RIGA GRADUATE SCHOOL OF LAW

Impact of European Data Protection Reform on Direct Marketing.

BACHELOR THESIS

Author: Alise Kornejeva
LL.B 2018/2019 year student
student number B016096

SUPERVISOR: Irene Nesterova
Dm. iur.

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) …….

RIGA, 2019

Abstract

This study explored the influence of the legislation adopted under the EU Data Protection Reform on the direct marketing. Since the introduction of the previous data protection legislation, the amount of data collected, processed and stored has grown exponentially, resulting in the increased risk to the data security of an individual. Thereby, introduction of new rules is a necessity in order to achieve proper execution of data subject's rights in the digital age and create efficient and simplified rules for the companies to apply. Direct marketing is based on the actions connected to personal information – data is gathered via cookies, stored for the purposes of communication and analyzed in order to provide targeted advertising. Thus, it is necessary for companies and especially direct marketers to understand the provisions of the enforced and upcoming legislation and adjust their marketing strategies and overall company structure to them in order to achieve compliance.

Summary

The objective of this paper is to analyze the influence of the enforced and upcoming legislation connected to data protection under the European data protection reform on direct marketing. The focus of the Thesis is on exploration of changes in the main aspects of the direct marketing since the introduction of GDPR and future modifications connected to the upcoming ePrivacy Regulation. The work is divided into two parts in order to explore separately the influence of the general and specific data protection legislation and thereby define the most substantial rules that can affect direct marketing. The author proposes the course of action for the companies and particularly for direct marketers that has to be undertaken to reach compliance in all analyzed matters. In order to conduct this research following methods were used: legal doctrinal analysis, interdisciplinary method and approach of a secondary source interpretation. The analysis is based on the number of versatile scholar opinions in the field of direct marketing and data protection and author's personal view on the matters. EU law related to the data protection is reviewed, cited and analyzed.

In the first part of the research the impact of the general legislation - GDPR - is examined in order to understand to which extent overall data protection rules influence marketing via electronic communications. The matters examined are: two legal basis under which direct marketing activities are most commonly executed - consent and legitimate interest; three data subject rights - right to be informed, right to object and right to erasure - that have to be incorporated into marketing strategy; and different types of cookies used in the direct marketing, from which some require consent and some do not.

The second section explores the influence of the specific legislation focused on the electronic communication - the currently enforced ePrivacy Directive and specifically the upcoming ePrivacy Regulation. Analysis of the level of confidentiality showed that under the ePrivacy Regulation there will be no possibility to perform direct marketing activities on the basis of legitimate interest. The ePrivacy Regulation is predicted to resolve issues resulted from the cookie law suggested by the ePrivacy Directive by simplifying the rules, re-allocating duties in combination with the provisions from the GDPR.

Paper comes up with the conclusion that the EU Privacy Data Protection Reform makes companies perceive data privacy in terms of direct marketing more seriously through stricter rules, increased monetary penalties and the possibility of being deprived of trust. From the first sight, the European Data Protection Reform, particularly GDPR and ePrivacy Regulation, can be seen as a source of obstacles for the direct marketing activities, but a further examination discloses a number of solutions to different complications connected to the introduction of the new legislation.

Table of content

Introduction

Direct marketing is not a static event, it is an immensely efficient process, developed on the conjunction of different features, that comprises pre-campaign actions such as schedule compilations, analysis of forecasts, development and enforcement of the campaign related to the target public, as well as post-campaign objectives, for instance, performance and marketing analysis.[1] As it can be identified from the first sight, all those actions are fully or partially dependent on the processing of personal data of the company's clients.

The times of the direct marketing in the form as it was when it was initially developed are nearly over. We live in the times, where business processes are very fast changing with marketing being one of the rapidest in volatility.[2] Organizations and companies store personal data in order to utilize it for their insight for the further elaboration of the understanding of people behavior.[3] Customers in the digital era are more focused on their privacy, rather than on the advantages of targeted offerings. In fact, personal data, as stated by Peter Sondergaard, global head of research at Gartner Inc, have become so important that is now called "the world's most valuable resource", being even more valuable than oil, due to the fact how much it influences the way organizations connect with their customers and how it positively influences customer experience.[4] Nevertheless, each data processing activity demands a legal basis, thereby it can be justified under General Data Protection Regulation (hereinafter, GDPR) and ePrivacy Directive, which will soon be substituted with ePrivacy Regulation. Marketers have to examine their legal basis both for processing data and the communication.[5]

The companies now have to thoroughly analyze what data is necessary for their marketing campaigns, provide users with information regarding their rights, if requested are obliged to remove all the personal data from their internal systems and have to concentrate on the anonymized non-identifiable information to make general advertising campaigns. If company does not comply, it will be subjected to enormous fiscal penalties and the deprivation of brand reputation. However, in fact there is a rapidly increasing desire for advertisers and marketers to utilize personal data in fresh, creative and impersonated methods. One of the grounds for such desire is a reaction on the users' escalating sharing of different types of more personal information than ever before throughout openly accessible platforms, followed by the openness of new and unusual data sets, analysis and understanding. The main challenge for marketers in the digital marketing field lies in reaching the balance between satisfying customers' desires and developing an innovative strategy, while as well complying with all today's and upcoming legislation. The question of compliance is complicated due to the introduction of GDPR and the future alterations to European Directive 2002/58/EC (hereinafter, e-Privacy Directive), each of which will modify the marketing and advertising scenery drastically.[6] However, concepts described in the GDPR and ePrivacy Regulation are

[1] Billy Sharma, *The Handbook of Direct Marketing* (Canada: Civil Sector Press, 2012), p. 9.

[2] Nicola Flannery, "Direct marketing and privacy: striking that balance", *PDP Journal* (Volume 10, Issue 3), p.1.

[3] The Direct Marketing Association (UK) Ltd, *GDPR for Marketers: Consent and Legitimate Interests* (London: 2018), available on: https://dma.org.uk/uploads/misc/5ae1d4cabcb24-gdpr-for-marketers---consent-and-legitimate-interest_v7[1]_5ae1d4cabca81.pdf, p. 6.

[4] Peter Sondergaard, "Data is the world's most valuable resource", *Assembly of European Regions*, available on: https://aer.eu/data-valuable-resource/. Accessed on April 10.

[5] The Direct Marketing Association (UK) Ltd, *supra* note 3.

[6] Nicola Flannery, *supra* note 2.

not exactly new. Most of them were already covered in the Data Protection Directive and ePrivacy Directive with smaller or bigger modifications, depending on the level of importance of the matter. Thus, the strategy and approach towards direct marketing actions and any processing involved in it, have to be not created from the beginning but reviewed and changed in order to be compliant with the new stricter rules.

In this research a number of main aspects introduced by new legislations were examined. All of them have to be considered when re-evaluating the way the direct marketing is approached in order to achieve compliance and avoid monetary penalties.

EU Data Protection Reform

The European Union (hereinafter, the EU) in the last few decades had adopted a number of legislations related to the protection of personal information, the primary one being the 1995 Data Protection Directive. Nevertheless, since the Lisbon Treaty, protection of personal information, as well as a right to access to data which was gathered and the right to have it erased, have turned into fundamental rights under EU legislation, accepted by the Treaty on the Functioning of the European Union and the Charter of Fundamental Rights of the European Union (hereinafter, the Charter).[7] This signifies that the EU now has a particular legal basis to adopt laws to safeguard these fundamental rights.

Fast technological progress in the last two decades has led to the new issues related to the protection of personal information. The amount of data, which individuals are making publicly available is growing exponentially. At the same time, social and economic integration, arisen from the functioning of the internal market, has also resulted into considerable growth in cross-border flows of information. Thus, to properly measure all of these expansions and encourage the digital economy, there is a necessity to guarantee a strong level of protection of personal information, while at the same time not fully restricting the free movement of such information. [8]

If to mention personal data in the context of law enforcement, there is an increasing necessity for authorities in the EU countries to process and exchange information as the component of the combat against terrorism and transnational crimes. In this case, understandable and consecutive laws on data protection executed by EU are necessary to strengthen partnership between those authorities.[9]

The Data Protection Reform consists of The Data Protection Law Enforcement Directive, and the GDPR. The next step in the transformation of data protection is the ePrivacy Regulation, which will replace the ePrivacy Directive.[10][11]

The first version of GDPR was introduced by the EU Commission in January 2012. The Commission wanted to renovate data protection rules due to the fact that there had been enormous technological developments since the 1995 Data Protection Directive, especially in

[7] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: https://www.refworld.org/docid/3ae6b3b70.html, Article 8. Accessed on April 12, 2019.
[8] European Council. Council of the European Union, "Data protection reform" (2019), available on: https://www.consilium.europa.eu/en/policies/data-protection-reform/. Accessed on April 13, 2019.
[9] ibid.
[10] ibid.
[11] European Commission, "Data Protection in the EU: Legislation" (2018), available on: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. Accessed on April 13, 2019.

the marketing field. The rules have to take into consideration new technological advances, the consequences of user's data proliferation, and altering consumer positions and anticipations.[12] The GDPR was adopted in May 2016 and was designed in order to prepare Europe for the digital age. The Regulation is a substantial step to enhance individual's fundamental right in the age of digitalization and assist companies by defining laws in the digital single market. A single regulation is also designed in order to liquidate fragmentation in different Member States' systems and promote harmonization.[13] Before the GDPR companies and organizations in the EU had to understand and apply 28 different laws related to data protection. For a number of businesses who were planning to enter new markets, this situation resulted in administrative overhead expenses. The GDPR solves this issue and liquidates, for instance, the obligation for companies to inform national data protection authorities from different states about the personal information they are maintaining and processing.[14] Companies are now obliged to renovate their digital production and websites by building in the privacy setting and have them activated by default. Organizations under GDPR also have to conduct on the regular basis privacy impact assessments and document the methods they utilize personal information. The GDPR provides a number of new rules which directly influence direct marketing, including more severe requirements for consent, transparency with users, right to object, providing access to an individual on any identifying data stored, cookie laws and overall increased privacy rights that have to be endorsed. Thereby, marketing specialists have to rethink their marketing strategy and adjust to a number of changes in order to satisfy all the requirements and avoid any monetary penalties.

