INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 04 Issue 08 August 2021

DOI: 10.47191/ijmra/v4-i8-17, Impact Factor: 6.072

Page No.- 1187-1192

To What Extent are Consumers Harmed in the Digital Market from the Perspective of the GDPR?

Ammar Younas[1], Bakhodir Tohir ogli Mirzaraimov[2]

[1]Ph.D. (Candidate), School of Humanities, University of Chinese Academy of Sciences Beijing China

[2]Lecturer, Tashkent state university of law

ABSTRACT: The European Union has recently enacted a new law, the General Data Protection Regulation (GDPR),[1] which is designed to strengthen existing data protection legislation in the EU. The selection of Regulation itself as a legal instrument makes the GDPR stronger than Directive as it ensures a uniform and consistent implementation of rules thereby, consolidating the EU digital single market. The GDPR reforms existing data protection policy by imposing more stringent obligations on not only data controllers but also on data processors relating to obtaining a valid consent,[2] ensuring transparency of automated decision-making[3] and security of data processing,[4] and by providing new rights for data subjects. Data subjects are entitled to withdraw their consent,[5] request their data to be transferred to another data controller[6] or to be deleted.[7] Also, the GDPR includes certain principles aimed at regulating its cross border transfers of the EU citizens' personal data to ensure a high level of protection outside the EU.[8] Taking into account the above mentioned policies along with others, some scholars describe the GDPR as 'the most consequential regulatory development in information policy in generation' that has teeth.[9] However, the GDPR cannot be claimed as a legal instrument that effectively deals with all threats of the digital market to consumers. This paper argues that although the GDPR has considerably expanded the rights of consumers thereby, enabling them to regain control over their personal data to certain extent, the effectiveness of its principles is limited and cannot ensure full security of data processing. Firstly, it examines the effectiveness of consent principle of the GDPR in empowering consumers to control over their data and make a genuine choice. Secondly, it analyzes "data control-rights" of consumers. Finally, it comprehensively discusses extraterritorial application of the GDPR and regulation of international transfers of data.

Consent under the GDPR

Certainly, consent constitutes one of the most common legal grounds for data processing among other six legitimate justifications embodied in the GDPR.[10] The GDPR sets procedural as well as substantive requirements for consent to be valid in order to protect interests of consumers in the digital market. In particular, consent must be 'freely given, specific, informed and unambiguous indication of the data subject's wishes' and represent "a statement" or "a clear affirmative action".[11] Each of these conditions is supposed to increase quality of consent.

[1] The European Parliament and the Council Regulation (EU) 2016/679 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) [2016] OJ L 119/1

[2] Ibid Art.4 (11); Art.7; Art.9

[3] Ibid Art.22

[4] Ibid Art.5;Art.28

[5] IbidArt.7 (3)

[6] Ibid Art.20

[7] Ibid Art.17

[8] Ibid Art. 3; Art.42; Art.44-46

[9] Hoofnagle and Borgesius (n 1) 65

[10] The GDPR (n 4) Art. 6 (a)

[11] Ibid Art.4 (11)

Firstly, "freely given" consent means that data subjects must make a genuine choice by granting their consent voluntarily without interference of any pressure or any other factor, which can impact on the outcome of that choice.[12] In practice, this principle should prohibit prevalent online services based on take-it-or-leave-it conditions or "tracking walls" concerning privacy.[13] Consumers are commonly required to agree to the use of data in exchange for gaining access to services. For instance, typical email and social network sites provide access to these services only if individuals tick consent boxes (terms and conditions) thereby, agreeing to the collection and processing of their data. Also, many websites employ a tracking wall as a means of collecting user's consent to tracking by third parties (such as advertisers), which is also known as a "cookie wall" – an obstacle to the content of the website that can be removed only by visitors' consent.[14] Such websites usually collect massive amounts of consumers' data including browsing behavior and typically use them for targeted advertising. When consumers confront with these types of conditional access to online services, majority of them are likely to click "I agree" in order to be able to utilize services[15] which cannot be described as a "freely given consent".

