Transparent scientific work
UDK 342.721:659.3/.4
DOI 10.7251/BLCMES1801112C
COBISS.RS-ID 7634200

IMPACT OF GDPR TO DIGITAL MEDIA

Jasna Čošabić[1]

Abstract

This paper shall analyze the impact of General Data Protection Regulation ('GDPR') to concept of business of digital media, having in mind their overwhelming presence and especially their impact to private data of their clients or customers. Special features that are going to be dealt with in this paper relate to processing of personal data by digital media under the GDPR, which include teritorrial scope of GDPR and its global applicability, type of personal data processed by digital media, profiling and behavioral advertising, options for consent, the use of cookies and geographical location. Purpose of their processing shall be analysed as well, with reflection to some important cases and examples. It relies on widely understood concept of digital media, including social media, online news portals, blog websites and shall pursue to point out to some crucial changes that that digital media are facing now, and that will affect their way of doing business, after the GDPR became operative on 25 May 2018.

Keywords: *personal data, cookies, consent, profiling, behavioral advertising, geolocation, GDPR,..*

Introduction-Teritorrial impact and digital media

The creators of General Data Protection Regulation[2] have envisaged its enormous influence to the protection of personal data not only in the European Union, but worldwide. The principle which leads to its global implementation is not a classic teritorrial competence, which is inherent in international law, when referring to teritory or teritorries of countries or jurisdiction of international organisations, but is a combination of teritorial and personal scope guaranteeing the protection of private data of persons in the EU. The crucial factor which brings the GDPR in play is that the persons whose personal data are at issue, are in the European Union, regardless of whether they are EU citizens or not, residents on any grounds, short visitors or travellers in transit.

It is applicable to both online and offline use of personal data. Having in mind the wide online access to digital media, there comes a question of teritorrial impact this regulation, which has been envisaged to cross the classic borders of international law according to Article 3 of the GDPR stipulating that it will apply to activities of an establishment of

1 Doc. dr Jasna Čošabić, CIPP/E, Banja Luka College

2 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) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

a controller or a processor in the European Union, regardless of whether the processing takes place in the EU or not.

As to the cross border activities of an establishement cases of Weltimmo case[3] and Google Spain case[4] should be underlined. The former one, Weltimmo, paved a road to consideration of what establishement is, grasping a less formal approach when deciding on teritorry of which country the establishement functions. It becomes less important where the establishement is formally registered, and more crucial where its business is directed to and performed. Thus, in this case, a real estate web page was registered in Poland, but used Hungarian language, had a bank account open in Hungary and a Post box there, so therefore it was considered as operating in Hungary as well. The same could be applied when considering social networks, online news platforms offering subscription to their customers, blogs offering regular updates to their readers and alike. Thus a website which functions outside of the EU but is accessible from the EU, is written on the language spoken in the EU, may be considered an establishment for the purposes of protection of personal data of customers in the EU. As to the language at least, having in mind that, for example, English is a widely spoken language, in the EU and outside of the EU, the impact of the GDPR is global. We may rather conceptualize the negative list of languages not spoken in the EU, not to be directed to persons in the EU, like a website running in chinese, japanese or arabian.

Google Spain case has already dealt with the spreading of teritorrial outreach of EU jurisprudence, asking for a global implementation of the 'right to be forgotten' in global internet access surroundings.

Apart from that, GDPR entails its impact to businesses worldwide whenever they process personal data by offering goods or services to persons in the EU, or monitor their behaviour when such behaviour takes place in the EU. With a view to digital media, this includes social media networks, targeted and behavioural advertising based on profiling on persons in the EU, placement of cookies, etc.