Directive (EU) 2016/680, The Data Protection Law Enforcement Directive safeguards fundamental right to information protection in the situations when personal information is utilized by criminal law enforcement authorities for the objective of law enforcement. It especially guarantees that the personal information of bystanders, victims and suspects of crime are properly secured, as well as contributes to cross-border partnership to combat against terrorism. The Directive was enforced on 5 May 2016 and Member States had to transfer it into their national legislation by 6 May 2018.[15] It is very unlikely to be applicable to the direct marketing.

The 2002 ePrivacy Directive, amended in 2009, is a significant legal instrument for protection of privacy and confidentiality of electronic communications and laws concerning tracking and control. It is the specific legislation, focused on the electronic communication and directly influencing marketing via emails and other digital forms of advertising. The enforcement of the GDPR required EU authorities to renew the text of the ePrivacy Directive; thereby the European Commission announced a proposal of the new Regulation on 10 January 2017. The new version will have to manage the fast developing technological landscape, including such challenges as privacy of machine-to-machine communication, which is known as Internet of

[12] The Direct Marketing Association (UK) Ltd, *GDPR for marketers: The essentials,* (London: 2018), available on: https://dma.org.uk/uploads/misc/5aabd9a90feff-gdpr-essentials-for-marketers----an-introduction-to-the-gdpr_5aabd9a90fe17.pdf, p. 8. Accessed on April 14, 2019.
[13] ibid.
[14] European Commission, "EU Data Protection Reform: better rules for European businesses", available on: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business_en.pdf p. 1
[15] European Commission, *supra* note 11.

Things, or the privacy of individual's communication on publicly approachable networks, for instance public Wi-Fi spots.[16]

The interplay of those three legislations is crucial for the successful result in the overall data protection. However, in this work the author will mostly focus on the interplay of the GDPR and ePrivacy Directive, as well as changes related to its transformation intro Regulation, since those are most relevant to the direct marketing and have the most influence on it.

For the nowadays and upcoming rules related to data protection to work, it is significant for all actors related to the Data Protection Reform to participate equally.

EU Member States have to prepare to new laws as soon as they are enforced, as well as revoke and correct existing national rules, introduce national data protection authorities.[17]

Data Protection Authorities, set up by the Member States, have to cooperate together as the European Data Protection Board. Their main objective is to safeguard the proper application of the laws including via the monetary penalties and to explain the application of provisions via creation of guidelines.[18]

At the same time organizations and companies have to prepare prior the enforcement of new laws, connect with your local Data Protection Authorities if any questions related to data protection arise and observe existing provisions.[19]

European Commission (hereinafter, the Commission) is obliged to control the application of the GDPR and react if necessary in the appropriate way, including - if required - the infringement procedure against EU Member States which will fail to apply new laws. The Commission aims to encourage consistency and restrict disintegration in the application process, as well as co-finance actions which increase awareness of the public.[20]

Citizens, from their side, have to find out their rights and reach out to their national Data Protection Authority if their rights are being breached.[21]

General legislation - The influence of GDPR on Direct Marketing

GDPR, a data protection legislation which sets up laws regarding storing, processing and using personal data from data subjects who are at the present time within the territory of the European Union, came into force on May 25 in 2018.[22] The new regulation replaced previous Data Protection Directive 95/46/EC.[23] GDPR aims to consolidate overall EU data protection to correspond to arising data protection issues caused by emerging digital technologies. Although the regulation only safeguards EU citizens, its influence can be

[16] "ePrivacy Directive", European Data Protection Supervisor, available on: https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en. Accessed on April 15, 2019.
[17] European Commission, "EU Data Protection Reform: a concerted effort to make it work" (2018), available on: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-who-does-what_en.pdf.
[18] ibid.
[19] ibid.
[20] ibid.
[21] ibid.
[22] Li, He, Lu Yu, and Wu He. "The Impact of GDPR on Global Technology Development." *Journal of Global Information Technology Management* 22, no. 1 (2019): 2. doi:10.1080/1097198x.2019.1569186.
[23] "2018 reform of EU data protection rules", European Commission, available on: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. Accessed on April 16, 2019.

recognized as of the global nature, impacting any company or organization that is connected to the European market or offers services and goods, as well as maintains personally identifiable data of citizens of EU. Thus, supporting the commonly named Brussels effect[24], those companies, independent of the place of their main department, must comply with the GDPR rules.

The introduction of the GDPR signifies that there is a reduction of the scope to store and process personal data for commercial reasons and especially for direct marketing.

In direct marketing, specialists highly depend on the collecting and processing of personal data from an enormous number of devices in order to establish personalized, based on the particular person's preferences and interests experience via marketing and advertising. Thereby, due to the high dependence on the personal data of the customers, there are a lot of rules which have influenced how the direct marketing is undertaken and managed since the GDPR came into force. Some of the main changes are: compliance management with the obligation to provide records of it; the users full control over their information, which involve right to object to processing of personal data and right to erasure of such data; compliance with the anti-spam rules and updated rules on cookies. In addition, all those points are liable to be subjected to audit and have to be self-evident. [25]

Nevertheless, it is not the objective of the legislators to limit or entangle business processes. Contrariwise, the purpose is to transform the maintenance and processing of data into more transparent procedure.[26] The rules are formulated in such way to reach the balance between potential advantages of data processing and the potential disadvantages. [27]

There are six grounds that can be applicable for processing data in the GDPR. Those are consent, legitimate interest, performance of the contract, compliance with the legal obligation, vital interest of the data subject and public interest.[28] In terms of direct marketing activities the most accurate types are legitimate interest and consent.

The Principle of Consent

A key feature of any organizations' or companies' direct marketing actions is obtaining appropriate prior consent.[29] The upgraded rules regarding consent in the GDPR and

[24] Deloitte UK, "A new era for privacy GDPR six months on", available on: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf, p. 10.

[25] "The Impact of the GDPR on Digital Marketing and How to Prepare for It", Netcentric, https://www.netcentric.biz/insights/2017/08/the-impact-of-the-gdpr-on-digital-marketing-and-how-to-prepare-f.html. Accessed on April 20, 2019.

[26] CAS Software AG, "CRM Guide EU General Data Protection Regulation" (2018), available on: https://www.infomat.eu/wp-content/uploads/2018/05/CRM-Guide-EU-General-Data-Protection-Regulation.pdf , p. 7.

[27] European Data Protection Board, "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities" (2019), available on: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf, p. 8.

[28] Tim Walters, "The Burdens and Benefits of the GDPR: A Practical Guide for Marketers", *The Content Advisory* (2018), available on: https://www.lytics.com/assets/documents/Lytics_Burdens_and_Benefits_of_GDPR.May.2018.pdf, p. 7.

[29] Nicola Flannery, *supra* note 2.

the upcoming new e-Privacy Regulation provide more severe standards and increased threshold for people in marketing departments to meet prior to the point when the consent is received. In addition to the severe standards, the scope of the principle of the consent has expanded to consolidate more types of technologies, for example the communication with the personal messages via social media platforms, web mail, instant messaging or unmanaged VoIP, all together recognized as Over-the-Top communication services.[30]

Consent by data subject throughout which he or she recognizes that his or her personal information is being processed for direct marketing purposes has to meet a number of requirements in order to be efficient (Article 4, 6(1) (a), 7 of the GDPR). If the subsequent requirements are violated, the grant of consent is revoked. The consent must be given voluntarily (Article 7(4)), in an informed way (Article 13, 14), for the particular case, undoubtedly and throughout a clearly assertive act. If the statement of consent is a part of another text, this must be clear, comprehensible and with typographic emphasis (Article 7(2)). In a like manner, the right to annul consent at any time should be also mentioned (Art. 7(3)). The data controller, which is accountable for the determination of the purposes and means of data processing, is bound to submit records of the consent supplied if inquired as the part of its documentation responsibilities (Art. 7(1)). Even though consent in the written form is no longer necessary, the statement of consent has to be accessible in a storable form. If the company or the organization cannot provide such records, a court or the public authority will suspect that the consent was not provided and that the marketing activities were undertaken unlawfully.[31]

In the case of the consent previously received, it has not to be acquired again, if the way in which the consent has been provided complies with the provisions of the GDPR (Art. 171 of the GDPR).[32] Nevertheless, since there is not enough case law yet, the practical interpretation of this condition by the courts and public authorities cannot be precisely predicted. Thus, according to author's opinion, it is reasonable for marketing specialists to receive consent once again to avoid any misunderstanding. Additionally, consents that were received throughout "opt-out" are scarcely to be considered valid.[33]

