appropriate pseudonym register. The principles of data protection do not apply to anonymised data, i.e. data that cannot identify an individual directly or indirectly.

Requests to disclose personal data sent by public authorities for the purpose of carrying out their official tasks should always be submitted in written form, reasoned and submitted sporadically, and they should not refer to the entire storage system ("The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing". (GDPR Regulation EU 2016/679).

At the time of writing this paper, the valid legal framework in the Republic of Croatia, apart from the basic provisions from Article 37 of the Constitution, was contained in the rules of the Act on Personal Data Protection as a transposition of EU Directive 95/46/EC on Data Protection from 1995, but with the start of the application of the GDPR, the new general framework consists of the General Data Protection Regulation, Act on the Implementation of the General Data Protection Regulation and special sector regulations on the specific rules for collecting and processing personal data. These special regulations include the Act on Medicinal Products, Act on Pharmaceuticals, Clinical Trial and Good Clinical Practice Code, Act on Catering Industry, Act on Consumer Protection, etc.

4. GDPR AND INFORMATION SECURITY

Considering the fact that the European Directive on Data Protection which regulated the area of personal data was adopted back in 1995 and that information technology and its

use has significantly changed since then, the European legislator decided to significantly improve and modernize the legal framework for personal data protection from the perspective of ensuring the protection of personal data as a fundamental right of individuals in the EU area, but also from the perspective of the emergence of a common digital market and the free data flow in the internal market (Katulić & Vojković, 2016).

Modern business is unimaginable without information technology which is integrated into every pore of everyday life. The exchange of personal data represented a problem in conducting everyday business between business operators in the EU. This happened due to the different national implementations of the GDPR, the consequently different legislative practice of member states, the practice of national regulatory bodies, and finally the disparities in the policies of personal data security and information security among the member states. The General Regulation must be implemented equally in the entire EU area and thus ensure a higher level of the data subjects' legal security and data protection.

The Regulation will surely have a big effect on the information security sector. Companies dealing with information security and based in the EU will be focused on defining their products anew, as well as their implementation strategies and the education of employees. GDPR contains numerous concepts and ideas which have for decades been recognized by the industry as good information security practice. According to Klaić (2006), data classification itself and intellectual property in a wider sense, with defined rights of access to these same data, are the prime characteristics of the contemporary information space in the segment of information security.

Information security and the protection of personal data are closely related, which implies that information security as such is becoming a value that is also protected by general provisions in other areas (ISO, 2016).

Before the GDPR, security products were focused on security, but this did not always mean that the design of certain security policies took the individual's rights into account. GDPR's provisions now have to be a mandatory part of all segments of information security, starting from defining projects to defining the policies of clients' privacy. The existing documents will have to be revised and updated in accordance with the Regulation. Information security consultants will be required to understand GDPR and how to implement it in practice for their existing and potential clients (PMI, 2004).

Experts and consultants working at the international level will have to be able to help clients to adapt to the Regulation. Since information is an asset, it is becoming crucial for decision-making in business processes, and information security experts will among other things have to be able to define the policies of clients' privacy in order to stay competitive. The function of Data Protection Officers (DPO's) is redefined with the GDPR. There is a large demand for experts who will be able to perform this task, and according to available data, many jobs will be created, which can mean several tens of thousands of new employment positions on the EU level. Europe will not be able to fill these positions in time, primarily because of the lack of sufficiently qualified experts for this role. Precisely here lies the chance for information security experts because they have the basic qualifications to perform this task and they are in a position in which clients will be able to hire them. Namely, GDPR requires a stronger emphasis on privacy and the appointment and training of an employee to fill the role of the DPO.

The term "information assurance" is increasingly used as an alternative term for information security, primarily because of the broad meaning of the word "security" (Legal Information Institute, 2003). In this sense, information assurance is the interaction between technology ensuring the conditions of secu-

rity, the processes which strengthen the effects of technology and the people who enable the functioning of technology in operative use (Brotby & Krag, 2009).

5. DATA SUBJECTS' RIGHTS

The beginning of the implementation of the GDPR from the perspective of marketing strategies will have a strong influence on the effect of campaigns because the modalities of direct marketing and profiling will not be as expansive as before, and with it the key success factors will have to be redefined. The GDPR has strictly defined the rights of consumers, i.e. data subjects, and prescribed new responsibilities for all controllers, i.e. persons in charge of collecting, processing and archiving collected personal data of existing or potential customers. In that sense the data controller does not have the possibility to create and automatically process subjects' profiles without their explicit consent.