Personal data

Personal data are widely construed as any data which may be connected to a certain person, and according to GDPR, means any information relating to an identified or identifiable natural person. It includes the most obvious ones like name and family name, postal address, social security number, e-mail address, to less obvious ones like the IP address, geo-location, and tracking online behaviour through cookies, ammounting to profiling. GDPR especially protects sensitive data like health data, religious belief, ethnic background, biometric data. It is in general prohibited to process sensitive data, but GDPR leaves space for exceptions under strict circumstances defined by Article 9 of the GDPR, by introducing, inter alia, a more demanding consent which is 'explicit consent' (Article 9, para 2a). Certain data like a photograph may represent both a personal data, and a sensitive data, if it is construed as 'biometric data for the purpose of uniquely idenfying a natural person' (Article 9, para 1) through a specific technical means. For example if the intention

3 Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-230/14, judgment of 1 October 2015, Court of Justice of the European Union, http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN

4 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, Court of Justice of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

of the use of photograph is recognition of individual through machine readable formats, then it is sensitive data, and as such is used by passport controls for example. If the photograph reveals religious signs, covering of head or wearing of religious symbols, it may, under certain circumstances, count as sensitive data revealing racial or ethnic origin, religious beliefs. If the purpose of photograph is sharing memories by its owner then it is just a personal data. This is widely used by social media networks such as Facebook, Instagram, Google+ and alike.

However, what counts as private data will also evolve with the growth of information technologies.[5] Like the geo-location was not present in everyday life until several years ago, we may expect that with the growth of internet communications, the type of data which may lead to connecting certain person with the data will also expand. This relates especially to Internet of Things communication when processing data between devices may reveal location of devices, habits of persons owing them, and thus may trigger advertising towards those persons. Such communication may also reveal sensitive information of health data when Internet of things is used for communication of devices connecting a patient needing constant monitoring of his heart rate or a dosage of terapy, and base hospital. In the hands of advertisers such data could trigger also bombarding of patients with medical ads, etc. Having in mind that advertisers often use the ad space from the webpages of digital media, it also spreads the responsibility of digital media as well.

Use of personal data by digital media

One of the first questions which comes out when speaking of compliance with GDPR of any controller, including digital media, is what is the purpose of the personal data processing.

Processing itself is every use of personal data, which may entail access to personal data, publishing, even mere keeping and storing personal data, reading personal data etc. According to Article 4, para 2 of the GDPR 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

Purpose of processing is the reason which stands behind such use of personal data. It implies that persons are sovereign holders of their data. For each use of personal data there must be a clear and visible purpose, and only for that certain purpose they may let other entities use their data. Purpose and means of processing data is determined by controllers of processing. On the other hand, processors are processing the data on behalf of the controller. They do not determine the purpose of processing, but they just enforce the processing. As to digital media, they are clearly controllers of processing data and they are responsible for ensuring that processing is in accordance with the principles of GDPR and especially that it is lawful.

Purpose must always follow the type of data required, meaning that only the data which is necessary for the said purpose may be required from the data subject, in line with the principle of data minimisation. For example, web news portals or blogs may offer their

5 Alan Calder, EU GDPR, A Pocket Guide, P. 63, IT Governance Publishing, Cambridgeshire, 2016

readers to subscribe to their editions, and in that regard a reader, data subject, is invited to leave his e-mail address in order to be provided with such editions and to give consent therefor. The e-mail address as a personal data is connected to its purpose, which is sending news editions. However, requiring for example a telephone number, ethnic origin, postal address (if not intended for sending hard copies) comes out of the scope of purpose of processing of personal data, which would render such processing illegal.

The same would come for offering of free subscriptions but requiring bank card number, or offering a free one-month trial and requiring a bank card number before such free trial. Compliance with the GDPR would entail cooperation of legal part of the establishement with the IT, the later having to find technology solutions to proper legal requirements. In the above example, this would entail requiring bank card number at the end of one-month free trial provided that the data subject wishes to continue to use the service, and this time to pay for it. Such a cooperation between law and IT is was presented in 90's for the first time as a concept by Ann Cavoukian, who oulined a 7 foundational principle of the privacy by design what was acknowledged and gained a crucial place in the protection of privacy, on the 32nd International Conference of Data Protection and Privacy Commissioners in 2010 in Jerusalem, when Resolution on Privacy by Design was adopted.[6] One of those principles, 'Privacy Embedded into Design' means that every legal requirement of privacy protection has to be accompanied by certain practical IT solution. It has to be inherent to digital media by visually clear solutions. GDPR has recgnized the importance of privacy by design and incorporated it into one of its requirements for the respect of private data, making the controller responsible for introducing technical and organisational measures, in order that data-protection principles be respected, in accordance with Article 25 of the GDPR. This comes especially into play when speaking of one of the most used grounds for processing of personal data when digital media are cocerned, the consent.