In order to be GDPR compliant marketing specialist will have to accomplish a number of steps. Firstly, they have to discuss with company's data management team how the new consent form will be designed, where the form will be displayed and in which way the form will be gathered. Secondly, overall privacy policy should be reviewed and incorporated into marketing strategy. The tracking policy should be also renovated: not paying attention to a box or closing pop-up window does not constitute consent anymore under GDPR. It is necessary to establish the way of recording all newly upgraded consent and the method for regularly scheduled testing and evaluating the efficiency of measures taken in order to succeed in data privacy. Evidence of consent is essential for the future, and shall comprise of

[30] ibid.
[31] EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1.
[32] Ibid.
[33] Thomas Nägele, Simon Apel, Steffen Henn and Alexander Stolz, "GDPR as a game-changer? E-mail marketing via newsletter in light of the new law", *SZA Schilling, Zutt & Anschütz,* available on: https://www.sza.de/fileadmin/fm-dam/Mandanteninformationen/Aktuelles_2018-05/2018_05_SZA_DSGVO_Newsletter_EN_.pdf, p. 3.

source of information, date stamp, and the exact identical opt-in language which user faced before providing consent.[34]

Even though the stricter rules related to consent may be a reason for a number of challenges connected to compliance for the direct marketing specialists at first, it can be a source of beneficial opportunities likewise. The possibilities arise from the fact that rather than obtaining a simple yes or no when inquiring user about his data, marketing specialist can now provide an individual with a diapason of choices, from which users can gain better understanding about what they are most interested in. Via consent, marketers can receive an insight into each user's concerns to ensure them with information that they are most likely to be interested in receiving. These not only contributes to being compliant with GDPR, but also assists to additionally section company's customers and concentrate your electronic communications based on the particular concerns of the user, instead of transmitting general emails to everyone.[35] The other advantage is the possibility to clean up maintained information and assure its up-to-date, precise, and still consistent.

Legitimate interest

Data processing may still be undertaken without the obligation to receive consent if it is essential to defend the legitimate interests of the third party or the data controller except the cases when the data subject's data protection concern or other interests take supremacy (Article 6 (1) (f) of the GDPR).

The notion of legitimate interests in the form of a legal basis for processing of personal data is substantially identical to Schedule 2 conditions proposed by the 1998 Act, with some modifications in detail.[36] Legitimate interest is a risk-based concept, where marketers have to balance their concerns in maintenance and processing of the personal data with any uncertainty related to the individual's privacy. It is not based on a specific goal and thereby provides marketing specialist a wider scope to possibly rely on it in a number of diverse circumstances. It is viewed as the most suitable basis when: the data processing activities are not necessary by law but are of a distinct advantage to the marketing specialist or others; there is a minimal privacy influence on the individual; the data subject should reasonably foresee marketers to utilize their information in such way; and company cannot provide a data subject with full prior control or bother him or her with disruptive consent request when there is a small opportunity for them to object to the data processing. [37]

One working in the direct marketing has to provide a clear opt-out, as well as information regarding any processing activities undertaken and have an irresistible explanation for why someone should be concerned about their services or goods.[38]

---

[34] Michael Concannon,"Direct Marketing Data and the Impact of GDPR," *The Department 3 Blog,* June 8, 2018, https://d3data.com/gdpr-impacts-direct-marketing-data. Accessed on April 24, 2019.

[35] Steven MacDonald, "GDPR for Marketing: The Definitive Guide for 2019" (April 15, 2019), https://www.superoffice.com/blog/gdpr-marketing/. Accessed on April 28, 2019.

[36] Information Commissioner's Office, *Lawful Basis for Processing, legitimate Interests* (22 March 2018*)*, 2, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf, p. 2.

[37] ibid, p. 3.

[38] The Direct Marketing Association (UK) Ltd, *supra* note 3, p.7.

In order to perform direct marketing activities on the basis of legitimate interest one has to conduct the legitimate interest test, the necessity test and the balancing test. Once the marketing specialist have distinguished legitimate interests, he or she have to determine whether planned processing of particular personal data is required, which is the obligation under the necessity test. All processing activities under direct marketing campaign have to be proven essential. For example, combining personal information with data from other channels that is not essential for the advertising of a product will be considered unnecessary. In addition, sharing information with a third party that would not be essential to provide services would also be viewed as excessive. In either situation, direct marketers have to consider another type of legal basis or determine to cancel the marketing campaign. Nevertheless, processing activities are an essential part of direct marketing. Without this activities connected to personal data, direct marketing would not survive due to the fact that advertising could not be personalized and adjusted to the particular audience. Theoretically speaking, it shall consequently be relatively simple for a marketer specialist to fulfill this part of the evaluation. Yet, this cannot be supposed and has to still be a part of marketer's evaluation. It is significant to recall that direct marketers have two objectives for processing of personal information. Those are profiling to set up and audience and the transmitting of marketing communication. The legal basis are necessary for the both of them.[39]

The most important part of the evaluation is to conduct the balancing test, under which marketers have to recognize the risks to a user's personal privacy. Marketing specialists have to take into consideration in which way their future campaign may influence this and record their conclusions. Companies may determine to make a number of changes to the marketing campaign as an effect of a balancing test. For instance, data retention time limits may be put into practice, which diminish the risk to violating individual privacy. Another illustration would be data minimization, under which only basic personal information for the marketing campaign is required. Inquiring more personal data than is essential enhances the risk to individual's privacy and is considered a violation of one of the main principles of GDPR. If in the end all conditions of the balancing test are satisfied, the legitimate interest may be used as a legal basis for the data processing activities.[40]

This type of the legal ground for processing of personal data offers marketers a beneficial legal route due to the fact that there are a number of cases when it can be applicable to their actions. Choosing the legitimate interest as the legal basis could signify escaping from the necessity to reconnect with customers and request their consent. Nevertheless, one still has to comply with the transparency rules (Article 13 and 14 of GDPR). Based on this ground, many companies may prefer to use legitimate interests and inquire consent only for specific channels for marketing and advertising if they obliged to do so.[41]

As far as the GDPR has no information regarding what type of parameters refer to the consideration of legitimate interests, the concept of the legitimate interest can be interpreted very extensively. Notwithstanding, in future it will be essential to provide reasoning to data subject at the time of accumulation of personal information behind any projected processing activities, their target, and the presence of a respective legitimate interest in a reasonably specific and clearly formulated form (Article 13(1)(d) and Article14(2)(b) of the GDPR).

[39] ibid, p.14.
[40] ibid.
[41] The Direct Marketing Association (UK) Ltd, supra note 3, pp.7-8.

The presence of the legitimate interest will make data processing more legitimate unless there are no less aggressive methods of reaching the same objective available and unless the concerns, fundamental freedoms, or rights of the data subject that contradict with the data processing do not predominate.[42] In this negotiation of interests, the features of the corresponding legitimate interest, the sensitiveness of the personal information, the outcome of the data processing for the data subject, the attitude of the data subject towards to the data controller, and the kind of the data processing all play a significant part. There will nonetheless be questions regarding what one may adequately anticipate concerning data processing as an outcome of the information received (Article 47 of the GDPR), thus transparency is required. A specific defensive concern applies in the scope of advertising to persons who have not yet reached the age of 16, when processing notably sensitive information (connected to health, ethnic, political and philosophical context), when utilizing new processing technologies (Article 35 of the GDPR), as well as when processing great volumes of information (Article 91 of the GDPR).[43]

Considering the high level of abstraction and versatility of the subject matter, legal certainty will be reached only after numerous interpretations by courts and public authorities will be undertaken. It will form the case law, from which the particular behavior in the situations involving legitimate interests will be distinguished. In addition, whilst legitimate interests is a flexible legal basis and can be applicable quite frequently, it is not relevant to every situation and marketers cannot utilize it as the default legal ground for all data processing activities. None of the six legal grounds have superiority over the others, and marketing specialists have to always apply the one that is most suitable to the circumstances of the particular case having in mind the specific objective of the processing activities. [44]

Data Subject Rights

Data subject rights are one of the main aspects of modification under the GDPR. The Regulation grants the following rights to the data subject: the right to be informed, the right of access, the right to rectification, the right to erasure (the right to be forgotten), the right to restrict processing, the right to data portability, the right to object and rights related to automated decision making and profiling.[45]

The GDPR expands some of already existing rights which data subjects can exercise against data controllers, and also proposes a number of completely new rights. The individuals and proper application of their rights are the main focus of the GDPR. Direct marketing specialists

[42] Thomas Nägele, Simon Apel, Steffen Henn and Alexander Stolz, *supra* note 33, p. 4.
[43] ibid, p. 3.
[44] "When can we rely on legitimate interests?", Information Commissioner's Office, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/. Accessed on April 17.
[45] EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1.

will thereby have to consider all parts of their data processing activities in light of data subject rights provided by the Regulation.[46]

All data subjects right have an influence on the direct marketing, in a bigger or smaller extent, and thus have to be taken into consideration, but in this research three data subject rights will be explored - the right to be informed, the right to object and right to erasure - since they are the ones requiring the most modification in the overall marketing strategy such as reviewing consent form and obtaining a new data storage system.

Right to be informed

Customers have the right to be informed about the gathering and utilization of their personal information, which is specified under Article 13 and 14 of GDPR. This is a main transparency requirement according to the GDPR. Direct marketers have to provide data subjects with information regarding objectives for data processing activities involving their personal data, maintenance periods for that data, and whether there will be third party involved. This is so-called "privacy information" and it has to be provided to customers at the time of gathering their personal data. If direct marketers receive personal information from other sources, they have to provide data subjects with privacy information within one month after receiving the data. Nevertheless, there are a number of circumstances when marketers do not have to deliver privacy information to individual, for example when a data subject already possesses the information or when it would cause a disproportionate effort to transfer it to him or her. The information provided has to use clear and simple language, as well as it has to be easily accessible, transparent, concise and understandable.