Right to processing information and access to personal data

Transparency is one of the key principles of the GDPR. Controllers are also bound by the Regulation to clearly and in simple terms inform the data subject or individual in what way the processing of their personal data is carried out.

According to Recital 60 of the Regulation, "the controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling".

The right to information provides access to the identity and contact information of the controller, the contact information of the data protection officer, the goal of processing and the legal grounds for the processing, the legitimate interests of the controller or third party, the personal data recipients or categories of recipients, etc.

According to Article 15 of the Regulation, the data subject has the right to receive information about any piece of personal data used for profiling and the creation of the subject's profile. The controller must also enable the data subject access to the created profile and explain to the data subject for what purpose the data is used. This part does not refer to the right to data portability when the controller is required to provide the data subject only with the collected data and not the created profiles. According to Recital 63 of the GDPR, the collector is protected from allowing the data subject access to created profiles in cases related to trade secrets or intellectual property. In this case it is prescribed that "that right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data".

The right of access to data provides the data subject the possibility to receive appropriate confirmation from the controller if the personal data concerning him or her are being processed, and if they are, the data subject must be provided access to them.

Right to rectification

The right to rectification provides the data subject the right to secure the rectification of inaccurate personal data referring to him or her from the collector without undue delay. Taking into account the purpose of processing, the data subject has the right to supplement the incomplete personal data, including by giving an additional statement.

Right to erasure

The right to erasure or the right to be forgotten provides the data subject with the right to

secure the erasure of personal data referring to him or her without undue delay. The collector is required to erase the personal data without undue delay.

Right to restrict processing

The right to restrict processing provides the data subject the right to secure a restriction of processing from the controller. If the processing is restricted, such personal data may be processed only with the data subject's consent, excluding storage, or for the establishment, exercise or defence of legal claims, or the protection of the rights of another natural or legal person, or for an important public interest of the EU or member state.

Right to data portability

The right to data portability provides the data subject the right to receive personal data concerning him or her and which have been provided by the controller in a structured, commonly used and machine-readable format and the right to transfer these data to another controller without interference from the controller to whom the personal data were given.

Right to object

According to Article 21(1) and (2) of the GDPR, the controller must enable the data subject to object and present the right to the data subject clearly and unambiguously. Controllers are specially required to provide this right if processing is carried out based on the provisions of Article 6 of the Regulation[1]. When the data subject exercises this right, the controller must immediately stop the profiling, unless the controller demonstrates a legitimate interest[2]. The GDPR does not explain or exactly prescribe how legitimate interest is demonstrated. In this case a proportionality test is carried out between the controller's business interest and the data subject's possible objection to processing. In carrying out the test, the controller must not only state a legitimate interest, but it has to be compelling and demonstrate a higher business interest. Article 21(2) provides the data subject the unconditional right to object to data processing for the purpose of direct marketing and profiling for the same purpose. According to Recital 70 of the GDPR, "Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information".

The right to object provides the data subject with the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her. The controller may not process personal data anymore, unless he or she can demonstrate compelling legitimate grounds for the processing.

Right to exemption of legal decisions during automated decision-making and profiling

The right to exemption from legal decisions during automated decision-making and profiling provides the data subject with the right

1 Article 6 of the GDPR, points: (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2 Recital 47 of the GDPR - The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

to request exemption from a decision based exclusively on automated processing, including profiling, which produces legal effects that concern him or her or significantly affect him or her in a similar way (EU Commission, 2016).

6. CONSENT FOR MARKETING PURPOSES

Article 4(11) defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 29 Working Party, 2016).

The basic concept of consent remains the same as in Directive 95/46/EC and thereby consent is the basic legal ground on which personal data may be processed, pursuant to Article 6 of the GDPR. Apart from that, the above definition of consent is supplemented with the provisions of Article 7 of the GDPR and recitals 32, 33, 42 and 43 as to how the controller must define the basic elements of consent. Furthermore, particular interpretations and recitals of the GDPR provide the data subject the right to withdraw consent an unlimited number of times, which depends solely upon himself or herself.

Valid consent in the sense of Article 4(11) must be given freely, it has to be specific, informing and clear, unambiguous for the data subject regarding how and in what way his or her personal data will be processed and used.