Subscription to online media portals is the first and most visible mode of using personal data. Another less visible way of using personal data is storing internet protocol addresses - IP addresses. According to the Court of Justice of the European Union ('CJEU') IP address also counts as personal data. IP address connects the device/computer the data subject is using with the data processor, or the entity recognizing that address. IT may be static or dynamic which changes with each connection to network. In its judgment of Breyer v. Germany[7], the Court of Justice of the European Union decided that even a dynamic IP address may present in certain circumstances a personal data. The CJEU held that in order that a dynamic IP address is a personal data, when the provider 'has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.' What is important about this judgment is that has drawn the attention to the fact that even not obvious signs of recognition of personal data, such as IP address and especialy dynamic one, may, if a person could be linked with it, present personal data. Therefore it comes under the auspices of the GDPR and every collection and storing of IP addresses must be done in accordance with it.

6 32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel 27-29 October, 2010, Resolution on Privacy by Design, https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

7 Breyer v Bundesrepublik Deutschland, Case C-582/14, Court of Justice of the European Union, http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

Social networks are probably the biggest databases of voluntary presented data which are not governed by states, i.e. not in public interest. As such, governing private data is a very sensitive issue, and a lack of carefully designed and implemented privacy policy may lead to high fines according to GDPR, and a loss of trust by its users. Recent affair with Cambridge Analytica and Facebook drew the attention of public of how powerfull weapon private data may be and the necessity of strict compliance with privacy standards.[8] The responsibility of social networks but also of administrators of fan pages run by these networks, as controllers, was recently determined by Facebook CJEU judgment[9], which pointed out that not only social networks are controllers of personal data but administrators of fan pages as well, putting on them an obligation to be compliant with data protection requirements.

With that in mind, the webpages of news portals for example, offering subscription to their readers, or placing cookies on their equipment are conrollers of data processing. But having in mind that they allow third parties to place advertisements to their pages, they also come take the place of controllers, when for example, place their, third party cookies[10] to terminal users equipment.

Therefore a privacy policy, together with a cookies policy has to be carefully designed and implemented throughout the webpage of a digital media. To that extent the concept of 'privacy by design', which conemplates the principles of protection of personal data embeded in design of a web page, is of a special importance.

Profiling, tracking behavior and targeted advertising

Profiling is often used by digital media for the purpose of targeted advertising. On the grounds of observation of person's preferences and habits, a special profile is being created in order that targeted advertising can be performed. According to Article 4 of the GDPR "profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'. It usualy consists of several stages, including collection of data, then 'mapping together' the collected data and its correlation and assembling of data and creation of user's profile, making behavioural technicques emerging into a new behavioural science[11].

Profiling is, in todays society of advertising, is very widely used and will have to go through crucial changes in order that the privacy is protected and that high standards of GDPR are observed. Profiling and behavior-based tracking, is generally recognized as a great risk to privacy, as it can be technically done even without the knowledge of data su-

8 See for example https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/

9 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, Court of Justice of European Union, judgment of 5 June 2018, http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN

10 See for example Eduardo Ustaran, p. 326

11 Chapter 2
On-line Behavioral Tracking: What May
Change After the Legal Reform on Personal
Data Protection, Georgia Skouma and Laura Léonard, © Springer Science+Business Media Dordrecht 2015 S. Gutwirth et al. (eds.), Reforming European Data Protection Law, Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8__2, page, 37, 38

bject. So not only that it is possible to perform it without consent, but can also imperceptible[12], and as such very dangerous.

