Professional paper / Stručni rad

THE IMPACT OF THE GDPR ON DIGITAL MARKETING

MARIJA BOŠKOVIĆ BATARELO
Parser compliance d.o.o.
Ulica Milana Amruša 19, 10000 Zagreb
marija.boskovic@parser.hr

ABSTRACT

This article aims to provide a comprehensive assessment of the interactions between digital marketing and data protection laws, focusing on the EU General Data Protection Regulation (GDPR).

Although other domains of the law are also relevant for the digital marketing compliance, such as consumer protection law, e-commerce and competition law, data protection laws are at the forefront of the relationship between digital marketing and the law. Many digital marketing activities involve the massive processing of personal data, including the targeting and personalised treatment of individuals on the basis of such data, thus it is crucial to understand and include the GDPR compliance as a part of a digital marketing strategy.

The article describes basic data protection terms and principles in the GDPR. It explains what it means to embrace data protection by design.

The author takes practical approach to the GDPR compliance and provides steps for ensuring compliant digital marketing activities. These steps also include the methodology for performing data protection impact assessments.

The conclusion of the article provides perspective on future developments regarding data protection and e-privacy laws and there influence on digital marketing.

KEYWORDS: digital marketing, GDPR, e-privacy, compliance, ethics, privacy by design, risk based approach, data protection impact assessment

1. INTRODUCTION

Digital marketing transforms traditional marketing activities. Digital transformation affects the way how companies communicate with their consumers, analyse their preferences, and predict their behaviour. Many companies aim to develop, so called ecosystem of trust, in which consumers are in the centre and they actively communicate and participate.

From this point of view, data about consumers becomes valuable and the base of digital marketing strategy. By analysing data, companies understand consumers and develop new advertisements, products, and services tailored to their needs.

This article aims to explain the interactions between digital marketing and legal framework on personal data protection and provide guidelines for compliant digital marketing activities. This is important, not only to minimise risks and avoid fines, but also to ensure trust of consumers.

2. LEGAL FRAMEWORK ON PERSONAL DATA PROTECTION

A right to protection of an individual's private sphere against intrusion from others was laid down in an international legal instrument for the first time in Article 12 of the United Nations Universal Declaration of Human Rights. The right to protection of personal data forms part of the rights protected under Article 8 of the European Convention of Human Rights, which guarantees the right to respect for private and family life, home and correspondence and lays down the conditions under which restrictions of this right are permitted.

In 2000, the European Union proclaimed the Charter of Fundamental Rights of the European Union. This Charter not only guarantees the respect for private and family life but also establishes the right to data protection, explicitly raising the level of this protection to that of a fundamental right in the EU law.

The principle legal instrument on personal data protection was introduced in 2016, as 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 - GDPR). Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The GDPR has been fully applicable from 25 May 2018 and has significantly raised the bar on data protection compliance, since it has prescribed fines up to 20 million euros or 4% of total worldwide annual global turnover.

The EU is determined to create digital single market and free flow of data, so the next step in this harmonised approach is the new e-Privacy Regulation which will replace 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).
While the GDPR sets basic principles for the personal data processing and protection of personal data, Directive on privacy and electronic communications regulates spam, cookies, and processing of location data. This article will focus on the GDPR, since the e-privacy legal framework is in the status of change at this point.

3. BASIC PRINCIPLES

Companies that perform digital marketing activities are data controllers, as they determine purposes and means of personal data processing (for example, they have a website or a web shop). Every personal data processing should set strict and clear purpose of data processing and limit the scope of the purpose. That is especially important, because companies need different sets of personal data for operating a web shop, running a loyalty club, and performing

promotion activities. Each legitimate purpose defines data that is necessary to achieve certain purpose.

In accordance with the GDPR, personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’);
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
d) accurate and, where necessary, kept up to date (‘accuracy’);
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

The principle of accountability puts burden of proof on data controller, which means, for example, that a consumer can ask questions and companies need to have explanations and documents that prove compliance.

It is also obligatory to inform a person on basic information on data processing activities. These basic information contain contact details of data controller and data protection officer, description of purpose and legitimate interest, as well as information on recipients of personal data. For this reason we usually see privacy policies on websites. While, the GDPR defines that these kind of information should be transparent and clear, usually these documents are quite long and complicated.

4. LAWFULNESS OF PROCESSING

Processing of personal data is lawful only if:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

From the aforementioned provisions, we can see why the GDPR has created lots of confusion. The GDPR actually does not tell us when it is legal to process personal data. Each data controller has to check all the relevant laws. If specific law prescribes that is obligatory to

process personal data, then this processing is a result of data controller's obligation. Usually, marketing activities are not obligatory and this is something what companies perform based on their legitimate interest or consent of data subject.

From the practical experience, consent is something that should be the last resort of processing personal data, since a data subject has a full control over the data and has the right to withdraw consent. Thus, the biggest part of the decision making on whether to process certain data is the product of legitimate interest analysis. The analysis actually analyse purpose of processing activities, risks and measures, and it is important to have sound legal arguments, research case law and reach decisions.