The "freely given" characteristic implies that the data subject has given his or her consent by his own free will and independently. The main rule stipulated by the Regulation and which must be taken into account if consent is to be regarded as freely given is that no conditions for the use of a service are set out and that the use of a service is not conditional upon consenting to provide personal data. If the provider of a service makes the use of a service conditional upon consenting to provide personal data, then the consent is not freely given. Apart from the guidelines of the Working Group from Article 29, various guides from national supervisory authorities are also available dealing with the nature of consent. The opinion (guide) of the British supervisory authority Information Commissioner's Office on the nature of consent is interesting and practical in this sense (ICO, 2018).

According to the mentioned sources, it can be concluded that according to the GDPR adequate consent must be particular (granular), unconditional, communicated in plain language, unambiguous and informed.

- Silence, a pre-checked box or a lack of activity should thus not be considered as consent.
- Consent should cover all processing activities carried out for the same purpose.
- Processing should be connected to consent.
- The data subject has the right to withdraw his or her consent at any time.
- Processing should be connected to the validity of consent (has the consent been withdrawn?).

Conditions for consent – when processing is carried out on the grounds of consent, the collector must be able to prove that the data subject has given his or her consent for the processing of his or her personal data. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract,

including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

According to the Act on the Implementation of the General Data Protection Regulation of the Republic of Croatia, consent to the processing of personal data given by a child is lawful if the child is at least 16 years old. If the child is under the age limit of 16, such processing is lawful only if and to the extent that the consent was given or approved by the holder of parental responsibility over the child.

7. RESEARCH RESULTS

The research carried out by the authors on 233 small and medium-sized enterprises in the Republic of Croatia on the use of marketing modalities and tools for the purpose of collecting data on target individuals has shown that the companies do not use digital marketing only to collect information about their consumers' preferences, but that their *a priori* goal is the concrete identification of an individual for the purpose of reducing the costs of marketing activities, directing tailor-made communication towards a target individual and creating a fast return of the marketing investment through the increase of sales – at the same time without a particular sensitivity to the protection of the individual's rights and personal data.

For the purpose of this paper, the authors conducted a digital survey over a period of 60 days, ending on 15 March 2018. The survey questions included a general understanding of the GDPR and the scope of the company's digital business with specific questions about the concrete use of direct and interactive marketing methods with the collection and classification of the target group's personal data with the goal of increasing sales.

The survey was completed by 233 respondents of which 220 or 94.42% are micro and small entrepreneurs, while 13 or 5.58% are medium-sized entrepreneurs. There were no large entrepreneurs among the respondents *(chart 1)*.

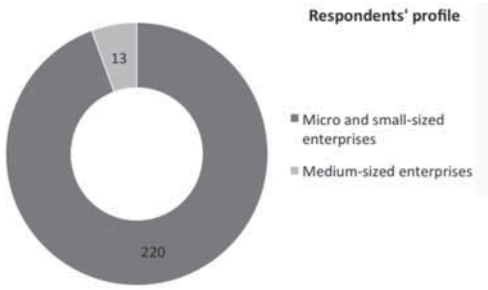

Chart 1. Respondents' profile

Source: authors

Considering the fact that the Regulation comes into force on 25 May 2018, the general awareness of Croatian companies about the GDPR is devastatingly low, i.e. 61% of the companies are not familiar with GDPR, while 39% of them know what GDPR is *(chart 2)*.

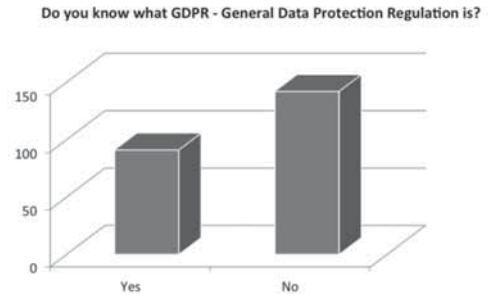

Chart 2. Awareness of GDPR – General Data Protection Regulation

Source: authors

Using direct marketing in business is very common and the respondents use it in almost 90% cases, i.e. 207 respondents use it, while around 10% or 26 of the respondents do not use direct marketing or do not know what it is *(chart 3)*.