Tracking behavior of data subjects is also a form of collecting personal data. Digital media very often for marketing purposes rely on tracking behavior of persons, their visiting web pages, through which their interests may be seen, resulting in offering marketing ads (for ex. pop-up ads) to data subjects. Tracking behavior is something that brings GDPR accross borders of the EU, under Article 3 para 2(b) of the GDPR, meaning that processors not established in the EU shall have to be compliant with it when their processing activities are relating to monitoring of behavior of data subjects, when such behaviour takes place within the Union. GDPR sees 'profiling' as a way of processing personal data and provides that the data subject should be informed of the existence of profiling and the consequences of such profiling (Recital 60). For informing data subject on profiling controllers should use standardised icons that are easily visible, intelligible and clearly legible, and if they are presentated electronically, they should be also machine-readable (Recital 60). Furthermore, if controllers, in this case digital media, process the personal data for the purposes of digital marketing, data subjects should have the right to object to such processing, clearly explained and visible to them (Recital 70). In praxis, it is recommendable that digital media approach persons or data subjects informing them of the intention of sending digital marketing ads with a clear opt-in option. In any case, data subject should have a simple posibility to opt-out, from any use of his personal data, including sending marketing ads, as easily as it was to opt-in.

Targeted advertising is one form of tracking behavior of individuals, which is based mainly on placement of cookies to their devices, which as a result reveals aptitudes, preferences or inclinations of individuals as on the use of goods and services and enables more individualized advertising in form of pop-ads or alike. However, through targeted advertising, the entity that carries it, may connect that behavior to a certain individual and thus interfere in his/her privacy and personal data.

Speaking in the context of publishers, an attention has to be drawn to third party advertising especially when it relates to third party cookies placement on visitors to the first mentioned publisher websites. One form of behavioural advertising may lead to publishers selling their space to display ads on their websites, as recognized by Article 29 Data Protection Working Party (A29 Party)[13]. A third party displaying ads, usually places cookies to users' terminal equipment, which enables them to track behavior for the reason of behavioral advertising. One of the information retrieved on that way is information about the user's geolocation which plays important part in profiling for the purposes of behavioral advertising. EPrivacy Directive of 2002[14] has brought the concept of a clear and comprehensive information that has to be served to the subscriber or user when the information is stored on his terminal equipment, and that he is also given the right to refuse such processing or storing the information. (Article 5 para 3). This has been strengthened by the

12 See, Gritzalis Dimitris, Furnell Steven, Theoharidou Marianthi, Information Security and Privacy Research, Springer, International Federation for Information Processing, 2012, p 236

13 Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising of 22 June 2010, https://iapp.org/media/pdf/resource_center/wp171_OBA_06-2010.pdf

14 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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=en

amendments to EPrivacy Directive of 25 November 2009[15] according to which the storing of such information to terminal equipment of the subscriber or user is allowed only when he has given his or her consent, having been provided with clear and comprehensive information, which amounts to prior and informed consent of users in order that such information like cookies are placed on his/her device.

Cookies

Tracking behavior leads us to the use of cookies. Cookies usually refer to a small text file delivered by a website server onto the computers of visitors to its website.[16] From the aspect of privacy, it is relevant that cookies enable website to recognize the person or to track its internet behavior, preferences, habits and alike.

Cookies may be used either to create better access to website to its user or to perform targeted advertising. In the first case, cookies may enable better quality functioning of the website for the particular user by remembering his previoulsy chosen options such as language choise. As to advertising, cookies may track internet behavior of the user and accordingly offer him services or goods, in line with his interests. Having in mind especially the latter, by using cookies, websites track and remember behavior of users on the internet and in that light interfere in his private zone. Therefore user must consent to such interference.

The ePrivacy Directive of 2002 introdues the consent requirement for cookies and according to Article 5 para 3 of the ePrivacy Directive 'Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.' The ePrivacy Directive also recognized the usefulness of cookies and contended that 'they can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information..' (Recital 25 of ePrivacy Directive of 2002). The ammendments to the said Directive in 2009 drew attention that users should be informed of cookies and about the right to refuse the cookies in a user-friendly way (Recital 66), with the exception of the right to refuse when there is a legitimate purpose of use of the services ans explicitly requested by the subscriber or user. What is also important, as it is often seen as a praxis of

15 DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

16 See for example Eduardo Ustaran Data Protection Law and Practice

digital media is that these ammendments allowed for expressing the user's consent by using the appropriate settings of a browser. So, it may be considered that when users have the possibility to set their browser as to refuse cookies that they do not wish, their consent was expressed. However it should be taken into consideration that WP Article 29 has rightfully drew attention to the wide use of browsers settings as a way to compliance with consent requirements and the possibility of 'click fatigue'.[17] The users must know of this possibility of browser settings, and furthermore that it should be more appropriate for consent to have browsers which actively have to be set in order to receive cookies and not vice versa.

