MIND JOURNAL https://doi.org/10.36228/MJ.15/2023.2 15/2023
Received: 17.05.2023 Accepted: 05.06.2023

Ihor Oklander, Ph.D. in Economics, Senior Lecture of the Department of Management and Marketing, Odessa State Academy of Civil Engineering and Architecture (Odessa, Ukraine)

DATA PROTECTION IN DIGITAL MARKETING

Abstract. *The article states that digital marketing is encompassing more and more areas of activity, and the matter of its legal support is being addressed. It discusses the key provisions of the General Data Protection Regulation (GDPR), which outline the process of handling personal data by legal entities. The article highlights the principles underlying the GDPR and emphasizes the categorical framework for collecting and storing personal data. It also examines the significance of safeguarding personal data when employing targeting strategies. Lastly, the article provides recommendations for implementing the General Data Protection Regulation within the marketing system of an enterprise.*

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

Introduction. Marketing is the science of winning in competitive battles. The goal of marketing is to ensure consumer satisfaction and, as a result, achieve maximum profitability.

Digital marketing is marketing that utilizes digital channels to attract and retain customers. Often, the term "digital marketing" is equated with "internet marketing," marketing on the internet. However, this is incorrect. These concepts are significantly different. They relate to each other as categories of dialectics – part and whole. Internet marketing is a part. The whole thing is digital marketing. Digital marketing includes internet marketing but is not limited to the internet. For example, internet marketing involves website SEO, contextual advertising, webinars, etc. – all channels that are accessible to users only on the internet. On the other hand, digital marketing encompasses internet marketing plus advertising and promotion on any digital media outside the internet. In other words, digital marketing implies digital communication that takes place both online and offline.

Types of digital marketing channels: SMS and MMS messaging; advertising on interactive and outdoor LED screens, self-service terminals; SEO (search engine optimization); contextual advertising; SMM (social media marketing); email marketing; advertising in apps, messengers, online games [Natorina, A., 2019].

Trends in digital marketing: video analytics on TikTok, YouTube, other social media platforms; measuring consumer engagement using machine learning; utilizing machine learning for predictive analysis; voice SEO optimization. Another trend is the use of the concept of the "Metaverse" [Chaikovska M.P., 2021].

Mark Zuckerberg defines the Metaverse as "an internet that you're inside of rather than just looking at," essentially a virtual space. It signifies the evolution of the internet into a unified virtual world accessed through virtual and augmented reality technologies. In other words, the Metaverse is a series of 3D worlds, similar to those found in computer games, where social interactions can occur on the internet. The Metaverse is not just a short-lived trend; it is the platform of the future, a new step in the era of the internet. As a new virtual world, the Metaverse holds the potential for the emergence of new forms of digital marketing. As digital marketing continues to encompass more areas of activity, the question of its legal framework becomes relevant [Sadchenko O.V., Robul I.V., 2020].

Research results. The European Union (EU) systematically works on the protection of personal data. Personal data refers to information about an individual that can directly or indirectly identify them.

Examples of general personal data include name, address, phone number, date and place of birth, passport information, and workplace and/or educational details.

Personal data on the internet includes email addresses, metadata (cookies), social media accounts and positions held on them, and IP addresses.

On April 27, 2016, the European Union (EU) adopted the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, replacing the Data Protection Directive of 1995. Unlike the directive, the GDPR does not require any changes in the domestic legislation of EU member states and is directly binding. Non-compliance with the law can result in fines of up to €20 million or up to 4% of the company's annual global turnover, whichever is higher, based on the previous financial year [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016].

This regulation defines the rules for processing personal data by legal entities. If a legal entity sells goods or provides services to EU citizens, or employs them, it must comply with the requirements of the GDPR.

The GDPR aims to give individuals control over their personal data and to simplify the regulatory framework for international economic relations by unifying regulations within the EU.

The GDPR is based on the following principles:

- Lawfulness, fairness, and transparency: Personal data collection is carried out on legal grounds, and its use requires transparency, with each party fulfilling their obligations.
- Purpose limitation: Personal data is collected for specified and legitimate purposes as stated in the privacy policy.
- Data minimization: Personal data is collected in the minimum necessary amount.
- Accuracy: Personal data must be accurate.
- Limitation of storage: Implementing time limits for data retention, conducting periodic audits, and deleting unused data.
- Protection, confidentiality, and security: Ensuring data integrity, preventing information leaks.
- Accountability: Appointing a responsible person for the collection of personal data.

The GDPR expands the concept of personal data and introduces the terms "cross--border data transfer," "pseudonymization," establishes the "right to erasure," and defines the role of a data protection officer.

