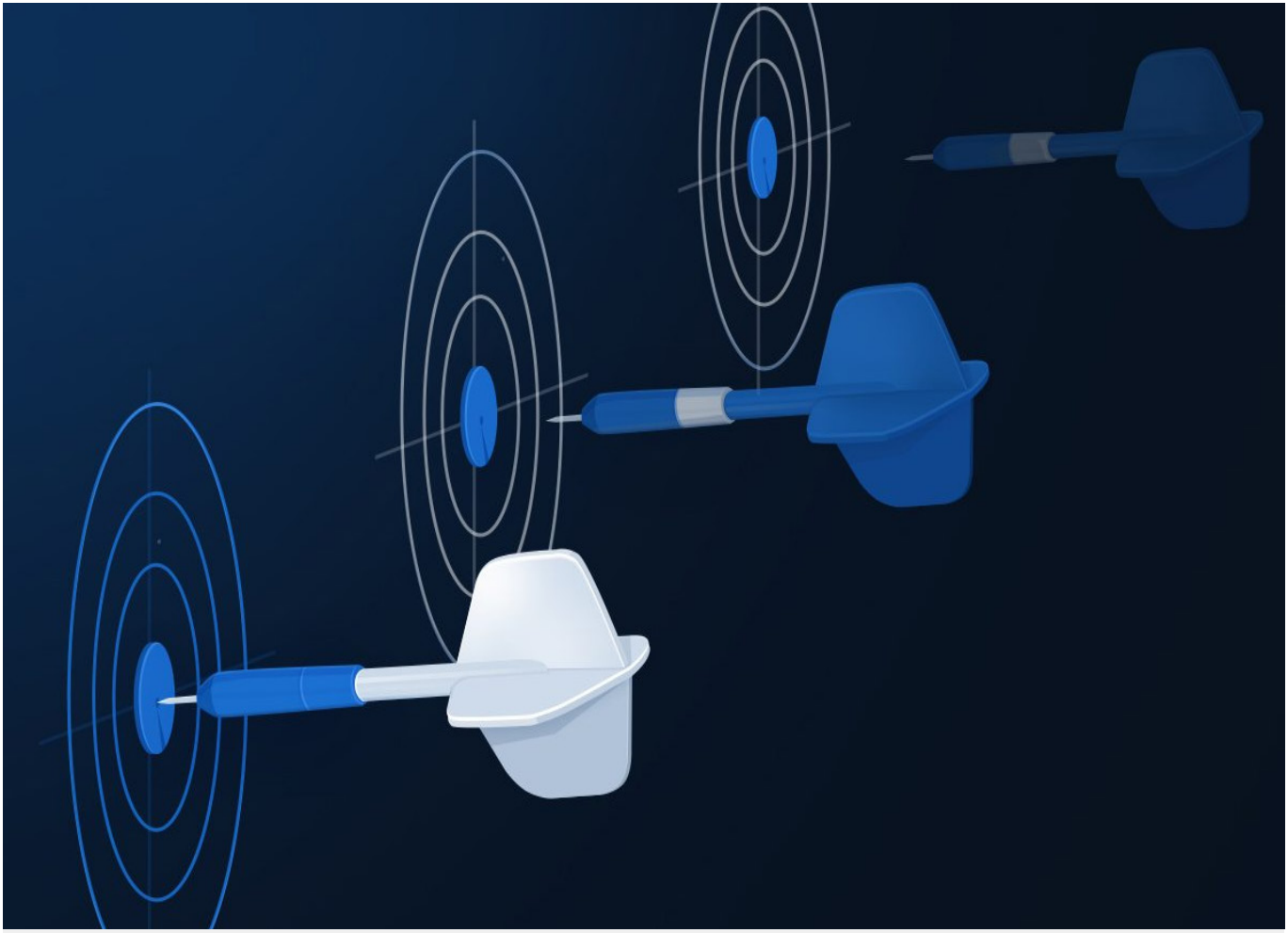


RESPONSIBILITY OF ONLINE RETAILERS FOR PERSONAL DATA - PERSONALIZED MARKETING (RETARGETING)

JPM | JANKOVIĆ POPOVIĆ MITIĆ

RESPONSIBILITY OF ONLINE RETAILERS FOR PERSONAL DATA - PERSONALIZED MARKETING (RETARGETING)
Publisher: JPM Janković Popović Mitić
Delta House, 8a Vladimira Popovića street
www.jpm.rs
Authors: Ivan Milošević, Partner
Design and prepress: JPM Janković Popović Mitić

Disclaimer:
The sole purpose of this publication is to provide information about specific topics.
It makes no claims to completeness and does not constitute legal advice.
The information it contains is no substitute for specific legal advice.