It is usually most efficient to provide privacy information to data subjects applying a combination of various methods including just-in-time notices (focused and relevant privacy information provided at the time company collects individual's personal data), layering (brief notices comprising of basic privacy information that have additional layers of more specific information), icons (short, expressive, symbols that represent the existence of a specific type of data processing), dashboards (preference management technique that inform individuals how marketers utilize their data and gives them an opportunity to decide what happen with it) and different types of smart and mobile device functionalities (such as voice alerts and pop-ups).[47]

Customers testing is a beneficial way to receive feedback on how efficient the company's transfer of privacy information is. Direct marketers have to constantly review, and where required, upgrade their privacy information. Individuals have to be provided with the updates every time marketing specialists have an intention to utilize their personal data for a new purpose. If the right to be informed is executed correctly it can contribute to achieving compliance with other provisions of GDPR and establish trustworthy relationships with consumers. However, not putting enough attention towards it can result for company in monetary penalties and reputation damage.[48]

[46] Matheson, "GDPR in Context: Data Subject Rights," available on: https://www.matheson.com/images/uploads/documents/MATH_10010_GDPR_in_Context_-_Data_Subject_Rights.pdf, p. 1.
[47] "Right to be informed", Information Commissioner's Office, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. Accessed on April 18, 2019.
[48] ibid.

Right to object and right to erasure (right to be forgotten)

Under the GDPR, individuals are provided with a right to be forgotten and right to object, which are introduced in Article 17 and 21 respectively. Both rights in the context of direct marketing activities are worth discussing, as well as the correlation between two notions should be mentioned.[49]

The GDPR sets up a right for an individual to object to activities associated with processing of personal data, but anticipate diverse requirements for application of this right and also diverse consequences for data controllers. The "general" right to object provided by Article 21(1) of GDPR can only be executed by a data subject on "grounds relating to his or her particular situation". Thus, an individual, at least in some degree, has to demonstrate that the processing activities influence his or her life. Moreover, in accordance with Article 21(2) of the GDPR, an individual can enjoy a slightly altered right to object to activities associated with processing of personal data for the direct marketing objectives without the need to satisfy any supplementary requirements. Additionally, under Article 21(3) of the GDPR the data controller must stop any data processing activities for the direct marketing objectives after the right to object was executed.[50]

Regardless of whether direct marketing is based on the legitimate interest, public interests,[51] consent or the processing for the scientific or historical purposes, the data subject has an unreserved right to object at any point of time (Article 7 (3) or Article 21(2) of the GDPR). If the right to object is realized, the personal information may no longer be utilized for the further processing manipulations. The data subject has to be provided in time with the information about the existence of this right. In time means at the moment of first connection and in company's privacy notice. This information has to be expressly delivered to the attention of data subject and has to be given clearly and apart from any other extra information.[52]

The only grounds for the continuation of data processing activities are: if one can provide irresistible legitimate grounds for the data processing, which prevail over data subject's rights, interests and freedoms; or the processing of the personal data is undertaken for the formation, implementation or justification of legal claims.[53]

This division into "general" right to object and concrete right to object connected to direct marketing is also reflected in Article 17(1) of the GDPR and the responsibility of the data controller to delete personal information.[54] Data subject right to erasure (right to be forgotten) plays a significant role in the future of the direct marketing. The right to erasure, which received a considerable amount of attention after the 2014 judgment of the Court of Justice of the EU, established the precedent for the right to be forgotten provision comprised in the GDPR. The case involved Google and a Spanish citizen, who wanted links with out-of-date information of his bankruptcy removed, because he did not wanted people to know about it

[49] Carlo Piltz, "The right to erasure, the right to object and marketing: finding the balance", Cecile Park Media Publication (2018), available on: https://www.reuschlaw.de/fileadmin/contents/2018_Newscontent/DPL_GDPR_Right_to_Erasure.pdf.
[50] ibid.
[51] Information Commissioner's Office, "Overview of the General Data Protection", available on https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf, p. 25.
[52] ibid.
[53] ibid.
[54] Carlo Piltz, *supra* note 49.

every time they have searched for his name. Certainly, keeping in mind rival interests and free enormous flow of data in Internet, the right to erasure is much more complex than a user simply inquiring that a company has to delete their personal information.[55]

The right to erasure is one of the most complicated GDPR data subject rights to put into use overall, as stated by IAPP-EY Annual Privacy Governance Report 2017.[56] This right is introduced in Recitals 65 and 66, as well as in Article 17 of the GDPR. Under this Article the data subject has the right to receive from the data controller the deletion of all personal information related to him or her across the whole company, and the controller is obliged to delete all data "without undue delay" if a number of requirements are satisfied. "Undue delay" in this context means approximately a month. The marketing specialist also has to confirm that the individual inquiring deletion is actually the data subject (Article 17 of GDPR).

Allowing data subject to exercise the right to erasure is an obligation of the data controller with a supplementary duty of information/ communication and deletion by the third parties, other receivers and other data controllers with particular exceptions and conditions related, among others, possibility of the inquired deletion in a proportionate manner. [57] In the situation of processing for the objectives other than direct marketing and the respective objection by an individual, the data controller has to carry out a balancing of interests in accordance with Article 17(1)(c) of the GDPR. The personal information has to be deleted unless there are existing overriding legitimate grounds for the continuation of data processing.This opportunity to balance diverse interests and potentially come to the agreement not to delete personal data, is not existing in the situations of processing data for direct marketing objectives and an objection under Article 21(2) of the GDPR.[58] Erasure of personal data is not only the right of the data subject. Data controller's records related to the data processing activities also have to, where feasible, include the foreseen time limits for deletion of the various types of personal data.[59]

The challenge for the marketers arises when data related to an individual is stored in various places and is processed for various objectives. The resolution to this issue is to possess a single system or a platform that maintains the records of consents of every single data subject. Possessing a single platform, for example CRM system, will assist marketing specialist in monitoring of all their authorized data and guarantee that they are GDPR compliant. The benefit of possessing a single system is that it provides users with possibility of giving consent and taking it back, for various objectives. Furthermore, for the marketing specialist it is an opportunity to understand more about their customers and target them with advertising comprised from the particular and relevant content. [60]

The main distinction between two data subject rights lays in the fact that right to be forgotten focuses on the personal information itself, when the right to object is concentrated on a particular action of processing. The difference is significant in the nowadays information security services context, where the identical personal information is frequently processed for

[55] "Everything you need to know about the "Right to be forgotten"," GDPR.eu, available on: https://gdpr.eu/right-to-be-forgotten/. Accessed on April 19, 2019.
[56] "The right to erasure or right to be forgotten under the GDPR explained and visualized," i-SCOOP, available on: https://www.i-scoop.eu/gdpr/right-erasure-right-forgotten-gdpr/. Accessed on April 19, 2019.
[57] ibid.
[58] Carlo Piltz, *supra* note 49.
[59] "The right to erasure or right to be forgotten under the GDPR explained and visualized," i-SCOOP, available on: https://www.i-scoop.eu/gdpr/right-erasure-right-forgotten-gdpr/. Accessed on April 19, 2019.
[60] ibid.

a countless number of objectives. The right to object only averts future data processing for single or a number of objectives, while the right to be forgotten averts data processing of any type due to the fact that information can no longer be maintained by the data controller.

The combination of right to object and right to erasure became also feasible after the Google vs Spain case. Court of Justice executed both rights at the same time to ratify the so-called "right to be delisted", which means eliminating the link between a particular search term and particular search result. The right to be delisted could be named a hybrid, where right to be forgotten demolishes the linkage between the term and result, and right to object concentrates specifically on one single processing activity - connecting name to search result. [61]

The European legislator has specifically expressed the connection between the right to be forgotten and the right to object.[62] Nevertheless, the right to be forgotten is completely different from the right to object to the utilization of contact data for the direct marketing aims. Data subject can object to direct marketing without involving the right to erasure of associated information. Neither will an execution of the right to object to data processing activities trigger the application of the right to be forgotten.[63] However, clearly deletion of contact information does prevent marketing specialists from direct marketing activities due to the fact that they wouldn't possess contact details of the particular person to do so.

Cookies

A cookie is a small amount of information sent from the website to the customer's computer where it is preserved as a basic text data. Cookies are designed in such way that every time when customer visits the website again, the cookies will be automatically transferred back from the customer's computer to the original website's server. Cookies were developed to be a secure mechanism for company's website to recall personal preferences of the customer, such as what types of goods were added in the shopping cart, what pages were visited, what language was chosen, etc. Due to this reason, web cookies play a significant role in the direct marketing activities, giving an opportunity to recognize the customer and provide a genuinely targeted advertising. Since the cookies contain the personal information of data subjects by which a particular person can be identified a number of cookies fall within the notion of personal data.[64]

Even though, the primary source for the EU rules related to cookies has always been the ePrivacy Directive, the enforcement of the GDPR has increased the complexity of cookies utilization. This is due to the fact that consent under the ePrivacy Directive is characterized by allusion to consent prescribed by the EU's data protection regime. Consequently, at the moment when the GDPR took over the Data Protection Directive, the definition of the consent under the GDPR applied also to the ePrivacy Directive. This signifies that, where necessary, cookie consent has to be now "freely given, specific, informed and unambiguous".

---

[61] Jef Ausloos, "The Interaction between the Rights to Object and to Erasure in the GDPR," Ku Leuven (2016), available on: https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/. Accessed on April 20, 2019.