In particular, the following concepts are introduced:

- Data controller: A data controller is a natural or legal person who independently or jointly determines the purposes and means of processing personal data, for example, a social network or a taxi service.
- Data processor: A data processor is a natural or legal person who processes personal data on behalf of and under the instructions of the data controller, for example, a cloud service provider.
- Data subject: A data subject is an individual whose personal data is being processed.
- Special categories of personal data: These are specific types of personal data that require additional protection due to their sensitive nature. They include information about race, political opinions, religious or philosophical beliefs, genetic data, trade union membership, biometric data for the purpose of uniquely identifying a person, data concerning health, and data concerning a person's sex life or sexual orientation.

According to the requirements of GDPR, a data protection button must be present on the website. The website owner is responsible for safeguarding the personal data of users on the network. Now, it is necessary to obtain consent for the collection of personal information on all websites. From the user's perspective, it is a simple process, but for advertisers, it requires implementing a series of updates as personal data needs to be stored.

A special platform has been created to facilitate data collection on the web. A separate interface is provided for users to review and accept requests for collecting confidential information. The platform's functions include data request, tracking, and storage, selecting a list of potential clients, and identifying the reasons for their interest in the product. The platform has become relevant since the introduction of the GDPR law. User information is stored in a separate database, making it clearer where visitor data is going. Marketers now have information about product demand. The issue of collecting and storing personal data is resolved, and simultaneously, information about potential clients is obtained.

The implementation of GDPR has elicited mixed reactions from users and advertisers. The question arose regarding which specific data should be protected. Personal information encompasses everything that a user chooses to provide. Special attention is given to sensitive personal data, which includes information about philosophical and political views, religious affiliation, and racial or ethnic origin. In social media platforms, users voluntarily fill out participant questionnaires.

Protection of personal data is particularly important when it comes to targeting, which involves personalized targeting of internet users. Currently, major information giants utilize approximately 52,000 personal characteristics of individuals to identify their interests, personality traits, weaknesses, and desires. Advertising platforms employ targeting as one of the most effective marketing mechanisms. However, targeting inherently carries certain risks for users [Bray D.A., Brooks P., Wander S., Goodman J., Carlson T., 2021].

Firstly, targeting is not solely based on data voluntarily provided by users, but also on "automatically" collected information by websites or social networks. This includes browsing history, online purchase and search history, level of activity on social media, and the nature and quantity of likes and reposts. Based on this information, a profile of the individual is formed, including their preferences and psychological characteristics. Most often, websites and social networks gather this information through third parties, so users may not even be aware that their personal data, previously left on one website, has been transferred to a targeted digital service that offers relevant advertising.

Secondly, targeting can lead to discrimination and user limitations. This possibility arises when digital services utilize a large volume of personal data. In practice, this manifests as the hiding of advertising offers based on gender, skin color, origin, financial or marital status. Based on the collected information, the service decides which advertisements will be relevant, depriving the user of the ability to independently choose offers, thereby automatically limiting their new search queries.

Thirdly, targeting is a technology used for manipulating the thoughts of users. For instance, during Brexit, both supporters and opponents of the UK's exit from the EU employed "shadow advertising" that was visible to certain groups of network users while being inaccessible to others. Targeted advertisements tailored to specific beliefs and sympathies were launched to stimulate voting for the desired outcome.

Thus, targeting leads to:

- Filter bubbles: situations where users are selectively presented with biased information, resulting in a lack of diverse perspectives.
- Information overload: situations of excessive information where users receive a large volume of conflicting information, making it difficult to distinguish between true and false claims, leading to uncertainty regarding economic, political, social, and other issues.

Article 6 of the GDPR provides an exhaustive list of lawful bases for the collection and processing of personal data. For marketing purposes, only two bases can be applied: (i) the data subject’s consent and (ii) the legitimate interests of the data controller, provided that it does not override the fundamental rights and freedoms of the data subject.

Articles 8-10 of the GDPR specify personal data that requires special conditions for use and can only be processed with the explicit consent of the user.

Article 8 addresses data concerning children, whose age, depending on the legislation of the Member State, ranges from 13 to 16 years old. Therefore, the collection and processing, including marketing activities, targeting such individuals can only be done with the consent of parents or legal guardians. For example, Instagram does not allow the creation of profiles for individuals under the age of 13 or blocks such profiles if they become aware of them.

Articles 9 and 10 of the GDPR pertain to data concerning health, political opinions, philosophical beliefs, religious beliefs, sexual orientation, and information about criminal convictions.

Article 15 Right of access – Every individual has the right to obtain their data or access to their data. This includes not only the information they have provided themselves but also the information that the company (data controller) has collected about them from other sources or even created themselves.

Article 16 Right to rectification – The data subject has the right to request the correction of inaccurate or incomplete information that is being processed by the company if it has lost its accuracy.

Article 17 Right to erasure (right to be forgotten) – The data subject has the right to request the deletion of their data from the data controller. GDPR provides only a few circumstances under which this right can be exercised.