The responsibility for placement cookies was accentuated in the latest Facebook judgment[18]. The Wirtschaftsakademie Schleswig-Holstein in Germany, which is an education institution, was using Facebook fan pages for the promotion of its activities, however, it was ordered by a supervisory authority under the Directive 95/46, to deactivate the page, under the threat of penalty payment, because neither the Wirtschaftsakademie nor the Facebook have informed visitors that Facebook collected their personal data by means of cookies.[19] Cookies are being placed for duration of two years with the intention of targeted advertising by Facebook and for the administrators of the fan page to obtain statistics from the visits to the page in order to further promote its activities. (see para 33 and 34). The administrator of the fan page gives the Facebook opportunity to place cookies of persons visiting the page, regardless whether they have a Facebook account or not (para 35). The conclusion of the CJEU is that even the administrator of a fan page hosted on a social network is to be considered as a controller under Article 2(d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This important judgment spreads out the responsibility for eventual data breaches, in this case, placement of cookies without previous informing or consenting the visitors, to administrators of social networks as well, and opens a much wider approach towards controlling of data breaches.

Geolocation

Location data may be extremely valuable for targeted advertising. Individuals often use social networks and place themselves information on their location, by tagging or sending photographs. However, location data is a private data. Therefore, protection attributable to private data by GDPR spreads on location data as well. Privacy by design is very important speaking of geolocation data. Users of mobile devices must be able to turn off location recognition parameters should they chose to. Transmission of geolocation unknowingly from mobile devices and contrary to users opt-out selection, leads to privacy breaches. Once, tracking of a person's movement was a matter of police and interior authorities upon very scrutinized procedure, which had to have legal grounds like the prevention of crimes, which is considered as permissible interference in right to respect to private life under the Article 8, para 2, of the European Convention for the Protection of Human Rights and

17 Data Protection Working Party Article 29, Guidelines on consent under Regulation 2016/679, of 10 April 2018.

18 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, Court of Justice of European Union, judgment of 5 June 2018, http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN

19 para 16 of the judgment above

Fundamental Freedoms, which is interference proportionate to the protection of public interest. However, in todays world of personalised information technologies allowing simple automatic tagging of location, this aspect of privacy must also be properly protected. This regards social networks using geolocation, news portals enabling advertising, etc. Thus, when the user gives his consent for the use of geolocation for a certain purpose, this purpose cannot be extended beyond his original consent. For example, if user searched for a local news portal in order to get informed about any traffic problems near his location, and later gets a series of ads on local restaurants, clubs, shops, his geolocation was used beyond his consent and beyond the original purpose for which he enabled the use of his geolocation data. The same applies when the user tags his location on a social network, in order to inform his friends of his whereabouts, but then gets load of ads on local events. So, the media portals must not use the geolocation information beyond the prior and informed consent of the use in order to be in line with the high demanding principles of the GDPR and other privacy standards.

Consent

GDPR provides for 6 lawful grounds for processing of personal data, but as digital media is at issue, the consent of the data subject takes the leading role.

Consent for processing of data is to be given by data subject above certain age whose data are to be processed. However, the consent, as a form of free will disposition, has to be freely given, specific, informed and unambiguous.

This presumes that whenever consent is a required legal ground for the processing of personal data, data subject or a customer must be informed on the purpose of giving his/her data. This consent cannot be presumed from the fact that customer uses the services, it has to be specific. Consent has to be given for every purpose of data disposition and the mode of giving consent may be by written statement, electronic means, or an oral statement, ticking a box at internet website, choosing technical settings for information society services. It is important that silence of user is not considered as consent. Pre-ticked boxes must not be offered by a webpage needing user's consent. (Recital 32 GDPR). The information given to the user on the reasons of requesting consent, must be presented in a clear and visually friendly way. As much easy and simple it is to give the consent, equally simple and easy must bi to withdraw consent by the data subject.