[62] ibid.

[63] ibid.

[64] Rebecca Cousin, Rob Sumroy, Natalie Donovan and Duncan Mykura, "Cookies consent and GDPR: a recipe for disaster", Privacy Laws & Business UK Report, Issue 100 (November, 2018), available on: https://www.slaughterandmay.com/media/2537128/cookie-consent-and-the-gdpr-a-recipe-for-disaster.pdf, pp. 1-2.

In compliance with the consent principle, it is prohibited to install cookies before receiving user consent. In practice, this signifies that company has to execute a script blocking mechanism. However, not all cookies are subjected to the consent requirement and thereby are exempt from the blocking technology. The types of cookies that are exceptional are as follows: technical cookies strictly essential for the provision of services; statistical cookies operated by the company (not third parties), as long as the information processed is not utilized for profiling purposes; and statistical cookies controlled by third party but completely anonymized (such as Google Analytics). Nevertheless, for all those types of identifiers the cookie policy and cookie banner are still essential. [65]

There is an opinion that the GDPR principle of consent shall not be applicable to cookies, due to the fact that Article 95 of the GDPR, which manages the relationship with the ePrivacy Directive, prevents introduction of further obligations by the Regulation where those issues are already subject to the resembling obligations in the ePrivacy Directive. Nevertheless, authorities do not view consent requirements as an "additional obligation", they consider them as the prerequisites for the lawful processing. Thereby, in order to reach compliance with the cookies that demand obtaining of consent, company's website has to be transparent and provide users with information about the existence of cookies, make clear how those cookies are functioning and for what reason, and receive unambiguous consent to maintain those cookies in their system. Even though, the process can appear as including only three simple steps, in practice there are many difficulties that can occur.[66]

Practical issues arise from attempting to obtain consent for cookies that fulfills the extensive requirements of the GDPR, at the same time preventing website modernization and damage to the online experience.[67]

The GDPR requirement for justified consent, which raises the biggest number of issues connected to cookies, is that it has to be received prior to the processing of data. This is a problem for cookie technology due to the fact that cookies are in the most systems set at once upon a user's appearance on the website. It has been clear that, where feasible, cookies shall be postponed until an individual have had the opportunity to understand and make his mind about which cookies are being installed. Nevertheless, growing number of organizations and companies are looking to resolve this problem.[68]

The requirement for the consent to be unambiguous has also resulted in a number of practical issues connected to cookies. Individuals nowadays are already used to managing with discreet pop-up banners at the end of the webpage. This "auto-accept" principle has a restricted influence on an individual's experience of a company's website, and can be clearly called as "freely given, specific and informed". Nevertheless, it is difficult to provide evidence that it is unambiguous. Specific attention should be devoted to assuring that clear and specific consent is received in the cases where privacy-intrusive cookies are being utilized.

A number of companies resolved this issue by implementing approach where the website shows a notification which prevents an individual from immediately entering the website,

[65] "Cookies and the GDPR: What is Really Required?," Iubenda, available on: https://www.iubenda.com/en/help/5525-cookies-gdpr-requirements. Accessed on April 20, 2019.
[66] Rebecca Cousin, Rob Sumroy, Natalie Donovan and Duncan Mykura, *supra* note 64, p 3.
[67] ibid.
[68] ibid, p 4.

unless the utilization of cookies is either accepted to in its fullness or the individual has otherwise chose the kind of cookies that he is willing to agree to, so called "cookie walls" [69]

To achieve the full compliance company will have to include the selection of cookies, as well as compel interaction with cookie consent. However, that course of action is complicated: not all cookie libraries endorse the purpose-based choice of cookies. Choice is a basic element in a freely provided consent. Consent is not considered freely received unless data subject are easily capable to disable cookies. Consequently, forced opt-in has to be utilized carefully. If a company utilizes forced opt-in method in order to deny access to individuals who selected to not give consent to any types of cookies they are operating unlawfully, because they deprive an individual of any choice. In addition, companies should abstain from utilizing consent mechanisms that only grant an option for the individual to consent without any distinct choices.[70]

When evaluating the problems connected to cookies and consent, it is undoubtedly significant to mindfully take into consideration the privacy influence of a specific cookie on individual. While there are a number of cookies that do represent privacy risk, others do not. The Council of the EU has specifically recognized that cookies should be viewed as a legitimate and beneficial instrument in the provision and evaluation of an digital service.[71]

Specific legislation: ePrivacy - from Directive to Regulation

GDPR plays a significant role for the marketers to understand and implement into their day to day work in order to avoid monetary penalties. Nevertheless, it is a general regulation, which affects overall data protection. It is necessary to analyze more specific EU legislation to properly understand legal framework for the digital marketing activities nowadays. Both the general GDPR and specific ePrivacy Regulation are components of EU data protection reform and therefore must be explored equally thoroughly.

The ePrivacy Regulation is estimated to go into effect later in 2019 and will replace ePrivacy Directive 2002/58/EC (hereinafter, Directive). Even though Directive is considered a legal act, it does not oblige all EU member states to implement it in the same manner. Substantially, member states have an opportunity to select what parts of the Directive they decide to inherit and enforce, which is opposite to the idea of a uniform legal framework. When the Directive came into force in 2002, it was sufficient enough. But since then, the usage of electronic devices and their overall development have significantly increased, contributing to growth in risk connected to the personal data privacy.[72] The ePrivacy Directive does not include electronic communication services ensured by providers that work over the Internet, in spite of the fact that they provide services that are functionally equivalent. Those providers will although be within the scope of the upcoming ePrivacy Regulation. The expansion of the scope of the ePrivacy regulation to functionally equivalent services, involving "Over-the-Top" services is a necessary component of the improvement. In addition, Regulation also is applicable once the information connected to the behavior of individuals is gathered, in spite of whether they have registered for a service or not. This method will not only provide the

[69] ibid.
[70] ibid.
[71] ibid.
[72] "The new EU ePrivacy Regulation: what you need to know," I-SCOOP, available on: https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/. Accessed on April 21, 2019.

users with the security they are entitled to, but it will also authorize just competition between data controllers.[73] ePrivacy regulation will utilize the same definitions as GDPR, but it concentrates particularly on electronic communications. When the Regulation will come into force, it will in fact override a number of provisions from GDPR related to data confidentiality and privacy in the field of electronic communications.[74] Right now the Regulation is still undergoing the legislative process.[75] Nevertheless, there are already a lot of information available about the changes and additions to the previous version.

The ePrivacy Regulation is specific legislation, concentrated on data protection in the electronic marketing communications. It has the aim to harmonize the national law necessary to provide an equivalent degree of protection of fundamental freedoms and rights, and specifically the right to confidentiality and privacy, with regard to the processing of personal information in the electronic communication field and to guarantee the free movement of this type of information, as well as electronic communication facilities and services (Article 1(1) of the ePrivacy Directive).[76]

The ePrivacy Regulation anticipates that software should follow a "privacy by design" concept giving users an opportunity to decide which privacy settings they want, modify them at any moment of time, and be reminded of this opportunity every six months. This notion is beneficial to direct marketers and online advertisers, in contrast with "privacy by default" concept that would avert web browsers from maintaining online tracking technologies, for example cookies, in the absence of individual's active ability to choose.[77] The GDPR protects the right to the protection of personal information set up under Article 8 of the Charter, while the ePrivacy Regulation is designed to safeguard proper application of the right for private and family life and right for protection of personal data written down in the Article 7 of the Charter. [78] In this respect, the ePrivacy Regulation seeks to complement and specify the rules from the GDPR, with reference to the processing of personal information in the electronic communication sphere.[79]

The interplay of GDPR and ePrivacy Regulation: lex specialis versus lex generalis.

The upcoming regulation is considered to be lex specialis to the GDPR and will "particularize and compliment" it in respect of electronic communications information that is defined as personal data. The ePrivacy Regulation is designed to particularize the provisions of the GDPR to such an extent as it concerns the processing of information that is recognized

[73] European Data Protection Board, "Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications," available on: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.
[74] Rebecca Cousin, Rob Sumroy, Natalie Donovan and Duncan Mykura, *supra* note 64, p 4.
[75] Nicola Flannery, *supra* note 2, p. 1.
[76] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available on: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058.
[77] Pilar Córdoba Fernández and Katherine Dagg, "The ePrivacy Regulation: Cookie setting from banner to browser," LithouseEurope (2017), available on: http://www.lighthouseeurope.com/fileadmin/documents/pdf/Publications/The_ePrivacy_Regulation__Cookie_setting_from_banner_to_browser.pdf, p. 1.
[78] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: https://www.refworld.org/docid/3ae6b3b70.html. Accessed April 22, 2019.
[79] European Data Protection Board, *supra* note 27, p. 8.

as personal data. The ePrivacy Regulation also aims to complement the laws of GDPR in the situations where the GDPR clearly is not applicable, for instance when it comes to information connected to legal persons.

