TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Vilma Isojunno

PROCESSING NON-USER PERSONAL DATA IN SOCIAL NETWORK SERVICES: THE GDPR APPROACH

Bachelor's thesis
Programme HAJB08/14 - Law, specialisation European Union and international law

Supervisor: Kari Käsper, M.A

Tallinn 2019

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 9812 words from the introduction to the end of conclusion.

Vilma Isojunno ……

(signature, date)

Student code: HAJB 166356
Student e-mail address: vilma.isojunno@dnainternet.net

Supervisor: Kari Käsper, M.A:
The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:
Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT 4
INTRODUCTION 5
1. PRIVACY POLICIES IN THE LIGHT OF THE GDPR 7
1.1. Background 7
1.2. Scope of application of the GDPR 8
1.3. Rights of the data subject under the GDPR 9
1.4. Principles relating to processing of personal data 11
1.5. Privacy policies of social network providers 14
2. LAWFUL PROCESSING OF PERSONAL DATA UNDER THE GDPR 16
2.1. Processing personal data based on consent 17
2.2. Processing personal data based on contractual obligation 19
2.3. Processing personal data based on legitimate interest 19
2.3.1. Belgian Commission for the Protection of Privacy v. Facebook Inc. 20
2.3.2. Balancing test 22
3. PROPOSALS 26
CONCLUSION 28
LIST OF REFERENCES 30

ABSTRACT

Under the General Data Protection Regulation, the processing of personal data is only lawful when there is a legal basis for processing prescribed by law. The privacy policies of some social network service providers such as Twitter, Snapchat, Facebook, WhatsApp and Instagram reveal that they process personal data of non-users when providing their services. However, the legal basis for processing such data is not defined in their privacy policies. The aim of the thesis is to examine whether there is a legal basis for processing non-user personal data and which legal basis it is under the General Data Protection Regulation.

The research is conducted based on a qualitative research method where applicable legislation and relevant academic literature are used for analysing the research problem. The thesis evaluates the privacy related issues of the privacy policies of the social network service providers and examines whether any of the lawful basis for processing under the Article 6 of the GDPR applies.

The author claims that the practice of collecting non-user personal data by the evaluated social network service providers is illegitimate. At the end of the paper some proposals are made in order to solve the privacy issues relating to the processing of non-user personal data.

Keywords: General Data Protection Regulation, privacy, social network services,
lawful processing

INTRODUCTION

Data protection legislation in the European Union (EU) underwent reform towards more privacy enhancing and transparent state. In relation to the reform, the General Data Protection Regulation (GDPR)[1] was introduced in order to further harmonize the protection of personal data within the EU. The GDPR came into force on 15 May 2018 repealing the old Data Protection Directive[2]. The aim of the GDPR was to establish rules governing the processing of personal data and to enhance the right to protection of personal data.[3] Hence, the processing of personal data was only lawful on the basis of consent of the data subject or when the processing is necessary for the performance of a contract, compliance with a legal obligation, protection of vital interest, performance of a task carried out in the public interest or purposes of the legitimate interest pursued by the controller.[4]

The privacy policies of some social network service (SNS) providers such as WhatsApp, Facebook, Snapchat, Instagram and Twitter reveal that they do not collect only personal data of their users but also personal data of non-users. For example, Snapchat[5] and Twitter[6] collect the address books of their users when the user gives his consent to it. WhatsApp[7], which is owned by Facebook requires the address book information frequently. Instagram[8], also owned by Facebook, and Facebook[9] collect not only the address books of their users but also call log and SMS log history when the user consent to it. In other words, the aforementioned SNS providers collect personal data of non-users such as names and phone numbers. The gathering of personal information of the users and non-users allows the possibility to use the data for data mining and

[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), OJ L 119, 4.5.2016, p.1-88.
[2] 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, OJ L 281, 23.11.1995, p. 31-50.
[3] OJ L 119, 4.5.2016 art 1.
[4] *Ibid.*, art 6.
[5] *Privacy Policy*. Snapchat. Accessible: https://www.snap.com/en-US/privacy/privacy-policy/#european-union-users 14 February 2019.
[6] *Privacy Policy*. Twitter. Accessible: https://twitter.com/en/privacy 14 February 2019.
[7] *Privacy Policy*. WhatsApp. Accessible: https://www.whatsapp.com/legal/?eea=1#privacy-policy 14 February 2019.
[8] *Data Policy.* Instagram. Accessible: https://help.instagram.com/155833707900388 14 February 2019.
[9] *Data Policy.* Facebook. Accessible: https://www.facebook.com/policy.php 14 February 2019.

profiling purposes. For example, a study suggests that location data combined with data collected from call log history could be used for predicting relationships between individuals.[10] The practice of collecting personal data of non-users is problematic from the perspective of the GDPR because non-users have not consented to the collection of their personal data by the SNS providers nor benefit of the processing of their personal data. Besides they might not even know that their personal data is being collected and processed by these companies and therefore cannot effectively exercise their rights provided by the GDPR.

It seems that the collection of personal data of non-users is a common practice among the major SNS providers in the EU, thus the processing impacts on many non-users whose personal data is processed. This bachelor thesis intends to challenge the lawfulness of processing personal data of non-users by the SNS providers. The research questions of the bachelor thesis are: Is there a legal basis under the GDPR for processing of personal data of individuals who do not use the social network services? If there is a legal basis under the GDPR, which legal basis is it? The hypothesis is that there is no legal basis for processing such personal data, thereby the practice is unlawful.