To comply with GDPR in digital marketing, the following steps are necessary:

1) provide information about the collection of personal data.

2) obtain user consent for the collection and processing of data. When users enter information into website fields, they should confirm their consent to data processing by checking a box that states, "I agree to the terms of data processing." Importantly, this must be an active action, and the checkbox cannot be pre-selected for the user. Additionally, the provision and deletion of data should occur upon the owner's first request.

3) The physical or legal entity collecting the data is responsible for it. If data is stolen due to a breach, leaks occur, or data is lost by any other means, users must be notified within five days.

Here are recommendations for implementing the General Data Protection Regulation (GDPR) into a company's marketing system:

– Familiarize yourself with the requirements of GDPR: Study the fundamental principles and requirements for processing personal data;

– Conduct a data audit: Identify the types of personal data that are collected, used, and stored within the marketing system;

– Analyze which of these data require consent, which require legitimate justification for processing, and which can be deleted;

– Update the privacy policy and user agreements: Ensure that they specify the purposes of data collection, the legal basis for processing, data retention periods, and user rights regarding their data;

– Verify consent procedures: Ensure that the company's marketing system has mechanisms to obtain explicit and documented consent from users for the processing and use of their personal data, and provide users with the ability to withdraw consent;

– Develop mechanisms for managing user rights: Take into account the rights granted by GDPR, such as the right to access, rectify, erase, and transfer data. Provide mechanisms to fulfill user requests;

– Organize staff training: Ensure that marketing personnel undergo training on the General Data Protection Regulation and implement its requirements in their daily practices;

- Conduct monitoring and audits: Regularly monitor and audit the functioning of the marketing system to ensure compliance with GDPR requirements. This includes assessing the processing and storage of personal data, identifying any breaches, and implementing corrective measures;
- Ensure secure storage and usage of data: Establish appropriate technical and organizational measures to protect personal data within the marketing system. This may involve data encryption, regular software updates, and access control;
- Establish agreements with partners: When collaborating with other companies, ensure that agreements include provisions for the processing of personal data and compliance with GDPR requirements for data protection;
- Respond to requests and breaches: Develop procedures to handle user requests regarding their rights under the GDPR and establish documented procedures in case of data security breaches or other incidents related to personal data;
- Regularly update and review data usage procedures: Ensure that procedures for the use of personal data are regularly updated and reviewed to maintain compliance with GDPR requirements.

To obtain consent for the collection of personal data, you can include it in your Cookies Policy or create a separate document such as a Privacy Policy Consent. In the Privacy Policy Consent, users should have the option to individually consent or decline the collection and processing of their personal data for marketing purposes. Additionally, it is mandatory to have a Cookies Policy that provides detailed information on what cookies are, their types, and the purpose of their usage. It's also recommended to create a Cookies Consent Form through which users can independently manage the use of different types of cookies.

When justifying the use of marketing mechanisms as a legitimate interest, the controller is obliged to provide substantial evidence that without this marketing activity, they will not be able to provide certain services. However, it is not enough to simply state this; it should be clearly defined in written form, specifying which personal data is collected, to whom it is shared, how long and where it is stored, and the categories of data subjects involved. Additionally, you should provide evidence that the legitimate interests of the company do not unduly infringe upon the fundamental rights and freedoms of the data subjects. This requires a detailed explanation of your company's activities, the specific marketing mechanism, its importance, and relevance.

The company determines the categories of individuals, which constitute its target audience (age, gender, financial status, etc.). The social network through which marketing is conducted independently decides, based on the criteria provided by the company, which data of its users to process, whom to show advertisements to, and which technologies are best suited for advertising. Thus, both the company and the social network jointly determine the purpose and means of data processing. Therefore, the responsibility in case of violation of the rights of data subjects or data breaches will be shared.

If the company, as the controller, bears sole responsibility, it independently determines the purposes and means of processing. However, considering the terms of use of social networks and the various marketing mechanisms they create, it is almost impossible to imagine such a situation. Social networks are not merely platforms where personal data is collected; they analyze, select, and offer pre-defined categories of data classified by gender, age, interests, and other factors.

Conclusions. The use of marketing tools in the Metaverse enables potential consumers to access new opportunities, while businesses can expand their sales capabilities. The emergence of this innovative business model transforms the relationship between consumers and companies, contributing to increased economic and social consumer value.

At the same time, despite the predicted significant potential of the Metaverse, several complex marketing questions remain unanswered, such as how to responsibly build a new boundless market and ensure secure purchases while maintaining the confidentiality of personal data. To overcome these challenges, marketers must commit to reducing the number of ethical and moral breaches in the Metaverse by developing responsible Metaverse management. It is necessary to establish guiding principles in the areas of data confidentiality, cybersecurity, platform regulation, compliance with marketing standards, as well as fairness, diversity, and inclusivity throughout the value creation chain for consumers.