In order to inform data subject of the processing in un understandable and structured manner, layered approach may be used. Layered approach may include existence of two or more layers behind a consent opt in. Each layer offers a more thorough information on the processing purpose.[20] Regarding consent for cookies, a nice and structured multiple choice could be a good solution.

Oracle website offers an excellent example of multiple choice layered approach. It divides cookies to required ones, functional and advertising cookies, and behind each option there is a visual explanation of what it entails.

20 See for example Eduardo Ustaran, European Data Protection Law and Practice, IAPP 2018, page 152, 153

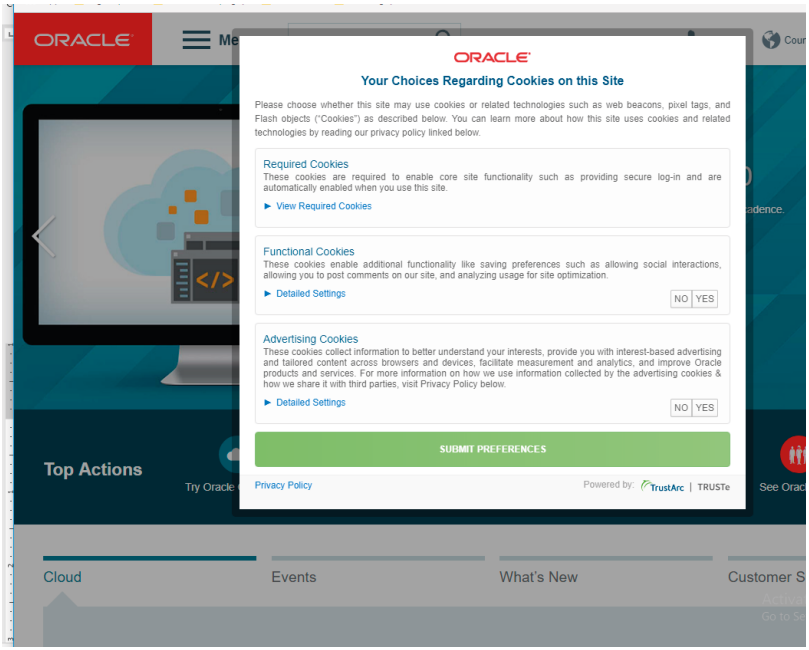

Image No. 1[21]

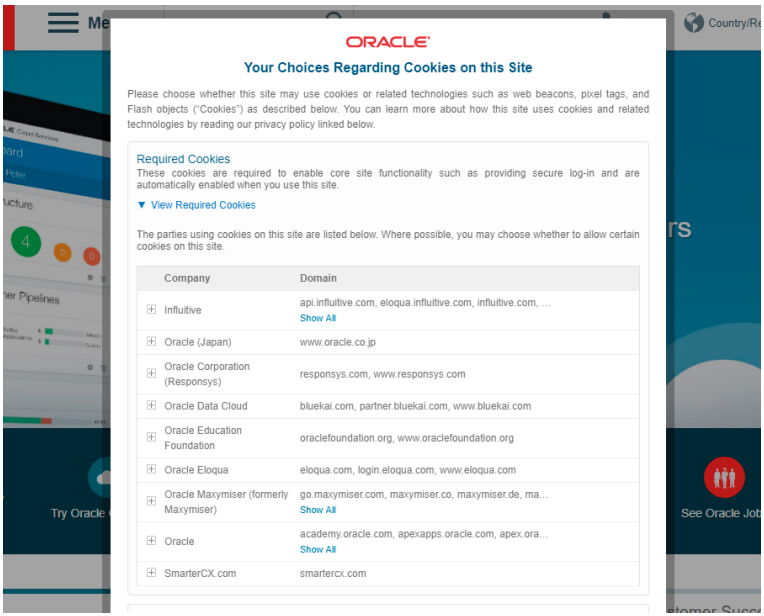

Image No. 2[22]

21 https://www.oracle.com/index.html
22 https://www.oracle.com/index.html

Salzburg traffic web page offering buses schedule, offers the option of 'All cookies allowed for the best browsing experience' and 'Only functional cookies allowed', placing data subject in a position to chose what is the best option for him/her.