The thesis is divided into three parts, in the first part of the thesis the scope of the application of the GDPR and basic principles will be introduced. Also, the conflict between the GDPR and the privacy policies of SNS providers will be explained thoroughly. This part is important in order to assess the impact of processing non-user personal data. In the second part of the thesis, the lawful basis for processing will be evaluated. The chapter will mainly focus on processing based on consent, performance of a contract and legitimate interest of the controller. As well, relevant case law and the balancing test relating to assessment of legitimate interest will be introduced. The third part will propose solutions to problems relating to processing of non-user personal data. The qualitive research method will be used in this thesis. The research question will be examined based on applicable laws and relevant academic literature as well as some case law will be introduced.

[10] Eagel, N., Pentland, A. S., Lazer, D. (2009). Inferring friendship network structure by using mobile phone data. – *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 106, No. 36, 15274-15278.

1. PRIVACY POLICIES IN THE LIGHT OF THE GDPR

1.1. Background

Privacy as a legal right was first introduced in the article: "The Right to Privacy"[11] by Warren and Brandeis in 1890. The right to privacy was defined by Warren and Brandeis as "right to be let alone."[12] Currently, the right to privacy and data protection are fundamental rights conferred by the Treaty on the Functioning of the European Union Article 16 and the Charter of Fundamental Rights of the European Union Articles 7 and 8. Both rights are important for maintaining a democratic society and necessary for guaranteeing the fulfilment of other fundamental rights, thus the right to privacy and data protection should be present as well on the internet.[13]

The GDPR was introduced in order to enhance the right to data protection and broaden the harmonization of data protection laws in the EU. Even though the effectiveness of the harmonization has been criticized, the Regulation aims to improve the protection of rights of data subjects.[14] The GDPR has been directly applicable in all Member States since 25 May 2018. The compliance with the legal requirements is essential, since according to the GDPR the administrative fines can be: "up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."[15]

In order to evaluate the impact of the processing of non-user personal data it is important to examine the privacy policies overall compliance with the GDPR. The following section will introduce the basic principles of the GDPR relating to the processing of personal data and the assessment of the privacy policies' compliance with the requirements of the GDPR.

[11] Warren, S., Brandeis, L. (1890). The Right to Privacy. – *Harvard Law Review*, Vol. IV, No. 5, 193-220.
[12] *Ibid.*, p 195-199.
[13] Hijmans, H. (2016). The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU. Vol. 31. Brussels: Springer, p 24-28.
[14] Blume, P. (2012). Will it be a better world? The proposed EU Data Protection regulation. – *International Data Privacy Law*, Volume 2, Issue 3, p 130-136.
[15] OJ L 119, 4.5.2016 art 83 sec. 5.

1.2. Scope of application of the GDPR

The SNS providers which collect and process information relating to identified or identifiable natural person, i.e. personal data, are obliged to comply with the requirements of the GDPR.[16] It is irrelevant whether the processing occurs in the Union or outside, since the GDPR is applicable even outside the Union as long as the data subject is located in the Union.[17] Therefore international companies processing personal data of individuals residing in the EU, such as Facebook Inc., Snap Inc. and Twitter Inc., must comply with the GDPR.

Users of social network services are exempted from the scope of application of the GDPR provided that their activities meet certain criteria. Natural persons processing personal data solely for personal or household activity are excluded from the scope of the GDPR.[18] There is no exact definition of personal or household activity but recital 18 of the Regulation gives examples of what might be included, for instance holding of addresses and correspondence.[19] It has been established in Case C-101/01 Lindqvist that the processing of personal data does not fall within the personal or household exception if the data is disclosed to indefinite group of people.[20] Address books on a mobile phone used for private purposes and communication through phone calls and SMS messages, should consequently be excluded from the scope of application of the GDPR, that activity being for personal use only and among restricted group of people. Nonetheless, the definition of personal or household activity in the context of social networks is more or less controversial due to the lack of case law and precise definition by law.[21]

In order to use WhatsApp, the user is obliged to provide his address book on regular basis to the provider according to the privacy policy.[22] If the user is using WhatsApp for his own personal communication, he is exempted from the scope of application of the GDPR. It is problematic, since the user is providing names and phone numbers of the other user and non-users to the service

[16] OJ L 119, 4.5.2016 art 2, sec. 1.
[17] *Ibid.*, art 3.
[18] *Ibid.*, art 2, p 2(c).
[19] *Ibid.*, recital 18.
[20] Court decision, 6.11.2003, Lindqvist, C-101/01, EU:C:2003:596, p 47
[21] EU Internet Law: Regulation and Enforcement. (2017). /Eds. T-E. Synodinou, P. Jougleux, C. Markou, T. Prastitou. Nicosia: Springer, p 25-28.
[22] *Privacy Policy*. WhatsApp. Accessible: https://www.whatsapp.com/legal/?eea=1#privacy-policy 14 February 2019.

provider, without being competent to do so. Provided that the GDPR applies to the user, the user would be liable for providing the personal data of non-users to WhatsApp in accordance with the requirements of the GDPR. As it is not the case, when processing personal data of non-users, WhatsApp cannot rely on the user's responsibility.