The recommendations for implementing the General Data Protection Regulation (GDPR) into a company's marketing system are as follows: familiarize yourself with the requirements, conduct a data audit, update the privacy policy and user agreements, verify consent procedures, develop mechanisms for managing user rights, provide mechanisms for fulfilling requests, organize staff training, perform monitoring and audits, ensure secure storage and use of data, establish agreements with partners, respond to requests and breaches, regularly update and review procedures for the use of personal data.

These recommendations provide marketers with ample opportunities to be unique in their approaches and open up new horizons for further scientific research on this topic.

References

1. Natorina, A. (2019). Online retailers' innovation activity: digital age. *Revista Espacios,* 40 (35), 25-32. Retrieved from: https://www.revistaespacios.com/a19v40n35/19403525.html (accessed 10 September 2021).

2. Chaikovska M.P. (2021). Conceptual and methodological principles of management of marketing IT-projects in digitally transforming environment: monograph. Odesa, 2021. 370 p.

3. Chaikovska M.P. (2021). Holistic marketing as a societal driver of convergent digital transformations. Marketing of innovations. Innovations in marketing: materials of the International Scientific Internet Conference (December, 2021). Bielsko-Biala: WSEH. P. 189–191.

4. Sadchenko O.V., Robul I.V. (2020). Economic and environmental marketing space of the economics of experience. Economic Innovations, vol. 22, no. 1(74). P. 129–139. https://doi.org/10.31520/ei.2020.22.1(74).129-139

5. 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) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

6. Bray D.A., Brooks P., Wander S., Goodman J., Carlson T. Report of the Commission on the Geopolitical Impacts of New Technologies and Data. Atlantic Council GeoTech Center. Commission on the Geopolitical Impacts of New Technologies and Data. May, 2021, 166 p.

7. A new ERA for Research and Innovation {SWD (2020) 214 final}. Brussels, 30.9.2020 Com (2020) 628 final Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. 22 p. URL: https://eurolex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0628&from=EN.

8. Reding D.F., Eaton J. Science & Technology Trends 2020-2040. Exploring the S&T Edge. NATO Science & Technology Organization. NATO: March 2020. 160 p.

9. Dachs B., Zahradnik G. From few to many: main trends in the internationalization of business R&D. Transnational Corporations, Volume 29, Issue 1. 2022, p. 107–134. https://doi.org/10.18356/2076099x-29-1-4

10. Jose M. (2019) Mateu1 and Alejandro Escribá-Esteve. Ex-Ante Business Model Evaluation Methods: A Proposal of Improvement and Applicability. Journal of Business Models. 2019. Vol. 7. № 5. P. 25–47.

11. Dasgupta, S., Gupta, B. (2019). Espoused organizational culture values as antecedents of internet technology adoption in an emerging economy. *Information & Management,* 56 (6). https://doi.org/10.1016/j.im.2019.01.004

12. Iskandar, M., Komara, D. (2018). Application marketing strategy search engine optimization. *International Conference on Informatics, Engineering, Science and Technology,* 407, 1-4. https://doi.org/10.1088/1757-899X/407/1/012011

13. Ivanova, N. (2018). Authentication of the region as the object of economic security in the context of economic development of Ukraine. *Revista Galega de Economía*, 27/2, 113--124. https://doi.org/10.15304/rge.27.2.5662

14. Natorina, A. (2019). The adaptive management system of marketing commodity policy. *Baltic Journal of Economic Studies,* 5 (1), 131-136. https://doi.org/10.30525/2256-0742/2019-5-1-131-136

15. Vakulenko, Yu., Shams, P., Hellstrom, D., Hjort, K. (2019). Online retail experience and customer satisfaction: the mediating role of last mile delivery. *The International Review of Retail, Distribution and Consumer Research*: 6th Nordic Retail and Wholesale Conference, 306-320. https://doi.org/10.1080/09593969.2019.1598466

16. Metaverse market revenue worldwide from 2021 to 2030. https://www.statista.com/statistics/1295784/metaverse-market-size.

17. Sarah Xu, Virtual Influencers: America's Next Top Model, Gartner. https://blogs.gartner.com/sarah-xu/2021/12/02/virtual-influencers-americas-next-top-virtual-model/?_ga=2.48004388.209790795.1660735131-2000439249.1660735131

18. Mike Proulx, Answer Four Questions Before Your Brand Jumps On The Metaverse Bandwagon. https://www.forrester.com/blogs/answer-four-questions-before-your-brand-jumps-on-the-metaverse-bandwagon/?ref_search=0_1660733878342

19. Rebecca Barnett-Smith, Marketing In The Metaverse: The Key To Targeting Gen Z? https://mention.com/en/blog/marketing-in-the-metaverse.

20. Daniel Ruby, Roblox Statistics 2023. https://www.demandsage.com/how-many-people-play-roblox.