Image No. 3[23]

When using cookies, it is important that the webpage offers cookie policy together with privacy policy, where it explains the purpose of placing cookies to terminal equipment of the user and what the user could expect from having cookies.

If webpages of digital media are used by third parties, who may also place their cookies, then digital media has also responsibility for third party compliance with cookie requirements. A nice example is the web page of a news portal express.co.uk, with images below, which first offers users to continue and accept all cookies and at the same time provides link to cookie policy and privacy policy. Under cookie policy, it also gives links to cookie policy of its partners, which are third parties in this case. What can be seen as a minus, is that it only offers the acceptance of all cookies, without diversifying them to functional, without which the user would not be able to correctly use the page, and others. All are functional.

23 https://salzburg-verkehr.at/

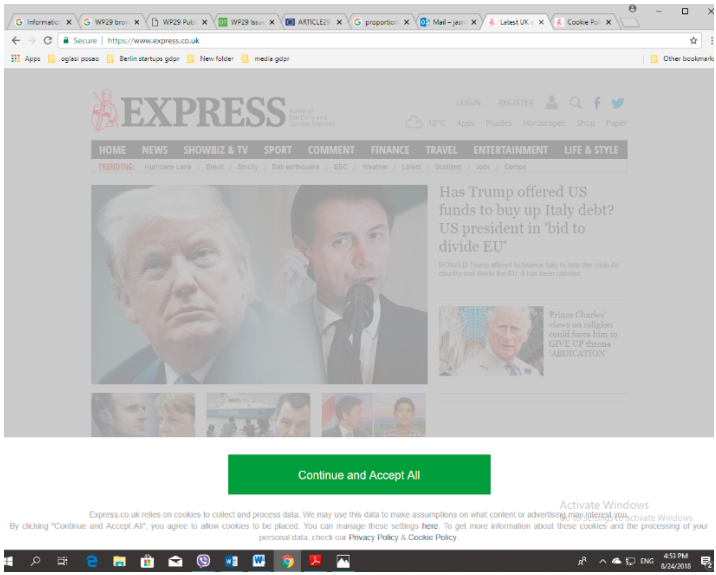

Image No. 4[24]

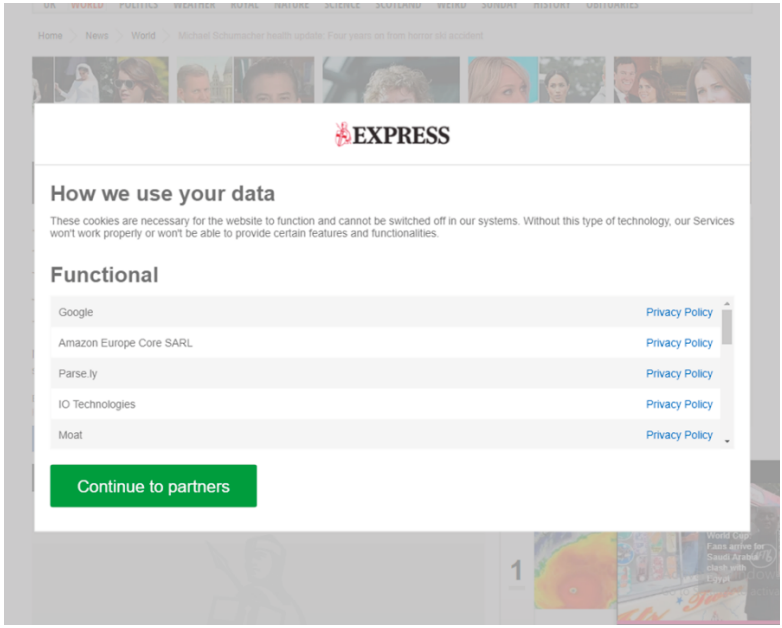

Image No. 5[25]