1.3. Rights of the data subject under the GDPR

The GDPR emphasises data subject's control over his own personal data.[23] Data subject is the person from whom the personal data is being collected, for instance a user of a SNS.[24] The GDPR provides rights to the data subject in relation to the processing of personal data. Compliance with these rights is substantial since the non-compliance could result in the most severe fines which can be imposed by the GDPR.[25] Under the GDPR data subjects have the right to:

a) be informed about the processing of their personal data,
b) access their personal data,
c) rectification and erasure,
d) restriction of processing,
e) right to data portability,
f) object processing of personal data
g) not to be subject of automated individual decision making.[26]

The right to be informed about the processing includes also the right to know what kind of personal data is being processed, who is processing and based on which legal basis. Right of access gives the right to obtain a copy of the personal data processed. Some suggest that the right of access could also be extended to include the right to inspect the data subject's personal data when it is processed in the controller's systems.[27] Right to rectification means that the data subject has the right to rectify any incorrect personal data. Right to erasure is also known as right to be forgotten and it gives the right for the data subject to demand the erasure of his personal data. The data subject has the right to restrict processing providing that certain criteria provided by the law

[23] van Ooijen, I., Vrabec, H. U. (2018). Does the GDPR Enhance Consumers' Control over Personal Data?: An Analysis from a Behavioural Perspective. – *Journal of Consumer Policy*, p 2. Accessible: https://doi.org/10.1007/s10603-018-9399-7, 13 March 2019.
[24] OJ L 119, 4.5.2016 art 4 sec. 1.
[25] OJ L 119, 4.5.2016 art 83 sec. 5.
[26] OJ L 119, 4.5.2016 art 13, 14, 15, 16, 17, 18, 20, 21 and 22.
[27] Kelleher, D., Murray, K. (2018). *EU Data Protection Law.* 1st ed. London: Bloomsbury Professional, p 204.

applies. Right to data portability enables the free flow of personal data between controllers, and it gives the right for the data subject to demand a transfer of his personal data to another controller in a commonly used machine-readable format. On certain grounds provided by the law, the data subject can object the processing of his personal data. The data subject can object automated individual decision-making when it creates a legal effect concerning him.

In the context of processing personal data of non-users by SNS providers, all aforementioned rights may be potentially infringed except for the right to object automated individual decision making since there is no legal effect or similar significant effect in relation to the processing. If the non-user is not aware of the processing activities, which are taking place, the non-user cannot effectively exercise his rights under the GDPR. For example, the data subject cannot object the processing or ask the erasure of his personal data if the service provider does not inform him about the processing activities.

Besides the GDPR requires the notification to be made for data subject, when the personal data is obtained from someone else.[28] In the notification, the controller must disclose some aspects relating to the processing, such as the time and purposes of processing, contact details of the controller and inform the data subject about the possible data transfer outside the EU, which is the case in relation to all of the SNS providers evaluated: Facebook, WhatsApp, Instagram, Snapchat and Twitter transfer personal data outside the EU.

The duty to notify is a bit controversial because the notification is not mandatory in case the notification would be impossible or requires disproportional effort.[29] Provided that the collecting of non-user personal data is lawful, the exception could be argued, since the controller will only receive phone numbers and names of the non-users. It could be disproportional to contact each of them via phone or to obtain more information of them, in order to notify of the processing activities. If the SNS providers were able to connect the phone numbers to the e-mail addresses of the non-users, the SNS providers would be able to contact the non-users. In that case the processing should be based on legal ground provided by the GDPR. However, the basis cannot be the necessity to comply with the legal obligation, as the legal obligation, obligation to notify of the processing activities, would be created artificially by the SNS providers when collecting the non-user personal data.

[28] OJ L 119, 4.5.2016 art 14.
[29] OJ L 119, 4.5.2016 art 14 sec. 5(b).

1.4. Principles relating to processing of personal data

The GDPR establishes certain principles relating to processing of personal data which the controller must comply with when conducting processing activities. The controller is the natural or legal person determining the purposes and means of the processing of personal data, in the present case that would be the SNS provider.[30] When the controller processes personal data, there are certain principles which it has to follow and be able to demonstrate compliance with.[31] The processing activities have to be conducted in the manner that personal data is:

a) Processed lawfully, fairly and in a transparent manner;
b) collected for specified, explicit and limited purposes;
c) adequate, relevant and limited to what is necessary;
d) accurate and kept up to date;
e) stored in a form which allows the identification of data subject for no longer than what is necessary; and
f) processed in a manner which secures the integrity and confidentiality of personal data.[32]

There are a few questionable aspects relating to the processing of non-user personal data. The fair processing of personal data should be interpreted meaning the transparent and lawful processing while taking into account how the controller considers the legitimate interest of the data subject.[33] It seems arguable, that the SNS providers collecting personal data of non-users on account of their right to privacy, would consider the legitimate interest of the data subject, especially when non-users do not benefit from the practice. Transparency is also essential part of fair processing but the practice does not seem to be transparent, since the privacy policies do not define well enough the basis of collection non-user personal data.