The extent to which ePrivacy Regulation complements the provisions of GDPR is much smaller than the extent to which it particularize GDPR.[80] All issues connected to the processing of personal information not concretely addressed by the Regulation are undertaken by the GDPR. The overlap with the GDPR leads to the revocation of a number of provisions, for example the Article 4 of the ePrivacy Directive about the security obligation.[81] In other words, in situations where both the ePrivacy Regulation and GDPR apply, the provisions prescribed by the Privacy Regulation will prevail on the basis of the principle of the lex specialis derogat legi generali. The direct marketers engaged in the processing of personal data are subjected to the specific laws enclosed in the Article 16 of the ePrivacy Regulation which governs "unsolicited and direct marketing communications". Consequently, both the ePrivacy Regulation and GDPR influences activities of the specialists working in the marketing department, who advertise their products and services through marketing emails. [82]

In territorial coverage the ePrivacy Regulation aligns with the GDPR, meaning that it extends broader than the EU and involves all companies and international organizations that gather personal data from data subjects in EU Member States. Under suggested new laws, business receivers of direct marketing can experience the same level of protection as individual customers. The sanctions and monetary penalties for one who do not comply also are identical to those of GDPR.[83] The Article 29 Working party, an independent European advisory body coping with the arising data protection and privacy issues working until 25 May 2018 when GDPR came into force, have issued an Opinion welcoming the fact that the new Regulation, similar to the GDPR and in contrast with the previous Directive, will have a direct effect in EU countries with Data Protection Authorities from every Member State being accountable for its enforcement.[8485] It is crucial that international organizations and companies engaged in the electronic communication and presently concentrated on implementing the GDPR provisions give sufficient attention to the ePrivacy Regulation.[86]

The laws connected to unrequested marketing communications, in addition to the general right to object to activities associated with direct marketing presented by the GDPR, are similar to current laws. The individual's prior consent is necessary before transmitting electronic communications for the aim of direct marketing. The exception may be granted if direct marketing services or products are comparable to those that an individual has purchased before. The ePrivacy Regulation also mentions that EU Member States can permit, by law,

---

[80] Brinkhof Advocaten, "A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation," Centre for Information Policy Leadership (2018), available on: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf, p. 36.

[81] European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 para. 1.2

[82] Pierre Dewitte, "Email me not: direct marketing, GDPR and ePrivacy Regulation", KU Leuven Centre for IT & IP Law (2018), available on: https://www.law.kuleuven.be/citip/blog/email-me-not-direct-marketing-gdpr-and-eprivacy-regulation

[83] Nicola Flannery, *supra* note 2, p. 1.

[84] "Article 29 Working Party," European Data Protection Board, available on: https://edpb.europa.eu/our-work-tools/article-29-working-party_en. Accessed on April 23, 2019.

[85] Nicola Flannery, *supra* note 2, p. 1.

[86] ibid.

direct marketing via voice-to-voice calls if addressee did not expressly showed his objection to obtain those calls. Nevertheless, in the upcoming Regulation, the scope of the related services is widened including all direct marketing communications transmitted through the "electronic communication services". The EU Parliament informs that it covers communications systems, automated calling, faxes, email, semi-automated systems that connect the caller with other people and other utilization of electronic communication services. The proposal also involves particular conditions circumstances applicable to unrequested marketing calls and consolidates protection for users.[87]

Confidentiality beyond the GDPR

Confidentiality of communications, which can be considered as the nowadays equivalent of the traditional postal privacy, is a fundamental right safeguarded under Article 7 of the Charter, already exercised by the ePrivacy Directive. This right to confidentiality has to be exploited to every direct marketing communication in electronic form, inconsiderable of the means by which they were forwarded, form the sender to the recipient, and has to also defend the stability of every consumer's terminal equipment.[88]

Electronic communications are the foundation stone of many vital actions of the nowadays social order, due to the fact that they endorse the implementation of a number of fundamental rights, for example freedom of expression, information, thought, religion, assembly, association, conscience, etc.[89] Thereby, it is an essentiality to strengthen the neutrality and confidentiality of the messaging services. Understanding the widespread and the significance of the usage of the electronic communications in modern digital world, they are very probably to contain, or to disclose, special categories of personal information, and shall thus be treated respectively. Consequently, author supports the approach of the upcoming Regulation, established on broad restrictions, limited exceptions, and the importance of consent. This approach creates almost no place for misunderstanding, is straightforward and thus is very likely to succeed with the objective of the creation of uniform laws regarding data protection. In contrast to the GDPR,[90] there shall be no probability under ePrivacy Regulation to undertake processing activities of metadata and content received from the direct marketing supported by an open-ended legal basis, for example "legitimate interests". Moreover, there should be no opportunity under the ePrivacy Regulation to process personal data from the electronic communications for the fulfillment of contractual obligations, which signifies that there should not be an exclusion based on the general objective of the performance of a contract, as the Regulation establishes which exact types of processing are allowed, for instance processing of personal data for billing intentions.[91] Nevertheless, it should be mentioned that data gathered from the direct marketing can still be processed without receiving consent after it has been completely anonymized. [92] In author's opinion, the

[87] Ernst & Young Global Limited, "The ePrivacy regulation proposal: a new data protection framework for electronic communications" (2018), available on: https://www.ey.com/Publication/vwLUAssets/ey-law-alert-digital-law-september-2018/$File/ey-law-alert-digital-law-september-2018.pdf p 2.
[88] European Data Protection Board, *supra* note 73, p. 1.
[89] Ibid, pp.1-2.
[90] G.-J. Zwenne, Quinten Kroes and Joost van Eymeren, "A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation" (19 July 2018), available on: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf p.4.
[91] European Data Protection Board, *supra* note 73, pp. 1-2.
[92] ibid.

principle of anonymization is a beneficial opportunity for service provides to create and develop innovative services at the same time safeguarding privacy and confidentiality.

Preservation of confidentiality of data gathered from electronic communications is a right already currently existing in the ePrivacy Directive. The 2002 ePrivacy Directive, which has been amended in 2009, has already settled a general restriction on the processing of personal data gathered through direct marketing communications in the electronic format. Under today's legislation, this type of operations is only executable with the consent of the consumer, taken within a reasonable time. Reasonable time in this context means prior any data processing activities are undertaken. Those activities are only possible with the prior consent of the data subject, or if any of the proposed exemptions written down in the ePrivacy Directive are met, such as billing purposes or the act of transporting of an electronic communication. As was mentioned before, those provisions will be kept in the proposed Regulation. In a like manner, the safeguarding of terminal equipment has already formerly been a right.[93] The utilization of storage capacity of the customer's terminal equipment is treated in a technology-neutral approach. Thereby, every tracking mechanism, including cookies, is already under ePrivacy Directive subject to consent of the data subject. Furthermore, the proposed Regulation establishes a number of new exceptions that were suggested by the WP292, for instance audience measuring and security improvement. Such exclusions are linked to certain types of personal data processing involving moderate privacy risks for the data subjects.[94]

Consent under ePrivacy Regulation: opt-in, soft opt-in and opt-out

As a general provision, Article 16(1) of the ePrivacy Regulation demands from company and its specialists to receive consumers' consent prior forwarding direct marketing communications in electronic format. Consent, under ePrivacy Regulation, is recognized as "opt-in". That concept, as defined in the Article 4 of the ePrivacy Regulation, is written down based on the Article 4(11) and Article 7 of the GDPR. All rules connected to consent are similar to the GDPR, meaning it has to be "freely given, specific, informed and unambiguous indication of wishes expressed by a statement of a clear affirmative action".[95]

Consent for the direct marketing activities is usually obtained when customer ticks a box. As mentioned before, it is written down in Article 7(3) of the GDPR that data subject has the right to revoke his consent at any time. Nevertheless, the controller may still maintain and process contact information for direct marketing objectives, but only in the situations where the soft opt-in can be applicable. Considering the fact that it involves substituting the consent with another legal basis, the Article 29 Working Party demands to inform data subject about that shifting in accordance with Article 13 and 14 GDPR. Whilst opt-in continues to be usual when practicing direct marketing communications in electronic format, Article 16(2) of ePrivacy Regulation specifies an exemption, recognized as the "soft opt-in". This signifies that consent is not essential if marketers are sending advertising message regarding similar goods and services to their customers. The provision is applicable if three particular conditions are satisfied. [96]

[93] ibid.
[94] ibid.
[95] Pierre Dewitte, *supra* note 82.
[96] ibid.

First condition that has to be met prescribes that contact details from the electronic communications must have been received "in the context of the sale or purchase of a product or a service". Simply registering in the company's website to look through its categories of goods provided would not establish the necessary pre-contractual negotiations. However, contacting the company in order to request information about the order possibility of out-of-stock goods or adding products to the basket would be satisfactory for the Article 16(2) of the ePrivacy Regulation to be applicable. Generally, it is the responsibility of the controller to provide evidence and justify the above.[97]

The second condition states that the company that has gathered the contact information is allowed to utilize it only "for direct marketing of its own similar products or services", meaning that only the company that originally gathered the email addresses can take advantage from the exceptions written down in the Article 16(2) of ePrivacy Regulation, not organizations utilizing bought-in marketing registers. In addition, the company can utilize them to promote its "own" and "similar" goods and services. Obviously, the user's interests are most likely to change after a period of time, and so are the categories of goods and services which may be promoted using the obtained contact details. The user's rational expectations should be the leading principle in this issue.[98]

The third and the last condition prescribes that an organization can only depend on Article 16(2) of the ePrivacy Regulation ensured that consumers "are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use". This also is the reference to the Article 21(2) of GDPR.[99]

The right to object, similar to the GDPR, has to be presented prior any collection or processing of the contact details and personal data and each time when they are utilized for the direct marketing communications purposes. This might result quite confusing for users, due to the fact that they can be introduced with both an opt-in - as a part of the overall marketing communications in the electronic format - and an opt-out - as a necessity for marketing communications under the Article 16(2) of the ePrivacy Regulation - at the moment of user's registration into company's website. In any situation, the opt-out has to also be introduced with every electronic communication, most commonly as a link at the end of the email. [100]

Cookie reform: simpler laws on identifiers

Today, under the current ePrivacy Directive, the utilizing of tracking technologies and means to access information saved on the individual's terminal equipment, for example cookies, is permitted only with the prior consent of the particular user. Studies have acknowledged that the cookies laws, as presented by the 2009 amendments to the ePrivacy Directive, are being unsuccessful to reach their objectives - to provide individuals with a real choice and grant informed consent. This failure resulted in the discomfort of the individuals, who have to constantly consent to the utilization of cookies, as well as encounter with "cookie walls".[101] Thereby, the cookie law is now being reviewed and hopefully the way the cookies

[97] ibid.
[98] ibid.
[99] ibid.
[100] ibid.
[101] European Parliament, "Reform of the e-Privacy Directive", *EU Legislation in Progress* (2017), available on: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf, p. 4.

are regulated is going to be completely changed in the upcoming ePrivacy Regulation. The process will be made clearer for both the users and the marketers.