On must bear in mind that certain space as lawful ground for processing of personal data for direct marketing purposes is left to legitimate interest groud under Recital 47 and

24 www.express.co.uk
25 ibid

Article 6 para 1 (f) of the GDPR. The interests of data subject and of his rundamental rights and freedoms must not be overriding. It is suggested that such legitimate interest exists when tehre is an appropriate relationship between the data subjectg and controller, when data subject is a client or in the service of hte controller, but this anyway requires a carefull assesment. It is substantive that a data subject has reasonable expectations as to processin of his private data at a certain point. Information Commissioner's Office of the Uinited Kingdom ('the ICO') points out that three elements are incorporated in the legitimate interests provision of the GDPR, suggesting a following test to be applied. The first one is a 'Purpose test' - inquiring as to whether there is a legitimate interest behind the processing. Second one is 'Necessity test' – inquiring whether the processing is necessary for that purpose and finally a 'Balancing test' of whether the legitimate interest is overridden by the individual's interests, rights or freedoms.[26] The ICO relied on the Rigas case of the Court of Justice of the EU, which points out to specific circumstances of the particular case[27].

Therefore, processing of personal data used for marketing purposes should not be a disturbance to users. In the example where a person looks for a restaurant and gives out location details for that purpose, being bombarded by tons of advertising offers from other services then restaurants, shops, fast food, etc. may come out of this concept. Sending advertisement by a restaurant might be acceptable and have a legitimate interest and expected by the data subject. However, on first sending such advertisement this restaurant should offer an opt-out possibility from sending this advertising. This could be seen as a balancing approach.

Conclusion

Overwhelming presence of digital media and their processing of personal data of its clients and users, require carefully established procedures and respected privacy standards. GDPR sets high standards of respect of personal data and places high fines for those making privacy breaches. Having privacy policy and cookie policy adopted and available to users may be a first step towards compliance. However, a thorough privacy by design principle should be embedded in every step of using private data, which should come as a result of continuous efforts on the sides of both legal and IT teams of digital media. Constant awareness by digital media of personal data protection requirements and their thriving to get complied with the GDPR will not only make them avoid penalties but most importantly will build trust by their users.

References:

1. 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)https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

26 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

27 Rigas case, Case C-13/16, Court of Justice of the European Union para 31, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1515682033041&uri=CELEX:62016CJ0013

2. Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C−230/14, judgment of 1 October 2015, Court of Justice of the European Union, http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN
3. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, Court of Justice of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN
4. Alan Calder, EU GDPR, A Pocket Guide, P. 63, IT Governance Publishing, Cambridgeshire, 2016
5. 32nd International Conference of Data Protection and Privacy Commissioners
6. Jerusalem, Israel 27-29 October, 2010, Resolution on Privacy by Design, https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf
7. Breyer v Bundesrepublik Deutschland, Case C−582/14, Court of Justice of the European Union, http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN
8. https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you--need-to-know/
9. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Case C−210/16, Court of Justice of European Union, judgment of 5 June 2018, http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN
10. Chapter 2 On-line Behavioral Tracking: What May Change After the Legal Reform on Personal
11. Data Protection, Georgia Skouma and Laura Léonard, © Springer Science+Business Media Dordrecht 2015 S. Gutwirth et al. (eds.), Reforming European Data Protection Law, Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8__2
12. See, Gritzalis Dimitris, Furnell Steven, Theoharidou Marianthi, Information Security and Privacy Research, Springer, International Federation for Information Processing, 2012,
13. Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising of 22 June 2010, https://iapp.org/media/pdf/resource_center/wp171_OBA_06-2010.pdf
14. Eduardo Ustaran, European Data Protection Law and Practice, IAPP 2018
15. 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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=en
16. DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
17. Data Protection Working Party Article 29, Guidelines on consent under Regulation 2016/679, of 10 April 2018.
18. https://www.oracle.com/index.html
19. https://salzburg-verkehr.at/
20. www.express.co.uk
21. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/
22. Rigas case, Case C-13/16, Court of Justice of the European Union para 31, https://eur- lex.europa.eu/legal-content/EN/TXT/?qid=1515682033041&uri=CELEX:62016CJ0013