There are also other issues with the transparency in relation to the collection of personal data. For instance, Facebook is divided into two mobile applications: Facebook and Messenger. Facebook is used for the main functions such as sharing pictures and comments and Messenger is used for sending messages or calling. The privacy settings of both applications cannot be synchronized but

[30] OJ L 119, 4.5.2016 art 4 sec. 7.
[31] OJ L 119, 4.5.2016 art 5 sec. 2.
[32] OJ L 119, 4.5.2016 art 5
[33] Maxwel, W. J. (2015). Principles-based regulation of personal data: the case of 'fair processing'. – *International Data Privacy Law*, Vol. 5, No. 3, p 208.

the user has to disable the sharing of contact information from both applications separately.[34] However, the other settings are synchronized. This is something that many users might not be aware of, since the user account is the same and the user can navigate through both applications as if they were the same entity, without having to open the application separately from the home screen. In addition, when using Facebook with a web browser, there is no distinction between Facebook and Messenger, but Messenger is integrated into Facebook. Therefore, some users might leak personal data even when they think they have disabled the sharing of information.

The purpose limitation appears to be an issue, since the purpose for collecting SMS or call log history, does not seem apparent to the user. Especially when the user cannot comprehensively understand the possibilities for further usage of that data. The initial purpose for collecting personal data should be informed and the processing activities should be compatible with the initial purpose.[35] How can the SNS provider ensure that the personal data collected is not processed for purposes which are incompatible with the initial purposes if the initial purposes have not been specified? Even though the processing would be legitimate, it is not sufficient to only give general overview of the processing activities.[36] The wordings in the privacy policies for collecting non-user personal data are mostly vague and do not exactly describe how the SNS providers intend to process the personal data. For instance, Twitter's privacy policy states that the address book information is used for connecting people and recommending content to the user and others. It does not explain how the content will be recommended and who will be included to "others".

Along with the purpose limitation, data minimisation plays an important role as well. The amount of data collected should be proportional in relation to processing activities and limited only to what is necessary in order to achieve the purpose of processing.[37] The evaluation of necessity requires the individual assessment of alternative ways to achieve the purpose of the processing.[38] It is questionable, whether the SNS providers comply with the data minimisation when collecting non-user personal data. For example, WhatsApp collects address book information to identify the contacts using WhatsApp in order to connect the users inside their service. Despite, WhatsApp is

[34] *How can I manage contact uploading with the Facebook app?* Facebook Help center. Accessible: https://www.facebook.com/help/355489824655936?helpref=faq_content 10 March 2019.
[35] Kuner, C. (2007). European Data Protection Law: Corporate Compliance and Regulation. 2nd ed. Oxford: Oxford University Press, p 100.
[36] Kelleher, Murray, *supra nota* 27, p 140.
[37] Voigt, P., von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide, 1st ed. Berlin: Springer p 90.
[38] *New European General Data Protection Regulation: A Practitioner's Guide Ensuring Compliant Corporate Practice.* (2018). /Eds. D. Rücker, T. Kugler. Baden-Baden: C. H. Beck, Hart, Nomos, p 66-67.

an internet-based service, where users have to register themselves and the communication is done via internet connection. An alternative way could be to provide possibility to search other users in WhatsApp, instead of making mandatory the sharing of the entire address book. Besides, Facebook, which owns WhatsApp, has a Messenger, which is a comparable application to WhatsApp and does not require address book information in order to function. It seems that there is an alternative solution, which Facebook is already using in its other application, thus the necessity for collecting the address book information could be in this case, questioned.

Storage limitation, which means that personal data should not be kept longer than what is necessary, seems to be an issue when collecting the non-user personal data. The privacy policies of any of the evaluated SNS providers do not reveal how long such personal data is stored and when it will be deleted. It is not even clear if upon termination of a user account such information will be deleted from the database. It is up to the controller to assess the necessary retention period for personal data, since it has to be evaluated case-by-case basis.[39] In order to demonstrate the controller's accountability, the transparency in the retention period would be welcome.

In addition, the GDPR requires privacy by default, there should be technical measures to ensure that only personal data which are necessary for each specific purposes can be collected and processed.[40] The option which is the least intrusive to privacy should be selected by default and if a user wants to share more information than what is required then he must change the settings in order to do so, but not *vice versa*.[41] If it is considered that there is no legal basis for collecting non-user personal data, the requirement for privacy by default is not met. In that case, the applications by default would be designed to collect personal data which they should not be collecting.

The sharing of non-user personal data is highly promoted by the applications. For example, when a user has downloaded Facebook Messenger and logs into his user account for the first time, the application suggests the sharing of address book information. The first option is to share address book information with the application, and it is highlighted with blue background, whereas the option refusing to share the information is displayed below but this option has not been highlighted with any colour. When choosing the option which does not allow the sharing of address book information the application gives a notification confirming whether the user is sure that he does

[39] Kelleher, Murray, *supra nota* 27, p 148.
[40] OJ L 119, 4.5.2016 art 25 sec. 2.
[41] Voigt, von dem Bussche, *supra nota* 37, p 63.

not want to share the address book information. Even though there is no pre-selected option, it seems obvious that the controller tries to persuade the user to share the address book information. The user must choose one or the other before he can continue to use the application and determine whether the sharing of address book is actually needed. The promotion of option which is not privacy friendly seems to be a grey area, since the controller should try to protect the personal data of the users according to the privacy by default principle even though active choosing of privacy settings by the data subject is encouraged.[42] At least it is misleading for the users, since the application only informs about the positive effects of the sharing of the address book information, but it does not inform the user about the risks relating to sharing of personal data of somebody else. To be on the safe side, it would be preferable to promote the privacy friendly option.