According to the article 7 of the GDPR, to evaluate whether consent is voluntarily given, it must be taken into account whether a service is dependent on consent of the users.[16] Tracking walls can be prohibited through the application of this principle. However, the GDPR does not expressly mention that take-it-or-leave it strategies of online services by all means result in invalid consent rather, it provides that "utmost account shall be taken" of whether a service is dependent on data subject's consent.[17] Nevertheless, certain recitals of the GDPR clarify its position regarding these strategies of collecting consent. Recital 43 states that in specific cases, where there is an explicit imbalance between the data controller (company) and the data subject, data subject's consent can be deemed to be involuntary.[18] For example, when a giant company such as Instagram uses personal data of its users based on consent, it can be claimed that its users may consider that they have no choice to consent due to the lack of balanced bargaining power. Moreover, recital 42 suggests that consent should not be deemed to be voluntarily granted in case the data subject is unable to reject consent without damage.[19] If not being allowed to use particular online service is considered to be "damage", this recital is supposed to invalidate consent collected depending on take-it-or-leave-it conditions. However, recitals do not have a legally binding effect and they are mainly used for interpretation. Therefore, the effectiveness of recitals can be examined only through decisions made on cases relating to this topic.

On the first day of the GDPR's enforcement, NOYB, non-profit organization has entered four complaints against giant companies such as Facebook, Instagram, WhatsApp and Google (Android) to the Data Protection Authorities (DPAs) of Austria, Belgium, Germany and France accordingly.[20] The complaints were related to the take-it-or-leave-it strategies of these services.[21] While three complaints are still under consideration, the French DPA imposed a penalty of fifty million Euros on Google for the lack of legitimate basis for targeted advertising.[22] It found that making the creation of Google account conditional on the acceptance of "terms of service" and "privacy policy" led to invalid consent because the users had to accept all types of personal data processing carried out by the company.[23] Google appealed the judgment before the French Administrative Court, which is still in process. If the other complaints also become successful, it will have a revolutionary result in practice, which can lead to the demise of non-negotiable privacy policies of giant companies.

Secondly, in order for consent to be "informed and specific", at the time of requesting consent, controller must inform the data subject at least about details of controller, types of data being used, methods of processing, and clearly express the purpose of the data use as a protection against "function creep".[24] With the information provided the data subjects must be able to easily

[12] 'GDPR: Consent'(*Intersoft Consulting*) <https://gdpr-info.eu/issues/consent/#:~:text=GDPR%20Consent,has%20consented% 20to%20the%20processing.&text=Consent%20must%20be%20freely%20given,given%20on%20a%20voluntary%20basis.> accessed 15 July 2020

[13] Hoofnagle and Borgesius (n 1) 79

[14] Frederik J Zuiderveen Borgesius and others 'Tracking Walls, Take-it-or-Leave-Choices, the GDPR and the E-Privacy Regulation' European Data Protection Law Review (2017) 3 (3) 3

[15] Ibid 6

[16] The GDPR (n 4) Art. 7 (4)

[17] Borgesius and others (n 19) 8

[18] The GDPR (n 4) recital 43

[19] Ibid recital 42

[20] 'GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook' (*Noyb* 25 May 2018) < https://noyb.eu/en/gdpr-noybeu-filed-four-complaints-over-forced-consent-against-google-instagram-whatsapp-and> accessed 15 July 2020

[21] Ibid

[22] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC. para.189 <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> accessed 15 July 2020

[23] Ibid para. 157

[24] 'GDPR: Consent' (n 15)

perceive processing operations that they are subject to.[25] According to article 29 Working Party (WP), in order to satisfy the requirement of "specific", data controllers seeking consent for several unrelated purposes should provide a separate request for each purpose thereby, enabling users to grant specific consent.[26] For example, if service providers intend to use personal data for purposes (personalized advertising) other than necessary for a particular service offered, they should provide separate tick-boxes to obtain specific consent for personalized advertising.