If you have any queries regarding the issues raised or other legal topics, please get in touch with your usual contact at JPM Jankovic Popovic Mitic.

Research of major global agencies shows that the realization of profit is proportional to the degree of trust that customers have in retailers, regarding the processing of their personal data. Retailers that consider themselves socially responsible should know that investing in the protection of customers' personal data is an added value for the company - this type of investment strengthens the trust of customers, contributes to strengthening the competitive position in the market and increases profit.

Most importantly, retailers have to understand that the personal data they collect from citizens is not their property and that the right to privacy is one of the elementary rights of citizens, which they are obliged to process in accordance with legal regulations.

Nowadays, anyone who understands the nature of doing business in the modern era, cannot imagine a world without advertising. The chain of online advertising (real-time bidding - RTB) includes online retailers, owners of e-commerce platforms, online platforms for offer and demand of ads, representatives of companies that offer advertising space and companies that want to advertise, data management platforms and platforms for automatic tracking of site visitors who follow ads and AdExchange platforms.

The advertising system is set up in such a way that companies, which have the best tools for automated monitoring of citizens' behavior on the Internet, will gain the upper hand at auctions "for selling profiles" (selling audience), that is, they will get the opportunity for advertising - sending personalized content. Companies which want to advertise their products sign contracts with companies which have the tools for tracking the behavior of citizens on the internet. When they create a profile of the user or visitor on an e-commerce platform or a website of an online retailer, their behavior is monitored on other websites in order to create the best possible profile. Such a profile is matched on AdExchange platforms with profiles that auction houses already have about those same citizens - in the end, the artificial intelligence system automatically sends personalized content to citizens.