1.5. Privacy policies of social network providers

The privacy policies of the SNS providers do not distinct comprehensively enough, which personal data is collected under which legal basis, which is why the legal basis for collecting non-user personal data is not apparent. Nor the purpose of processing non-user personal data is apparent from the privacy policies of the SNS providers evaluated. For that reason, it is difficult to know how and what for the personal data is being used. Privacy policies should be written in plain language understandable for everyone as well the purposes for which the personal data is used should be mentioned, especially if used for profiling.[43] It is not known whether the personal data will be used for profiling of non-users but it definitely gives the possibility for the controller to use the collected personal data for such purpose. Besides, lack of transparency could be also consumer protection issue, as it could be considered as unfair commercial practice.[44]

It would seem evident that the interests of the SNS providers are in conflict with the nature of the objectives of the GDPR. The SNS providers who profit from collecting personal data and serving as an advertisement platform, have the interest to collect as much personal data from as many people as possible. At the same time, users are quite unaware of how their personal data is actually

[42] Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., Leucci, S. (2018). Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR – *European Data Protection Law Review*, Vol. 4, p 183-185.
[43] Reforming European Data Protection Law. (2015). /Eds. S. Gutwirth, R. Leenes, P. de Hert. Vol. 20. Brussels: Springer. p 54-55.
[44] Kerber, W. (2016). Digital markets, data, and privacy: competition law, consumer law and data protection. – *Journal of Intellectual Property Law & Practice*, Vol. 11, No. 11, p 862.

used.[45] Due to the large user basis of the evaluated SNSs, it is almost impossible not to be tracked by them since they extent the tracking of the users to non-users as well. After all, it is the responsibility of the SNS providers to demonstrate their compliance with the GDPR and implementation of the legislation into their privacy policies.[46] The users and non-users should not be guessing how their personal data is processed and for which purpose.

[45] Castelluccia, C. (2012). Behavioural Tracking on the Internet: A Technical Perspective. – *European Data Protection: In Good Health?* (Eds.) S. Gutwirth, R. Leenes, P. de Hert, Y. Poullet. Brussels: Springer. p 21-33.
[46] OJ L 119, 4.5.2016 art 24.

2. LAWFUL PROCESSING OF PERSONAL DATA UNDER THE GDPR

In the EU, the processing of personal data is generally prohibited, unless the processing is based on a legal ground provided by the GDPR.[47] Each legal ground considered equal but it should be determined before processing and informed to the data subjects.[48] The legal ground must be one or more of the following from the exhaustive list:

a) data subject's consent;
b) necessity to perform a contractual obligation;
c) necessity to comply with a legal obligation;
d) necessity to protect vital interest of the data subject;
e) necessity for performance of a task carried out in the public interest;
f) necessity for purposes of legitimate interest pursued by the controller.[49]

In the following sub-chapters, the processing activities will be evaluated based on consent, contractual obligation or legitimate interest. When processing is based on legal obligation, the obligation should be such that the controller cannot refuse to process the personal data.[50] In relation to the processing of personal data of non-users there is no legal obligation based on which the SNS provider ought to collect the personal data which they are collecting of the non-users. When the processing is based on protection of vital interest, there should be a threat to life, which is not the case. Processing based on performance of a task carried out in the public interest cannot be a legitimate ground either since it should be done based on Union or Member State law, which the controller is subject to.[51] Again, there is no law which would give the authority for the SNS providers to collect the personal data of non-users. Since these legal bases are not relevant in the present case, they will not be further considered.

[47] Rücker, Kugler, *supra nota* 38, p 51.
[48] Gil Gonzalez, E., de Hert, P. (2019) Understanding the legal provisions that allow processing and profiling of personal data – an analysis of GDPR provisions and principles. – *ERA Forum*, p 3.
[49] OJ L 119, 4.5.2016 art 6
[50] Rücker, Kugler, *supra nota* 38, p 79.
[51] OJ L 119, 4.5.2016 art 6 sec. 3 (a) and (b).

2.1. Processing personal data based on consent

The GDPR defines consent as "freely given, specific, informed and unambiguous indication of the data subject's wishes".[52] The consent is valid when the criteria is fulfilled. When the SNS providers are processing personal data of non-users, consent cannot be the legal basis since the criteria is not met. Silence is not considered as a valid consent because it does not clearly indicate that the data subject has consented the processing.[53] Non-users obviously have not agreed to the processing of personal data and because they do not actively object the processing it does not mean that the SNS providers have the consent for processing. Besides, while the users of the services cannot consent the processing on behalf of someone else, the controller has the burden of proof to demonstrate that the data subject has consented the processing.[54]

Moreover the other criteria, for 'freely given' consent is not fulfilled for example in the case with privacy policy of WhatsApp, where it is impossible to opt-out from the requirement of providing address book information.[55] A requirement of this sort, does not qualify as 'freely given', since the user cannot make a choice whether to give that information or not.[56] Also, the requirement is restrictive since a person who is conscious of privacy of those in his address book, cannot use the service at all. Some believe that tracking wall, which occurs when a service is made available only, when the user allows the tracking of his personal data, is not categorically prohibited by the GDPR.[57] However, the clear imbalance of powers between the service provider and the user should be taken into account when assessing the validity of the user's consent.[58] There is no room for negotiations between the user and WhatsApp and without giving a consent to WhatsApp for tracking the user, the user cannot use the service. It is evident that the consent cannot be regarded as 'freely given' in this context. When the consent is not 'freely given' and cannot be negotiated, the legal basis for processing should be contractual obligation.[59]