The ePrivacy Regulation's objective is to provide individuals with control over their personal information by clarifying the laws related to cookies. The European Commission first proposal concerning the ePrivacy Regulation affirmed that cookie consent conditions would be modernized, with the new laws ensuring a simple process for individuals to accept and deny cookies and other types of identifiers via the settings on their web browsers in the situation where there privacy is at risk.[102] In accordance with the Article 8 of the ePrivacy Regulation, the utilization of cookies and other types of identifiers is allowed on the basis of six grounds: if the use of cookies is based on the prior consent of an individual, in situations when it is essential for the transportation of electronic communications, in order to present an information society service inquired by an individual or in cases where it is an essential part of the web analytics. The European Parliament adds possible circumstances for the utilization of cookies for the purpose of web analytics, especially on the maintenance of data. It also suggests other grounds to be called an exception: in situations when it is essential for security renovations of the terminal equipment and when cookies are used on the basis of employment relationships. The European Council suggests the identical exception connected to security renovations, endorsing security in information for the purpose of fighting the deception, but there is no exception regarding the cookies as a part of employment relationships.[103]

The general rule stating that consent is necessary for the utilization of cookies is maintained in the upcoming ePrivacy Regulation. Nevertheless, proposal assures that no consent is necessary for not privacy intrusive identifiers which are refining online experience. The example of this type of cookies is to recall goods that were put in the cart by the particular user. In addition, cookies set by a company on the website in order to count the number of users visiting the website will not demand consent anymore.[104]

One of the most important changes that will be incorporated into the ePrivacy Regulation is connected to re-allocation of duties between browsers and providers of websites. By separating duties the upcoming ePrivacy Regulation supports the view of the Article 29 Working Party, which states that "[t]he risk to data protection comes from the purpose(s) of processing rather than the information contained within the cookie". Modern rules make website operators liable for the storage and also for the retrieval of cookies, as well as for the following data processing activities developed from them. By assigning a responsibility of storage and retrieval to web browsers, and thus permitting website operators to expect the fulfillment of this duty from them, the upcoming Regulation should make it clearer that following processing has always been a legally distinct action subject not to the particular cookie rules but, if it is connected to personal data, to overall data protection law. Information received from cookies should not be considered as a special case, but rather as another kind of personal information, whose data processing activities are subjected to the entire range of data protection rules. This should provide more proper controls for both the users and website operators, and renovated experience likewise.[105]

---

[102] Rebecca Cousin, Rob Sumroy, Natalie Donovan and Duncan Mykura, *supra* note 79, p.5.

[103] Ernst & Young Global Limited, *supra* note 87, pp. 1-2.

[104] European Commission, Press Release, "Commission Proposes High Level of Privacy Rules for All Electronic Communications and Updates Data Protection Rules for EU Institutions," (Jan. 10, 2017), available on: http://europa.eu/rapid/press-release_IP-17-16_en.htm. Accessed on April 28, 2019.

[105] Andrew Cormack, "The Draft ePrivacy Regulation: No More Lex Specialis for Cookie Processing?," *Scripted*: 2017, pp. 347, doi: 10.2966/scrip.140217.345.

The Article 29 Working Party commented on the European Commission proposal for the upcoming ePrivacy Regulation that the principle of lex specialis will only apply to accessing and storing cookies, not following processing, and that storing and accessing can only be undertaken with a prior, informed consent. The Working party also emphasized that now in a form of Article instead of a Recital, such "consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet" and that, to be considered valid, those settings have to be the outcome of a "clear, affirmative action" by an individual. [106]

Nevertheless, understanding an obvious failure of nowadays legislation that simply stated the opportunity of basing on technical settings to give consent, there is a new statement according to which "web browsers … are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment". Thus, to guarantee that browsers, in future, perform in such way, a new legal responsibility on those delivering web browsers to the EU market was proposed by the Commission and the Parliament.[107] They suggest to explicitly prohibit providers to reject individuals' access to any functionality or service on the basis that they have not presented consent for maintaining, collecting and processing needless data.[108] In addition, the upcoming ePrivacy Regulation demands providers of software allowing electronic communications, or those permitting restoration and presentation of data to make an option accessible to hinder third parties from maintaining data on the individual's terminal equipment. At the time of the setting of the software, an individual shall be provided with information about privacy settings, and his consent gathered for a setting. If the software already is set up on individual's device, the provision has to then be enforced with the update of the software, but the individual has to be informed within the period of three months of the day the ePrivacy Regulation becomes enforced.[109]

An active choice provided when a browser is set up or first updated may grant justified consent for maintaining and accessing cookies but, as long as the definitions and requirements for valid consent described in Articles 4(11) and 7 of the GDPR shall be met, it is not probable that it will also grant valid consent for following processing activities. Thereby, whilst the draft Regulation will signify that website operators can depend on browser technical settings to receive individual's consent to the maintaining and accessing of cookies, the Article 29 Working Party's proposal that the same consent could be utilized to following data processing activities based on those cookies no longer is viewed tenable. Website operators will thus have to take their own actions to assure that their processing of data derived from cookies is compliant with the legislation. They will need to distinguish and apply the relevant provisions of the GDPR when undertaking any processing activities connected to the personal information based on cookies. The GDPR was specifically created to develop a comprehensive system to control such processing. Moreover, applying the GDPR guarantees that the same laws apply to processing regardless of who performs it or what type of technology may be utilize.[110] If authorities and website operators now recognize the

[106] ibid. p 349-350.
[107] ibid.
[108] Ernst & Young Global Limited, *supra* note 77.
[109] Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, (Jan. 10, 2017), Art. 10 at 28.
[110] Andrew Cormack, supra note 105, p. 357.

possibility to apply cookie provisions from GDPR with the ability to make it more simpler by re-allocation of responsibilities between browsers and website operators under the upcoming ePrivacy Regulation, there shall be much less complications and frustration from both users and website operators.

Conclusion

The purpose of this Thesis, as was stated in the beginning of the research, was to explore the impact of legislation enforced under the European data protection reform on direct marketing. Since the most influential rules on direct marketing are the GDPR and the ePrivacy Directive, which will be soon upgraded to the ePrivacy Regulation, the study was mostly focused on the modification introduced by them.

It was discovered that there are two main legal bases for direct marketing activities under GDPR - consent and legitimate interest. Consent under upgraded rules has to be given freely, it has to be specific, informed and unambiguous, as well as it should be provided by a statement or a clear act and has to be "clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language" (Recital 32 and Article 7 of the GDPR). In order to satisfy those requirements direct marketers will have to create new consent forms and tracking policies to record all new received consents and evaluate the efficiency of the measures taken. The consent policy once created can have a beneficial influence on direct marketing. Via consent marketing specialist can gain better understanding of the interest of the particular person and thereby create a more personalized advertising. The other possibility that arises with the proper consent management is the better sectioning of the company's customers.

Direct marketing activities can still be executed without the obligation to obtain consent if it is necessary to safeguard the legitimate interests of the third party or the data controller, unless the data subject interests in the data protection take supremacy. The research showed that the most suitable circumstances for data processing on the basis of legitimate interest are when: the data processing activities are not essential by law but are of a certain advantage to the direct marketers or others; the data subject should anticipate marketing specialists to use his or her data in such way; organization cannot provide an individual with full prior control or distract him or her with incessant consent requests when there is a minor possibility for data subject to object to the particular data processing activities. If applying the legitimate interest as legal basis direct marketers have to perform the legitimate interest test, the necessity test and the balancing test, through which it should be identified whether the actions which will be undertaken under particular marketing campaign are genuinely necessary and evaluate potential risk for the user. The research identified that the data security of an individual and the concept of the utilization of only strongly necessary data are central to the GDPR and ePrivacy Regulation likewise.

Data subject rights are one of the main areas of modification under the GDPR. In this research the impact of right to be informed, right to object and right to erasure (right to be forgotten) on direct marketing were explored both separately and simultaneously. Under the right to be informed direct marketers have to provide data subjects with the "privacy information", which includes purposes for data processing, maintenance period for the personal information, and whether the data will be also processed by any third parties. The study revealed that the most efficient way to deliver privacy information to data subject is through application of a number

of different methods including layering, just-in-time notices, icons and dashboards. During the analysis it was identified that the right to object is the easiest in execution, because it only involves the termination of processing acitivites. In contrast, the study showed that the right to erasure is a source of potential challenges for direct marketing, since many companies are maintaining data of one individual in a number of places and utilize it for different reasons. The possible resolution advised by the author can be obtaining of a single platform, in which it would be easier to sort and find data. In addition, it provides users with the opportunity to consent and object to use of personal data for various purposes.