Lastly, "unambiguous" element requires the consent to be expressed through "a clear affirmative act" or "a statement".[27] Recital 32 suggests that in practice, making a statement or ticking a box can be considered as unambiguous consent that explicitly shows approval of data use for a particular purpose.[28] Moreover, a strong argument is included in recital 32, which claims that 'silence, pre-ticked boxes or inactivity should not constitute consent'.[29] In recent *Planet 49* case, this statement is fully approved by decision of the European Court of Justice.[30] The case concerned online promotional lottery established by Planet 49, where there was a pre-selected box involving consent to tracking based on cookies used for targeted advertising, followed by click button for playing the lottery.[31] Although it was pre-selected, it was not conditional on playing the lottery and required users to deselect so as to reject the request.[32] The ECJ held that "clear affirmative action" refers to active behavior made by the data subject that is necessary for lawful consent, and therefore, pre-ticked boxes are not sufficient.[33] Thus, the prohibition of silence, pre-selected boxes and the condition of active behavior enhances consumers' control over their personal data.

The Rights of Data Subjects under the GDPR

The GDPR has introduced several novel rights for data subjects, which are designed to increase consumers' control over their personal data in the digital market: the right to data portability,[34] the right to withdraw consent[35] and the right to be forgotten.[36] This section thoroughly discusses each of these rights to evaluate their effectiveness in protecting consumer rights to privacy.

The right to data portability can be divided into two principles. The first principle entitles individuals to receive a copy of their personal information from data controllers.[37] Accordingly, this principle allows them to investigate whether their personal data are legally processed by the data controller or not. The second principle provides users with the right to ask the controller to transfer their personal data to another controller where it is technically possible.[38] For instance, Facebook users can transmit their data to Google without any barrier. Thus, these two principles can considerably contribute to strengthening individuals' control over their data. However, there are certain limitations of the right to data portability. In particular, it only applies to personal information that has been given to the data controller.[39] But it does not mean that the portable data are limited to the actual data provided by the users for subscribing such as name, nationality, age and e-mail address. Rather, it also includes personal data collected by tracking a user's activities such as search practices, browsing history and location data.[40] Nevertheless, where the controller creates particular data depending on the information provided by the users, such data including a user profile cannot be made portable.[41]

Another novel right introduced by the GDPR is the right to withdraw consent, which entitles the data subjects to revoke their consent at any time.[42] Before giving consent, the data subjects must be informed about their right to withdraw consent by the

---

[25] Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679* (10 April 2018) 14

[26] Ibid 12

[27] I.Van Ooijen and Helena U. Vrabec 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from A Behavioural Perspective' Journal of Consumer Policy (2019) 42 (91) 100

[28] The GDPR (n 4) recital 32

[29] Ibid

[30] Case C-673/17 *Planet 49* [2019] ECLI-801 in Klaus Wiedemann 'The ECJ's Decision in "Planet 49" (Case C-673/17): A Cookie Monster or Much Ado about Nothing?' International Review of Intellectual Property and Competition Law (2020) 51 (4)

[31] ibid

[32] ibid

[33] ibid

[34] The GDPR (n4) Art.7 (3)

[35] Ibid Art.20

[36] Ibid Art.17

[37] Ibid Art. 20 (1)

[38] Ibid (2)

[39] 'Right to Data Protability' (*Information Comissioner's Office*) < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/> accessed 20 July 2020

[40] Ibid

[41] ibid

[42] The GDPR (n4) Art.7 (3)

controllers, and it should be ensured that the data subjects can revoke their consent as easy as they have provided them.[43] However, the scope of its application is limited to the future processing activities of the controller meaning that it does not affect to the legality of the past processes made on the basis of this data before the revocation.[44] Article 7 does not clarify whether the revocation of consent requires the removal of the information as well or not.

The right to erasure originally comes from the DPD (as part of the right to access)[45] and *Google Spain* case, which allows the data subjects to gain from the controller the erasure of their personal information on the internet. [46] Since exercising this right involves conflict of different interests such as the data subject's right to personal data protection and internet user's right to freedom of expression , the ruling made in *Google Spain* case has caused a lot of controversies. In *Google Spain*, the ECJ held that the data subjects have a right to request data controllers including search engines to delete links to personal data concerning them from its list of results.[47] In order to strike a fair balance between conflicting interests, the ECJ took into account the type of information at issue, its sensitivity for the data subject's privacy and his role in public life.[48]