---

[52] OJ L 119, 4.5.2016 art 4 sec. 11
[53] Borghi, M., Ferretti, F., Karapapa, S. (2013). Online data processing under EU law: a theoretical framework and empirical evidence from the UK. – *International Journal of Law and Information Technology*, Vol. 21, No. 2, p 120-121.
[54] OJ L 119, 4.5.2016 art 7 sec. 1.
[55] *Privacy Policy*. WhatsApp. Accessible: https://www.whatsapp.com/legal/?eea=1#privacy-policy 14 February 2019.
[56] Borghi *et al*., *supra nota* 53, p 123-124.
[57] Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C., Helberger, N. (2017.) Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. – *European Data Protection Law Review*, Vol. 3, Issue 3, p 360-361.
[58] *Ibid*.
[59] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (WP259) 28.11.2017, p 8.

Whereas sharing non-user personal data is optional under privacy policies of Instagram, Facebook, Snapchat and Twitter where the users can choose to share the address book information and with Facebook also the call log and SMS log history if they like.[60] When processing is based on consent, the necessity of processing is not required to the same extent as it is when processing is based on other legal grounds.[61] Which is why giving an option for the user to decide whether to share the data or not implies that there is no necessity for processing such data. In this case the SNS provider could not process personal data of non-users in any other legal ground. If the SNS provider would still process address book information, call log and SMS log history despite the user's refusal, requesting a permission for processing would be unfair for the user and therefore would be better to rely on legitimate interest as a legal ground for processing.[62] The privacy policy of Snapchat actually states that even though they are not relying on consent when processing contact data, they still ask for permission to access it.[63]

Furthermore, WhatsApp's privacy policy states that the user is responsible for providing the address book information in accordance with applicable laws.[64] The statement indicates that WhatsApp attempts to shift its liability to the user when it comes to the legal collection of the personal data. The user liability could be argued but as established earlier in section 1.1. the personal use exception applies to the users of WhatsApp. Besides, the SNS providers cannot rely on user's responsibility to provide the non-user personal data as per law if the collection of such data lacks the purpose and legal basis from the beginning. If the data subject has not expressed in any way desire for processing, there is no consent and the processing activities cannot take place.[65] As there is no consent from the non-users, there cannot be processing of personal data based on consent.

[60] *Data Policy*. Instagram. Accessible: https://help.instagram.com/155833707900388 14 February 2019; *Data Policy*. Facebook. Accessible: https://www.facebook.com/policy.php 14 February 2019; *Privacy Policy*. Snapchat. Accessible: https://www.snap.com/en-US/privacy/privacy-policy/#european-union-users 14 February 2019; *Privacy Policy*. Twitter. Accessible: https://twitter.com/en/privacy 14 February 2019.
[61] Gil Gonzalez, de Hert, *supra nota* 48, p 4.
[62] *Ibid.*, p 4.
[63] *Privacy Policy*. Snapchat. Accessible: https://www.snap.com/en-US/privacy/privacy-policy/#european-union-users 14 February 2019.
[64] *Privacy Policy*. WhatsApp. Accessible: https://www.whatsapp.com/legal/?eea=1#privacy-policy 14 February 2019.
[65] Zuiderveen Borgesius, F. J. (2015). Personal data processing for behavioural targeting: which legal basis?. – *International data privacy law*, Vol. 5, No. 3, p 170.

2.2. Processing personal data based on contractual obligation

The processing of personal data should be unavoidable part of performance of a contract in order to claim processing of personal data based on this provision.[66] There is a contract between the SNS provider and the user, in exchange of personal information the user can use the platform for social communication. Yet, there is no contract between the non-user and the SNS provider and the GDPR clearly expresses that the data subject must be party of the contract.[67] For that reason, the processing cannot be based on contractual obligation as there is no contract.

In addition, the processing lacks the element of necessity. If there is an option given to the user, as it is in case of privacy policies of Facebook, Instagram, Twitter and Snapchat, the processing cannot be truly necessary for performance of a contract, otherwise it would not be optional. The provision should be interpreted to include strictly the processing of personal data which is necessary for performance of a contract.[68] Moreover, there seems to be a consensus in the EU that personal data processing for behavioural targeting, which is the usual purpose for processing personal data by the SNS providers, cannot be based on necessity for the performance of a contract, especially when the data subject is not aware of it.[69]

2.3. Processing personal data based on legitimate interest

When the controller processes personal data based on its legitimate interest, it should be necessary to achieve the purpose of the processing. The legitimate interest of the controller should not prevail over the interest or fundamental rights and freedoms of the data subject.[70] The controller is to assess whether it has a legitimate interest, and in addition is accountable for demonstrating the legitimate interest based on which the processing takes place.[71] Legitimate interest could be understood to be any interest which is not against law, for instance commercial interest.[72] The