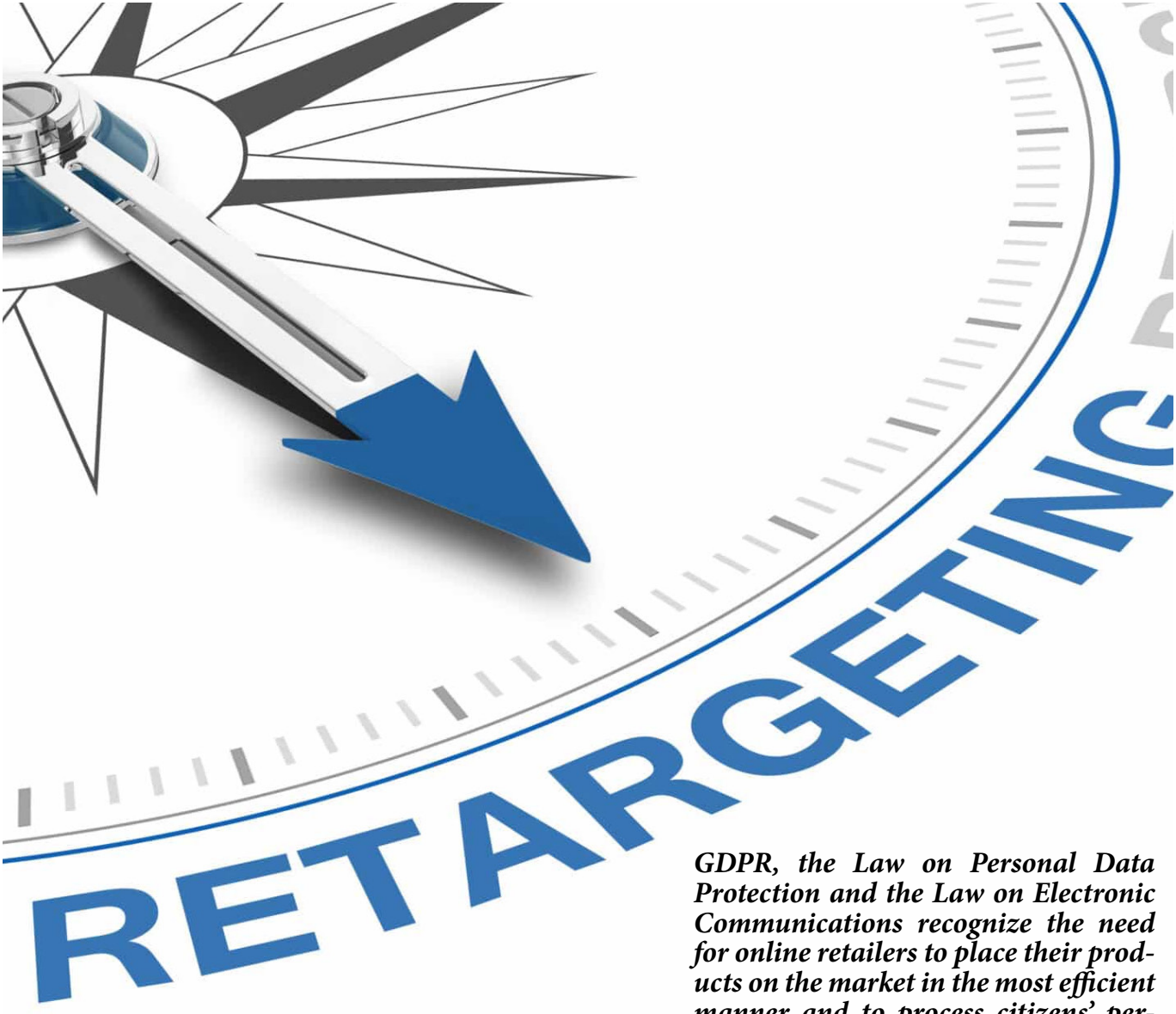
GDPR, the Law on Personal Data Protection and the Law on Electronic Communications recognize the need for online retailers to place their products on the market in the most efficient manner and to process citizens' personal data to achieve this goal. On the other hand, the regulations governing the protection of personal data require that citizens have control over their personal data because this right is inextricably linked to the right to privacy and dignity of citizens. Online retailers must inform the citizens in a simple and understandable manner, what they are doing with their personal data and divide and regulate the responsibility for the processing of personal data with partner organizations they hire to carry out personalized marketing.

Retailers usually do not understand that the use of cookies without collecting personal data of citizens, i.e. use of the so-called online identifiers - personal data that allow citizens to be identified and their behavior on the Internet to be monitored, is not possible. We base this position on the continuous cooperation of our team, which consists of attorneys at law and experts in information security and digital forensics, in the implementation of the GDPR and the Law on Personal Data Protection. The GDPR and the Law on Personal Data Protection explicitly define personal data as any data related to a natural person *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. In support of our claims are the recent decisions of the European supervisory authorities regarding the transfer of data in the so-called third countries - that AdTech companies do not anonymize the IP addresses of citizens, but rather perform pseudo-anonymization, therefore the GDPR and the Law on Personal Data Protection are applied. When hiring partner organizations to profile the behavior of visitors and customers on their websites and platforms, online retailers must in a privacy notice inform citizens on how their personal data is processed, in a clear language and in an accessible form. It is also necessary to inform data subjects on which partner organizations they hire and in what capacity, as well as to define mutual rights and obligations with partner organizations - conclude data processing agreements. In order to profile the behavior of customers on their websites and e-commerce platforms, retailers, in most cases engage partner organizations in the capacity of processors, because these organizations perform certain processing actions on their behalf.

In case of filing a lawsuit for damages due to the violation of rights of citizens prescribed by the law, retailers will be protected, because they will be able to prove before the court that they are not responsible for segments of processing they have no influence on. Online retailers will, in the privacy notice, in clear language and in an accessible form, inform citizens that they act as joint controllers with partner organizations, and instruct them which controller to contact for each segment of personal data processing. The distinction of responsibility is especially important because of the ongoing procedure against one of AdExchange platforms, for alleged violation of the provisions of the GDPR before the supervisory authority of Belgium.