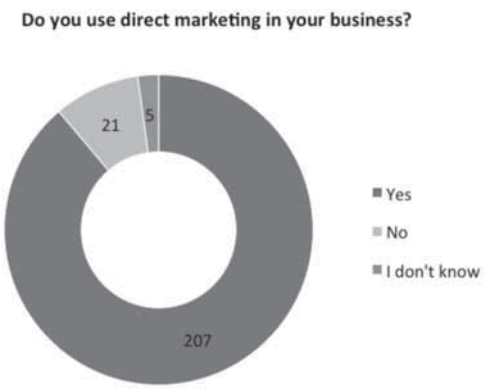

Chart 3. Using direct marketing in business

Source: authors

Out of the most commonly used direct marketing methods, around 80%or 185 respondents use the newsletter system, around 15% or 32 respondents use telephone calls as the direct marketing model, 6% or 15 respondents use contact in person, while 27% of them, i.e. 64 respondents, frequently make personal contacts for the purpose of promoting their business on social networks *(chart 4)*.

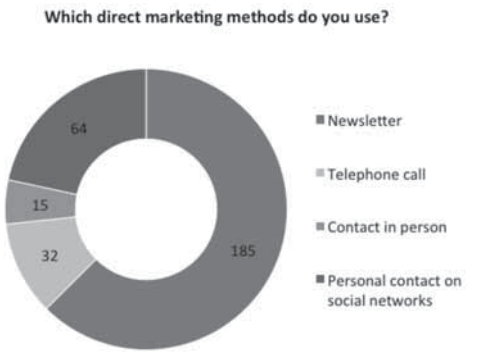

Chart 4. Frequency of using particular types of direct marketing per method of choice

Source: authors

Digital marketing campaigns are used by 97% or 226 respondents, while 3% or 7 respondents do not use them. No respondent stated that they did not know what a digital marketing campaign was *(chart 5.)*

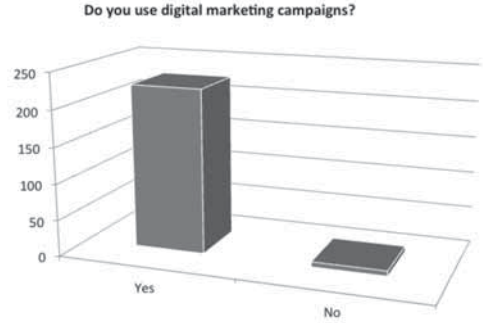

Chart 5. Use of digital marketing campaigns

Source: authors

The choice of communication channels is of crucial importance for the success of reaching the target group. Around 80% of the respondents, i.e. 185 of them, stated that they used newsletter systems as the most common channel for communicating with potential buyers; social networks with the options of Facebook Ads and Instagram Ads turned on are used by 60% of the respondents, i.e. 143 of them, while 30% or 68 of the respondents use Google AdWords. Only around 20% or 48 respondents use media portals for marketing placements. Two per cent or 4 respondents use SMS as a direct marketing model in digital marketing campaigns *(chart 6.)*

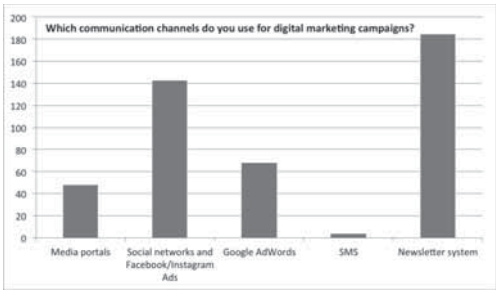

Chart 6. Choice of communication channels when using digital marketing campaigns

Source: authors

Prize competitions in communication messages are an extremely attractive channel for personal data collection for the purpose of direct marketing and 50% or 117 of the respondents use this modality for growing their database with potential buyers, while 30% or 78 of the respondents do not use it and 7 respondents do not know if they use it *(chart 7)*.

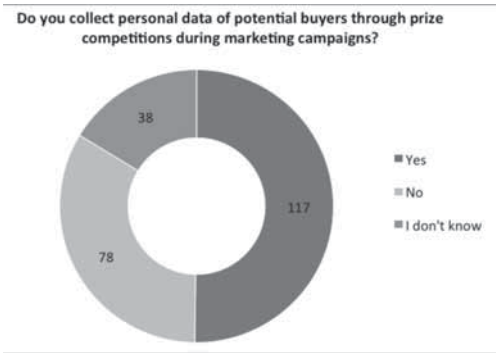

Chart 7. Collection of personal data when using prize competition marketing methods