Special categories of personal data, such as data about health, is generally forbidden to process. Only if the GDPR and special laws allow such processing, data controller can subsequently check beforementioned six legal grounds for processing personal data.

5. DATA PROTECTION BY DESIGN

Data Protection by Design was introduced in the GDPR as a form of Privacy by Design concept. Privacy by Design dates from October 2010, when, at the International Conference of Data Protection and Privacy Commissioners in Jerusalem, Ann Cavoukian, Ph.D., Canadian Information and Privacy Commissioner, proposed this resolution.

The principle consists of a set of seven foundations:

a) No action is required on the part of the individual to protect their privacy - it is built into the system, by default;
b) Privacy is integral to the system, without diminishing functionality;
c) Avoid the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both;
d) Extend throughout the entire lifecycle of the data involved - strong security measures are essential to privacy, from start to finish;
e) Seeks to assure all stakeholders are operating according to the stated promises and objectives, subject to independent verification;
f) Require architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user - friendly options.

The GDPR prescribes that data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

This means, for example, to have in mind basic principles and legal grounds, and from the beginning of the project, such as web shop, place technical measures to ensure only minimum data is collected and to determine, for example, which cookies are essential, which data is required to perform purchase, and how the e-mail addresses will be used in the future marketing activities.

6. DATA PROTECTION IMPACT ASSESSMENT

If we consider modern digital marketing tools and trends, we can notice that Big Data analysis have been performed, AI based technologies have been developed and companies use pixels, beacons, and cookies for profiling and targeting. In this context, companies often feel confused whether all these activities can be justified as their legitimate interest to promote products and keep the business sane.

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall in accordance with the GDPR, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Each EU Member State (its Data Protection Authority) published a list of processing activities that are likely to result with a high risk. These lists are not exhaustive, so data controllers perform these assessments on a case by case basis.

A data protection impact assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects;
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

Such assessment shall provide balanced model and efficient system of checks and balances whilst it is a matter of a current state of mind what interests and human rights will prevail in the specific case. Unfortunately, as we cannot predict court decisions, in the same way we cannot say for sure what should be considered as a legitimate interest. The balance should be found in each individual case and all the above-mentioned principles should be taken into account in the process of balancing between various interests and different human rights.

7. WHAT IS NEXT?

From the legal point of view, regulation of digital marketing in the aspect of personal data protection has put a lot of burden on companies. They have to assess, prove, and document their marketing activities. Consumers and their fundamental rights and freedoms have high level of protection within the EU legal framework.

Although, principles and assessments are obligatory in accordance with the law, we can see many digital marketing activities performed unlawfully. It is not an easy task to regulate new technologies. The GDPR is technologically neutral, it only regulates processing of data, but is the question how and who will actually check and audit compliance.

For this reason, we can notice that the law has been more and more put in the code. By doing this the code actually becomes the law. The law which is the same everywhere. This kind of regulation by code is something that we will probably see more in the future and digital marketing strategies will be no longer equipped to circumvent regulation. New proposal of e-Privacy Regulation proposes provisions on cookies as something that will be set in an Internet browser and a person will decide in the device settings what is actually allowed to be stored in the terminal equipment.

We will see more privacy enhancing technologies that innovate certain marketing activities in a way that they ensure the GDPR compliance in its settings and build trustful relationship with the user. There are already plug-ins and browsers that block online advertisements and Firefox and Safari have been blocking by default third party cookies. It was published that Google Chrome will do the same, in certain phases, during next two years.

Google and Apple are also working on data science techniques, such as differential privacy and multi-party computation, in order to ensure privacy and data protection through advanced encryption techniques.

It seems that the future of digital marketing is on its crossroad. Certain strategies that are not built on human rights protection will be abolished and we will see new and creative strategies that value consumer.

REFERENCES

1. European Court of Human Rights (1950). Convention for the Protection of Human Rights and Fundamental Freedoms https://www.echr.coe.int/Documents/Convention_ENG.pdf, accessed [30/6/2020] (Internet reference)
2. L. Lessig (1999). The Law of the Horse: What Cyberlaw Might Teach, Research Publication No. 1999-05 12/1999 (Article reference)
3. M. Kearns, A. Roth (2019). Ethical Algorithm. Oxford University press (Book reference)
4. M. Bošković Batarelo, (2015). Smart Privacy in Smart Cities. Tilburg University. (Master's thesis reference)
5. Official Journal of the EU (2002). 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 accessed https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 [30/6/2020] (Internet reference)
6. Official Journal of the EU (2016). 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 https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed [30/6/2020] (Internet reference)
7. The Verge (2020.) https://www.theverge.com/2020/1/14/21064698/google-third-party-cookies-chrome-two-years-privacy-safari-firefox, accessed [30/6/2020] (Internet reference)
8. The Medium (2019.), https://medium.com/@dimitrov.anton/the-world-needs-privacy-preserving-computations-13fd05c39323, accessed [30/6/2020] (Internet reference)

9. United Nations (1948). Universal Declaration of Human Rights, https://www.un.org/en/universal-declaration-human-rights/, accessed [30/6/2020] (Internet reference)