Furthermore, it is necessary for consent for data processing via cookies to be obtained in the manner prescribed by the Law on Electronic Communications. Article 126 paragraph 3 of this law stipulates that the use of electronic communication networks and services for the purpose of storing or accessing data stored in the subscriber's or user's terminal equipment is permitted if the subscriber or user **is given clear and complete notice of the purpose of data collection and processing, in accordance with the law governing the protection of personal data, as well as that he was given the opportunity to refuse such processing**. Regarding the method of giving consent, the Law on Electronic Communications allows the use of the opt-out option, i.e., giving consent in the manner defined by EU Directive on Privacy in Electronic Communications before its amendment in 2009. We note that we have received the interpretation from the Commissioner that the Draft of the new Law on Electronic Communications prescribes a solution in accordance with the judgment of the European Court of Justice in case C-673/17.

Regarding the use of cookies by partner organizations – online retailers are obliged to obtain the consent of citizens for each of the cookies and to provide information on the purpose of collection and processing of personal data.



GDPR, the Law on Personal Data Protection and the Law on Electronic Communications recognize the need for online retailers to place their products on the market in the most efficient manner and to process citizens' personal data to achieve this goal.

This is in accordance with the requirement from the Law on Personal Data Protection that the consent for data processing must be "granular", i.e. detailed enough so that citizens can know which data processing they are consent to.

It is not enough to give citizens the opportunity to refuse different categories of cookies, but it is necessary to explain to them to which category each cookie belongs to (marketing, advertising, third party) and for which purpose it is used - referring to complicated cookie policies can make it difficult for citizens to understand the purpose of processing and to choose to give consent for the processing of personal data.

Finally, when personal data is processed for the purpose of personalized marketing, retailers are obliged to carry out Data Protection Impact Assessment (DPIA) - an assessment of the impact of processing activities on the rights and freedoms of citizens.

This obligation is prescribed by the Commissioner's Decision on the list of the type of personal data processing operations for which an assessment of the impact on personal data protection must be carried out and the opinion of the Commissioner for Information of Public Importance and Personal Data Protection must be asked for ("Official Gazette of RS", no. 45/2019 and 112/2020).

This decision stipulates that the assessment is carried out in case of i) the use of new technologies or technological solutions for the processing of personal data or with the possibility of processing personal data that serve to analyze or predict the economic situation, health, preferences or interests, reliability or behavior, locations or movements of natural persons and ii) processing of personal data which includes tracking the location or behavior of an individual in systematic processing of communication data generated by the use of telephone, internet or other means of communication.

There is no doubt that in the case of engaging partner organizations with the use of artificial intelligence systems for profiling the behavior of citizens on the Internet and sending personalized content, a DPIA assessment is required. The focus of the assessment is to identify the risks to the rights and freedoms of the citizens, the level of probability that such risks may occur in real-time, and measures to mitigate the risk to an acceptable level.

The substance of the assessment is to what extent retailers can protect citizens' personal data in a situation where they are unfamiliar with the artificial intelligence systems used by their partner organizations for the purpose of creating profiles and sending personalized content to citizens. Accordingly, the biggest challenge is the assessment of the risk, i.e. impact of algorithmic artificial intelligence systems, produced by third parties, on the rights and freedoms of citizens.

Risk of the impact of artificial intelligence systems on the rights and freedoms of citizens, in RTB processes of automated processing of personal data, can arise in all phases of the system's life cycle. According to the available information in the scientific community, 96 different risk factors with different impacts on the confidentiality, integrity and availability of personal data in the process of automated processing with profiling have been identified. Yet, a universally applicable framework and tool for such an assessment is not publicly available.

Therefore, to comply with the GDPR and the Law on Personal Data Protection, at least a more specific division of responsibilities of all participants in the RTB direct e-marketing system is required, with as much as possible clear and comprehensible information about the functionalities, methods of training the machine learning module and the types of algorithms applied in the artificial intelligence system.