The GDPR has made a valuable contribution to the development of the right to erasure by making it an independent right under Article 17, by providing specific legitimate bases for its exercise[49] as well as exemptions for balancing conflict of interests.[50] Moreover, the right under Article 17 includes both the right to erasure and the right to be forgotten. Although these two terms can be used interchangeably, they are not identical at all. The right to erasure requires a data controller only to erase data, while the right to be forgotten also refers to the need for information to be removed "from all possible sources" in which it is available.[51] Article 17 (2) provides that where, the controller has shared particular personal information with third parties and this information is requested to be deleted, the controller must take all the reasonable actions such as technical measures and inform other controllers about the data subject's request of erasure.[52] This statement is also approved by the interpretation of the ECJ in *Google LLC v. CNIL* case, where French Data Protection Authority requested a preliminary ruling concerning the territorial scope of delisting request.[53] The ECJ held that under the current EU law, de-listing requests are required to be accomplished by a search engine operator only on EU versions of search engines but it also asserted that worldwide de-listing is not also prohibited.[54] Consequently, the ECJ found that if national authorities of Member States adopt an order requiring worldwide de-listing it would comply with the EU laws as far as individual's right to privacy is sufficiently balanced against other fundamental rights.[55]

The GDPR Principles Concerning its extraterritorial application and Cross-Border Transfers of Personal Data

The GDPR includes certain provisions aimed at regulating the protection of EU citizens' personal data outside the EU. The GDPR applies to the use of personal information ' in the context of the activities of an establishment of a controller or a processor in the EU regardless of whether the processing takes place in the EU or not".[56] It means that if a company such as Google is based in the US and the processing of personal data of the EU citizens takes place in the US through its establishment in the EU, the GDPR becomes applicable. Even more stringent principle is embodied in the Article 3 (2), which provides that even without an establishment in the EU, data controllers and processors can be subject to the GDPR if their processing practices concern the personal data of the EU citizens and are related to the supply of products and services to them,[57] or associated with the tracking of their behavior as long as behavior happens in the EU. [58] Online shopping businesses can be an ideal example of the service

[43] ibid
[44] ibid
[45] The European Parliament and the Council Directive 95/46/EC 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 [1995] OJ L 281/31 Art.12
[46] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Espanola de Datos (AEPD), Mario Costeja Gonzalez* [2014] ECLI-317

[47] Ibid para. 88
[48] Ibid para.81
[49] The GDPR (n 4) Art.17 (1)
[50] Ibid Art.17 (3)
[51] Eugenia Politou, Efthimios Alepis and Constantinos Patsakis 'Forgetting personal data and revoking consent under the GDPR: Challenges and Proposed Solutions' Journal of Cybersecurity (2018) 1 (20)
[52] The GDPR (n4) Art.17 (2)
[53] Case C-507/17 *Google v. CNIL* [2019] case in Harlan Grant Cohen 'International Decisions' The American Journal of International Law (2020) 114 (2)
[54] ibid
[55] ibid
[56] The GDPR (n4) Art. 3 (1)
[57] Ibid Art. 3 (2) (a)
[58] Ibid Art. 3 (2) (b)

providers, which are subject to GDPR when they merely offer their services to customers from the Union and use their personal data.

Furthermore, one chapter of the GDPR is devoted to the regulations governing international transfers of personal data.[59] Accordingly, cross-border flows of data are comprehensively regulated by the GDPR. There are several principles designed to ensure the equal data protection in third parties. Two well-known principles are adequacy decision made by the EU Commission[60] and standard data protection clauses.[61] Under the adequacy decision principle, transfers of personal data can be carried out to the third country which is considered by the EU Commission that the country at issues guarantees a sufficient level of protection. As regards standard data protection clauses, a contract template is created by the EDPB, which must be employed by data controllers when they transfer data from the Union to the third country which do not benefit from adequacy decision.

CONCLUSION

In conclusion, the GDPR addresses many practical issues relating to the data protection that consumers frequently encounter in the digital market. As widely discussed above, stringent requirements for obtaining a valid consent have started to improve the quality of consent to personal data processing. For example, companies can no longer presume that pre-ticked boxes, silence and inactivity amount to a valid consent. However, one drawback of the consent principle of the GDPR is that although it is stricter than its predecessor Directive regarding "freely given" requirement of consent, it does not categorically forbid the collection of consent based on take-it-or-leave-it conditions. Moreover, effective principles concerning "specific" consent are included in legally non-binding guidelines or recitals which can undermine effective rules of the GDPR.