Source: authors

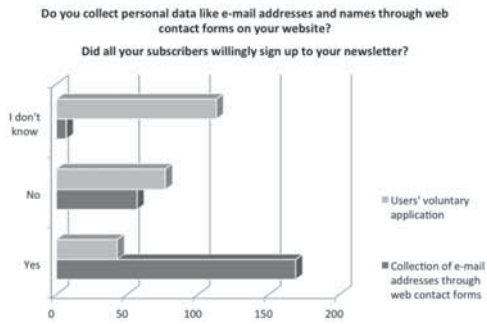

Chart 8. Relationship between the awareness of personal data collection and processing and the perception between using the option of willing user subscription to the newsletter in relation to collecting e-mail addresses through contact forms

Source: authors

In the relationship between the awareness of personal data collection and processing and the perception between using the option of users' voluntary subscription to newsletters in relation to collecting e-mail addresses through contact forms, there is a noticeable gap between understanding the collection of personal data from one's own web contact form and a certain degree of ignorance about the personal will of the newsletter subscriber to appear on the subscription list, and particularly noticeable is the finding that businesses which use direct newsletter marketing are aware that subscribers are not in their databases willingly.

Around 75% of the respondents, i.e. 169 of them, responded that they collected personal data such as e-mail addresses and names through web contact forms on their websites, while 25% or 57 of the respondents said they did not do that. Seven respondents did not know if they collected personal data in this way. Regarding the voluntary subscription to newsletters, around 20% of the respondents think that their users subscribed voluntarily, but more than 30% of them or 77 respondents are aware that the subscribers did not apply willingly, which implies that the subscribers have found themselves on the subscription lists in a way that is not legitimate. As many as around 50% or 113 respondents do not know if the subscribers signed up to their newsletter willingly *(chart 8)*.

8. CONCLUSION

Due to the rapid development of technology, in the past ten years digital marketing has given rise to sophisticated automated models for successfully affecting the behaviour of consumers whose fundamental rights, such as the right to privacy and the right to the protection of personal data, have often been violated because of the discrepancy between the regulations and the actual use of personal data.

Business operators are not prepared for the new European regulation in the field of personal data protection and the new higher standards of protection, nor are they aware of the rights their users have. The collection and processing of buyers' personal data without defining a transparent and unambiguous purpose, if they are not regulated by another law, will no longer be possible for marketing purposes in the ways that have so far been the most common and most favourable with regards to costs, with targeting a specific individual and his or her personal preferences without his or her consent.

Research has clearly shown that companies have not so far been particularly sensitive to the collection, processing and archiving of personal data and that the start of the imple-

mentation of the GDPR can cause great restrictions in the most commonly used marketing modalities and tactics of placement planning.

In general, the purpose of the General Data Protection Regulation is to ensure the adequate level of protection of individuals' rights with regards to personal data processing. Data subjects' rights which were implicit in the preceding legal framework are now clearly defined by the Regulation. In this sense, we can call the Regulation a milestone in the context of digital marketing, since the focus is back on the position of data subjects which influences the modality of using technologically highly advanced ways of marketing processing from the perspective of personal data protection.

REFERENCES

Act on the Implementation of the General Data Protection Regulation, Article 19, Official Gazette 42/2018. Retrieved from https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html. Accessed on 18 May 2018.

Article 29 Working Party Guidelines on consent under Regulation 2016/679. Retrieved from https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf. Accessed on 21 March 2018.

Brotby, W. Krag (2009). Information security management metrics. Auerbach Publications.

Chaffey D., Smith PR (2008). Emarketing excellence: planning and optimizing your digital marketing, 3rd edition, Oxford: Butterworth-Heinemann, Elsevier.

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018. Retrieved from http://ec.europa.eu/justice/data-protection/index_en.htm 17/EN WP251rev.01. Accessed on 21 March 2018.

Heeter, C. (1989). Implications of new interactive technologies for conceptualizing communication. Salvaggio J., Bryant J. (eds.) in Media Use in the Information Age: Emerging Patterns of Adoption and Consumer Use. Lawrence Erlbaum Associates, pp.217-235.

ICO. Information Commissioner's Office. Retrieved from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/. Accessed on 18 May 2018

Katulić, T., Vojković, G. (2016). From Safe Harbour to European Data Protection Reform, MIPRO ISS, Opatija 2016, pp. 1694-1698.

Klaić, A., (2006). Information security requirements in the information systems planning process. 17th IIS Conference, FOI, Varaždin, pp. 265-269.