[66] Kuner, *supra nota* 35, p 243-244.
[67] OJ L 119, 4.5.2016 art 6 sec. 1 (b).
[68] Voigt, von dem Bussche, *supra nota* 37, p 102.
[69] Zuiderveen Borgesius (2015), *supra nota* 65, p 165-167.
[70] OJ L 119, 4.5.2016 art 6 sec. 1 (f).
[71]Ferretti, F. (2014). Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights. – *Common Market Law* Review, Vol. 51, Issue 3, p 858.
[72] Kamara, I., de Hert, P. (2018). Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. – *The Cambridge Handbook of Consumer Privacy*. (Eds.) E. Selinger, J. Polonetsky, O. Tene. Cambridge: Cambridge University Press, p 330.

legitimate interest provision could be considered as a leeway for controllers to conduct such processing activities which would not qualify under other legal grounds for processing.[73]

Undeniably, SNS providers have legitimate interest towards the connections of their users. SNS provider such as Facebook have built a profitable business model around tracking people and selling their personal data to advertisers.[74] If personal data were not valuable, the SNS providers would not be interested in processing the non-user personal data. The more extensive the collection of personal data is, the better the SNS providers can target their customers. Notwithstanding, excessive collection of personal data endangers privacy and can have a negative impact on economy.[75]

It is not sufficient to only acknowledge the legitimate interest of the controller. The interest of the controller has to be assessed with the level of data protection, which the data subject could have had without the processing, and whether the level of data protection is appropriate when the processing occurs.[76] If it is deemed that the rights and freedoms of the data subject are overridden by the interest of the controller, the processing is unlawful.

2.3.1. Belgian Commission for the Protection of Privacy v. Facebook Inc.

Brussels Dutch-Speaking Court of First Instance ruled against Facebook for tracking non-users with "datr" cookie in 2015.[77] The Belgian Commission for the Protection of Privacy had found out that when a person visited Facebook's website, whether user or non-user, a browser would install a "datr" cookie.[78] The cookie would be installed when a person visiting third-party website with a Facebook plug-in, such as "like" button, interacted with the plug-in.[79] The "datr" cookie, which would stay on hard disk for two years, identified an internet user's browser and when he visited website with Facebook's plug-in button, the information would be sent to Facebook's servers.[80] The main concern in the case was the non-users who were tracked by Facebook with the "datr"

[73] Ferretti, *supra nota* 71, p 856.
[74] Esteve, A. (2017). The business of personal data: Google, Facebook and privacy issues in the EU and the USA. – *International data privacy law*, Vol. 7, No. 1, p 36-37.
[75] Kerber, *supra nota* 44, p 856-866.
[76] Balboni, P., Cooper, D., Imperiali, R., Macenaite, M. (2013). Legitimate interest of the controller New data protection paradigm: legitimacy grounded on appropriate protection. – *International Data Privacy Law*, Vol. 3, No. 4, p 246.
[77] Nederlandstalige rechtbank van eerste aanleg Brussel, 2015/57/C, 09.11.2015.
[78] *Ibid.*
[79] *Ibid.*
[80] *Ibid.*

cookie. The court examined the lawful basis for processing the personal data but considered that none of the lawful basis were satisfied.[81] The judgement was criticized for too narrow interpretation of legitimate interest, since Facebook claimed the cookies to be necessary for security purposes, which the court ruled inadmissible in this case.[82]

The case was taken into the Brussels Court of Appeal on 29 June 2016, where the court overturned the decision of the Court of First Instance.[83] The Court of Appeal considered that the Data Protection Directive[84] did not have direct effect in Belgium legislation, which was why the Belgian courts did not have jurisdiction over Facebook Inc. and Facebook Ireland Limited., which where the defendants along with Facebook Belgium SPRL.[85] In spite of the outcome of the latter decision, the Belgian Commission for the Protection of Privacy started even more extensive proceedings against Facebook Ireland Limited, Facebook Inc. and Facebook Belgium BVBA.[86] The dispute concerned Facebook's tracking activities of users and non-users with different cookies: "datr", "c_user", "xs", "sb", "fr" and "lu" as well with "pixels".[87] Relying on "Google Spain"[88] decision the court ruled its international competence.[89] Hence the court decided on 16 February 2018 that:

a) the use of cookies without informed consent of the user should be ceased;
b) the users should not be misled of the real functions of the cookies;
c) the personal data which have been collected pursuant to these cookies should be deleted, and that;
d) Facebook has to publish the ruling on its website.[90]

The Facebook's cookie policy was lacking transparency and informed consent for tracking users and non-users.[91] The systematic collection of personal data was deemed not essential or at least unproportionate.[92] In addition, a fine of 250 000 Euros per day up to 100 000 000 Euros was issued

[81] *Ibid.*
[82] Truyens, M. (2016). No More Cookies for Unregistered Facebook Users in Belgium: Belgian Data Protection Legislation Applies to Facebook. – *European Data Protection Law Review*, Vol. 2, Issue 1, p 139.
[83] Hof van beroep Brussel, 2016/KR/2, 29.06.2016.
[84] OJ L 281, 23.11.1995.
[85]Van Bael & Bellis. (2016) Facebook Wins Privacy Appeal before Belgian Court of Appeal. – *Van Bael & Bellis on Belgian Business Law*, Vol. 2016, No. 7, p 7-8, Accessible: https://www.vbb.com/media/Insights/BE_07_16.pdf , 16 March 2019.
[86] Nederlandstalige rechtbank van eerste aanleg Brussel, AR 2016/153/A, 16.02.2018.
[87] *Ibid.*, p 5.
[88] Court decision, 13.05.2014, Google Spain and Google, C-131/12, EU:C:2014:317.
[89] Nederlandstalige rechtbank van eerste aanleg Brussel, AR 2016/153/A, 16.02.2018, p 19-20.
[90] *Ibid.*,p 41.
[91] *Ibid.*, p 34.
[92] *Ibid.*, p 36.