As regards the rights of data subjects, the right to data portability, the right to withdraw consent and the right to be forgotten enable data controllers to regain control over their personal data. However, the effectiveness of the right to be forgotten regarding worldwide de-referencing requests is yet to be seen. When it comes to the international transfers of personal data, it must be noted that the GDPR allows consumers to control their data even in third countries.

BIBLIOGRAPHY

1. The European Parliament and the Council Regulation (EU) 2016/679 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) [2016] OJ L 119/1
2. Frederik J Zuiderveen Borgesius and others 'Tracking Walls, Take-it-or-Leave-Choices, the GDPR and the E-Privacy Regulation' European Data Protection Law Review (2017) 3 (3) 3
3. 'Right to Data Protability' (*Information Comissioner's Office*) < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/> accessed 20 July 2020
4. Turdialiev, M. A., & Komilov, B. (2020). The Legal Issues Of International Investment Activity In Uzbekistan: Critical Analysis And Legal Solutions. The American Journal of Political Science Law and Criminology, 2(12), 16-21.
5. Akramov, A., Mirzaraimov, B., Akhtamova, Y., & Turdaliyev, M. A. (2020). Prospects For The Development Of Trust Management In Uzbekistan. Psychology and Education Journal, 57(8), 530-535.
6. Narziev, O. (2021). The Perspectives Of The Establishment Of International Financial Centers In Uzbekistan And The Implementation Of English Law. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(4), 1104-1108.
7. ТУРДИАЛИЕВ, Муҳаммад Али. "ЭРКИН ИҚТИСОДИЙ ЗОНАЛАР ДОИРАСИДА ИНГЛИЗ ҲУҚУҚИНИ ЖОРИЙ ЭТИШНИНГ ХОРИЖ ВА МИЛЛИЙ ТАЖРИБАСИ." ЮРИСТ АХБОРОТНОМАСИ 1.6 (2020): 151-158.
8. Akhtamova, Y., 2016. Protection of International Investments. Analysis of Certain Clauses in International Agreements. Uzbekistan Case Study. Analysis of Certain Clauses in International Agreements. Uzbekistan Case Study (March 25, 2016).
9. Yulduz Akhtamova , Akramov Akmal and Bakhodir Mirzaraimov, and. "Foreign experience related to the legislation and practice of trust management of property in business activities." Збірник наукових праць ЛДОГОΣ (2020): 12-14.
10. Yulduz, Akhtamova. "BALANCING INVESTMENT PROTECTION AND STATE'S REGULATORY SPACE IN THE LIGHT OF INVESTMENT TREATY REGIME ABSTRACT." Review of law sciences 1.Спецвыпуск (2020).
11. Akramov, Akmal, Bakhodir Mirzaraimov, Yulduz Akhtamova, and Mukhammad Ali Turdaliyev. "Prospects For The Development Of Trust Management In Uzbekistan." Psychology and Education Journal 57, no. 8 (2020): 530-535.

[59] Ibid Chapter V
[60] Ibid Art.45
[61] Ibid Art.46 (2)(c)

12. Yulduz Akhtamova "EU Freedom Of Establishment And The Theories Of Incorporation In The Context Of Free Movement Of MNEs" The American Journal of Social Science and Education Innovations 2 (12) 2020: 303-312
13. Akramov, Akmal, et al. "Prospects For The Development Of Trust Management In Uzbekistan." Psychology and Education Journal 57.8 (2020): 530-535.
14. Akramov, Akmal, Bakhodir Mirzaraimov, and Yulduz Akhtamova. "Foreign experience related to the legislation and practice of trust management of property in business activities." Збірник наукових праць ΛΌГОΣ (2020): 12-14.
15. Mirzaraimov B., 2020. Effective Measures Of Preventing Due Process Paranoia In International Arbitration. The American Journal of Political Science Law and Criminology, 2(11), pp.72-80.
16. The European Parliament and the Council Directive 95/46/EC 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 [1995] OJ L 281/31 Art.12
17. Eugenia Politou, Efthimios Alepis and Constantinos Patsakis 'Forgetting personal data and revoking consent under the GDPR: Challenges and Proposed Solutions' Journal of Cybersecurity (2018) 1 (20)