Law on Implementation of the Regulation(EU) 2016/679 of the European Parliament and of the Council – General Data Protection Regulation (OG 42/2018)

Lewis, B. (2017). International Organization for Standardization; Information Security Management System auditors welcome ISO/IEC 27007 publication. Retrieved December 5, 2017, from https://www.iso.org/news/ref2232.html

McMillan, S. J., Downes, E. J. (2000). Defining interactivity: a qualitative identification of key dimensions. New Media & Society, Vol 2 No 2, pp 157–179.

Nikolić, G., Sičaja, Ž., Parlov, N. (2018). GDPR – analiza pripremljenosti malih i srednjih poduzeća na novu europsku regulativu i njezin utjecaj na poslovanje u budućnosti. PAR International Leadership Conference Proceedings. ISBN: 978-953-59508-20-0.

Parlov, N., Perkov, D., Sičaja, Ž. (2016). New trends in tourism destination branding by means of digital marketing. Acta Economica Et Turistica, 2(2). doi:10.1515/aet-2016-0012

Parlov, N., Sičaja, Ž. (2017). Utjecaj društvenih mreža na porast posjećenosti web stranica u turizmu. Tourism and Development 2017 Conference Proceedings, University of Maribor Press, doi: doi.org/10.186907978-961-286-121.6

PMI, (2004). A Guide to the Project Management Body of Knowledge, 3rd Ed., Project Management Institute.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR), (2016). European Parliament and European Council. Retrieved from http://data.europa.eu/eli/reg/2016/679/oj

Sicilia, M., Ruiz, S., Munuera, J. L. (2005). Effects of Interactivity in a Web Site: The Moderating Effect of Need for Cognition. Journal of Advertising, Vol 34 No 3, pp 31–45.

U.S. Government, Legal Information Institute, Title 44, Chapter 35, Subchapter 111, §3542, Cornell University Law School. Accessed on 21 March 2018, URL: www.law.cornell.edu/uscode/44/3542.html

GDPR – UTJECAJ OPĆE UREDBE O ZAŠTITI OSOBNIH PODATAKA NA DIGITALNI MARKETING

Sažetak:
Digitalni marketing je tijekom zadnjih desetak godina uslijed ubrzanog tehnološkog razvoja iznjedrio sofisticirane automatizirane modele uspješnog utjecaja na ponašanje potrošača kojima su zbog raskoraka u regulaciji i stvarnosti uporabe osobnih podataka često bivala povrijeđena temeljna prava poput prava na privatnost i prava na zaštitu osobnih podataka.
Mogućnost targetiranja, odnosno ciljanja dovedena je na zavidnu razinu – precizno ciljajući identificiranog pojedinca i njegove osobne podatke te kompletnu demografiju, sociografiju i psihografiju - otvarajući time vrata mogućnosti preciznih prediktivnih analiza i plasmana bihevioralnih strategija kombiniranjem različitih digitalnih kanala u kreiranju komunikacijskih poruka poticanja na kupnju te kontinuiranog praćenja pojedinca i njegovih navika.
Informacijska sigurnost, s druge strane, u marketinškom svijetu pojam je od kojeg zaziru sve strane uključene u pružanje tehnoloških usluga usmjerenih automatiziranoj uporabi u marketinške svrhe, odnosno third-party-side alati s ciljem prikupljanja podataka.
Svrha Opće uredbe o zaštiti podataka je zaštita osobnih podataka i prvenstveno prava na privatnost u digitalno doba te će snažno utjecati na dosadašnje modalitete korištenja digtalnog marketinga. Istraživanje koje su proveli autori na 233 mala i srednja poduzenika u Republici Hrvatskoj o korištenju marketinških modaliteta i alata u svrhu prikupljanja podtaka o ciljanim pojedincima pokazalo je da tvrtke digitalnim marketingom ne prikupljaju samo informacije o preferencijama svojih potrošača, već im je a priori cilj konkretna identifikacija pojedinca u svrhu smanjenja troškova marketinških aktivnosti, usmjeravanje prilagođene komunikacije na ciljanog pojedinca te stvaranje brzog povrata marketinške investicije podizanjem prodaje - istovremeno bez posebne osjetljivosti na zaštitu prava pojedinca i njegovih osobnih podataka.
Cilj rada je identifikacija najčešćih metoda i taktika digitalnog marketinga te njihovih nesukladnosti s Općom uredbom o zaštiti osobnih podataka koja stupa na snagu krajem svibnja ove godine.
Ključne riječi: GDPR, Opća uredba o zaštiti osobnih podataka, osobni podaci, digitalni marketing, zaštita potrošača