The research showed that cookies, as any other technologies utilizing personal data require "freely given, specific, informed and unambiguous" consent, which has to be also, obtained prior any processing activities. Thereby, cookies now have to be postponed until the user decides what type of cookies he will agree to set up. Particular focus should be devoted to the fact that consent should be unambiguous, meaning that "auto-accept" principle can lead to a number of problems with compliance. However, as analysis shows, not all types of cookies require consent. The cookies that fall under exception are: technical cookies that are necessary for the provision of services; statistical cookies operated by organization itself or by third party when they are completely anonymized.

The research showed that the confidentiality under ePrivacy Regulation is stricter than under GDPR, meaning that there is no opportunity to perform direct marketing activities on the basis of open-ended legal ground, such as legitimate interests. Nevertheless, there is a possibility of "soft opt-in", which is applicable if the direct marketer is sending information about similar good or service and a number of conditions are satisfied.

The study also showed that one of the main changes that ePrivacy Regulation will introduce are simpler rules on identifiers and cookies, since the nowadays laws suggested by the ePrivacy Directive were called inefficient. The main idea of the new rules is based on the separation of duties between providers of websites and browsers. The author proposes that the most successful approach could be to assign the duty of storage and retrieval to web browsers under ePrivacy Regulation, while providing website operators possibility to focus on the consent related to processing actions on their website under provisions of GDPR.

Overall, as it happens with any new legislation, the GDPR and upcoming ePrivacy Regulation will keep on being evaluated, tested, and implemented by the direct marketers in the future. After a period of time, there will be more case law on the matter, which will ensure growth of legal certainty as well as a uniform system of data protection. The introduction of new legislation under European data protection reform, developed in order to confront the realities of comprehensive, ubiquitous data in the era of the digitalization, is a beneficial opportunity for direct marketing specialists to improve, sustain and re-establish trust in data protection, opt-ins, and electronic communications with old and new users alike.

Bibliography

Primary Sources

1. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available on: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058.

2. European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: https://www.refworld.org/docid/3ae6b3b70.html.

3. EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1.

4. Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, (Jan. 10, 2017), Art. 10 at 28.

Secondary Sources

Books

1. Sharma, Billy. *The Handbook of Direct Marketing* (Canada: Civil Sector Press, 2012).

Journal Articles

1. Ausloos, Jef. "The Interaction between the Rights to Object and to Erasure in the GDPR," Ku Leuven (2016), available on: https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/.

2. Brinkhof Advocaten, "A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation," Centre for Information Policy Leadership (2018), available on: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf.

3. CAS Software AG, “CRM Guide EU General Data Protection Regulation” (2018), available on: https://www.infomat.eu/wp-content/uploads/2018/05/CRM-Guide-EU-General-Data-Protection-Regulation.pdf .

4. Concannon, Michael. ”Direct Marketing Data and the Impact of GDPR,” *The Department 3 Blog*, June 8, 2018, https://d3data.com/gdpr-impacts-direct-marketing-data.

5. Córdoba Fernández, Pilar and Katherine Dagg, “The ePrivacy Regulation: Cookie setting from banner to browser,” LithouseEurope (2017), available on: http://www.lighthouseeurope.com/fileadmin/documents/pdf/Publications/The_ePrivacy_Regulation__Cookie_setting_from_banner_to_browser.pdf.

6. Cormack, Andrew. “The Draft ePrivacy Regulation: No More Lex Specialis for Cookie Processing?,” *Scripted*: 2017, pp. 347, doi: 10.2966/scrip.140217.345.

7. Cousin, Rebecca, Rob Sumroy, Natalie Donovan and Duncan Mykura, “Cookies consent and GDPR: a recipe for disaster”, Privacy Laws & Business UK Report, Issue 100 (November, 2018), available on: https://www.slaughterandmay.com/media/2537128/cookie-consent-and-the-gdpr-a-recipe-for-disaster.pdf.

8. Deloitte UK, “A new era for privacy GDPR six months on“, available on: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf.

9. Dewitte, Pierre. “Email me not: direct marketing, GDPR and ePrivacy Regulation”, KU Leuven Centre for IT & IP Law (2018), available on: https://www.law.kuleuven.be/citip/blog/email-me-not-direct-marketing-gdpr-and-eprivacy-regulation.

10. Ernst & Young Global Limited, “The ePrivacy regulation proposal: a new data protection framework for electronic communications” (2018), available on: https://www.ey.com/Publication/vwLUAssets/ey-law-alert-digital-law-september-2018/$File/ey-law-alert-digital-law-september-2018.pdf.

11. European Commission, “Data Protection in the EU: Legislation” (2018), available on: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

12. European Commission, “EU Data Protection Reform: a concerted effort to make it work” (2018), available on: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-who-does-what_en.pdf.

13. European Commission, “EU Data Protection Reform: better rules for European businesses”, available on: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business_en.pdf.

14. European Commission, Press Release, “Commission Proposes High Level of Privacy Rules for All Electronic Communications and Updates Data Protection Rules for EU Institutions,” (Jan. 10, 2017), available on: http://europa.eu/rapid/press-release_IP-17-16_en.htm.

15. European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

16. European Council. Council of the European Union, “Data protection reform” (2019), available on: https://www.consilium.europa.eu/en/policies/data-protection-reform/.

17. European Data Protection Board, “Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities” (2019), available on: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

18. European Data Protection Board, “Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications,” available on: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.

19. European Parliament, “Reform of the e-Privacy Directive”, *EU Legislation in Progress* (2017), available on: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf.

20. Flannery, Nicola. “Direct marketing and privacy: striking that balance”, *PDP Journal* (Volume 10, Issue 3).

21. Information Commissioner's Office, *Lawful Basis for Processing, legitimate Interests* (22 March 2018*)*, 2, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf.

22. Information Commissioner's Office, “Overview of the General Data Protection”, available on https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf.

23. Li, He, Lu Yu, and Wu He. "The Impact of GDPR on Global Technology Development." *Journal of Global Information Technology Management* 22, no. 1 (2019): 2. doi:10.1080/1097198x.2019.1569186.

24. MacDonald, Steven. "GDPR for Marketing: The Definitive Guide for 2019" (April 15, 2019), https://www.superoffice.com/blog/gdpr-marketing/.

25. Matheson, "GDPR in Context: Data Subject Rights," available on: https://www.matheson.com/images/uploads/documents/MATH_10010_GDPR_in_Context_-_Data_Subject_Rights.pdf.

26. Nägele, Thomas, Simon Apel, Steffen Henn and Alexander Stolz, "GDPR as a game-changer? E-mail marketing via newsletter in light of the new law", *SZA Schilling, Zutt & Anschütz,* https://www.sza.de/fileadmin/fm-dam/Mandanteninformationen/Aktuelles_2018-05/2018_05_SZA_DSGVO_Newsletter_EN_.pdf.

27. Piltz, Carlo. "The right to erasure, the right to object and marketing: finding the balance", Cecile Park Media Publication (2018), available on: https://www.reuschlaw.de/fileadmin/contents/2018_Newscontent/DPL_GDPR_Right_to_Erasure.pdf.

28. Sondergaard, Peter. "Data is the world's most valuable resource", *Assembly of European Regions*, available on: https://aer.eu/data-valuable-resource/.

29. The Direct Marketing Association (UK) Ltd, *GDPR for Marketers: Consent and Legitimate Interests* (London: 2018), available on: https://dma.org.uk/uploads/misc/5ae1d4cabcb24-gdpr-for-marketers---consent-and-legitimate-interest_v7[1]_5ae1d4cabca81.pdf.

30. The Direct Marketing Association (UK) Ltd, *GDPR for marketers: The essentials*, (London: 2018), available on: https://dma.org.uk/uploads/misc/5aabd9a90feff-gdpr-essentials-for-marketers----an-introduction-to-the-gdpr_5aabd9a90fe17.pdf.

31. Walters, Tim. "The Burdens and Benefits of the GDPR: A Practical Guide for Marketers", *The Content Advisory* (2018), available on: https://www.lytics.com/assets/documents/Lytics_Burdens_and_Benefits_of_GDPR.May.2018.pdf.

32. Zwenne, G.-J., Quinten Kroes and Joost van Eymeren, "A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation" (19 July 2018), available on: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf .

Websites

1. "Article 29 Working Party," European Data Protection Board, available on: https://edpb.europa.eu/our-work-tools/article-29-working-party_en.

2. "Cookies and the GDPR: What is Really Required?," Iubenda, available on: https://www.iubenda.com/en/help/5525-cookies-gdpr-requirements.

3. "ePrivacy Directive", European Data Protection Supervisor, available on: https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en.

4. "Everything you need to know about the "Right to be forgotten"," GDPR.eu, available on: https://gdpr.eu/right-to-be-forgotten/.

5. "2018 reform of EU data protection rules", European Commission, available on: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

6. "Right to be informed", Information Commissioner's Office, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/.

7. "The Impact of the GDPR on Digital Marketing and How to Prepare for It", Netcentric, https://www.netcentric.biz/insights/2017/08/the-impact-of-the-gdpr-on-digital-marketing-and-how-to-prepare-f.html.

8. "The new EU ePrivacy Regulation: what you need to know," I-SCOOP, available on: https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/.

9. "The right to erasure or right to be forgotten under the GDPR explained and visualized," i-SCOOP, available on: https://www.i-scoop.eu/gdpr/right-erasure-right-forgotten-gdpr/.

10. "When can we rely on legitimate interests?", Information Commissioner's Office, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/.