to defendants.[93] Although, the latter case was decided on the basis of the Data Protection Directive,[94] which was implemented in the Belgian national law, the same legal basis for processing personal data applies to the GDPR. Since there is no ruling regarding of the collection of non-user personal data from the European Court of Justice, the latter cases can serve as a standpoint for comparison of how similar issue has been interpreted in the EU. Regarding the cookie policies, there is the ePrivacy Directive which specifically regulates the use of cookies.[95]

2.3.2. Balancing test

The legitimate interest must be balanced with the data subjects' fundamental rights and freedoms, this is called balancing test.[96] Firstly the legitimate interest should be identified.[97] The legitimate interest should be real, present and clearly articulated.[98] The SNS providers have a legitimate commercial interest to the personal data of non-users. The legitimate interest is not clearly indicated in their privacy policies which is why, the legitimate interest is only assumed to be legitimate business interest. When processing is based on legitimate interest, the SNS providers should disclose their legitimate interest with the data subjects.

Secondly, the necessity of processing should be evaluated.[99] Even though the processing is deemed necessary, the principles relating to processing of personal data cannot be overrun.[100] According to Zuiderveen Borgesius, necessity can be further divided into two steps: subsidiarity and proportionality.[101] From the perspective of subsidiarity, the processing of personal data should be the least restrictive measure and there should not be an alternative option to achieve the legitimate interest.[102] The evaluation of the necessity and the legitimate interest is not straightforward since the purpose of collection of non-user personal data is not well-defined in the privacy policies. Nonetheless, it seems quite a restrictive measure to collect personal data of the users' connections, especially of those who do not use the service. Even if the processing of personal data is considered

[93] *Ibid*., p 41 D.
[94] OJ L 281, 23.11.1995.
[95] 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), OJ L 201, 31.7.2002, p 37-47, recital 25.
[96] Kamara, de Hert, *supra nota* 72, p 332.
[97] *Ibid.*, p 330.
[98] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC (WP217), 09.04.2014.
[99] Kamara, de Hert, *supra nota* 72, p 331-332.
[100] *Ibid.*
[101] Zuiderveen Borgesius (2015), *supra nota* 65, p 168.
[102] *Ibid*.

as necessary, it should be done in accordance with the principles relating to processing, following the proportionality step.[103] Regarding the necessity of collecting non-user personal data, individual assessment is needed.

The user of WhatsApp must share address book information frequently with the service provider.[104] Address book is needed for the recognition of the users of WhatsApp from the address book and consequently connect the users inside the application. For every user, WhatsApp creates an ID number which consists of the phone number of the user which enables the recognition of the users from the address book.[105] The contacts, which are not users of the service, are stored in the database, differentiated from the users.[106] The phone number as a part of the user ID is not technically essential because when the phone number of the user changes, it is possible that the user ID remains the same.[107] It might be useful that the user does not have to add the address book himself. However, it is a feature of the application but not necessary in order to provide the core messaging service. Besides, it is not known, for how long the personal data is stored in the database.

Even though the processing of personal data is based on legitimate interest, the data minimisation and purpose limitation rules or any other rules relating to processing still apply. The service provider cannot collect as much personal data as it wants, but only the personal data which is strictly necessary to achieve the purpose of processing. The main purpose for processing personal data, is to offer the messaging service to its customers. WhatsApp would be able to offer the service without having to check through the address book. Facebook Inc. has another similar application, Messenger, which does not require the frequent sharing of address book by default. In essence, Facebook Inc. is already using alternative option for connecting the users of the application without the need to collect phone numbers of the users. As it has been already established, the necessity by definition requires the use of the least restrictive alternative, which WhatsApp however is not using. Which is why the argument concerning the necessity of collecting address book information of the users cannot be considered valid.

---

[103] *Ibid*.
[104] Privacy Policy. WhatsApp. Accessible: https://www.whatsapp.com/legal/?eea=1#privacy-policy 14 February 2019.
[105] Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. – *Digital Investigation*, Vol. 11, Issue 3, p 204.
[106] *Ibid*.
[107] *Ibid*., p 212.

Facebook and Instagram collect the users' address book information, call log and SMS log history if the user agrees to it.[108] Both applications request the user's consent in order to access the information, although personal data of non-users cannot be processed based on his consent as the user cannot consent on behalf of someone else. Therefore, the collection of such data lacks the element of necessity as the address book information, call log and SMS log history is not needed for the functioning of the service. Call log and SMS log history themselves contain phone numbers, names of the sender or the recipient but also the time and date which becomes personal data as well, since the specific time and date are linked to an identifiable person. It cannot be proven that this personal data is used for data mining, but it most certainly gives more information of how often the user of the service and his contacts are interacting with each other. The practice seems disproportionate, taking into account the possibility of using the call log and SMS log history for data mining purposes together with unspecified purpose for collecting that data.

Snapchat and Twitter both collect address book information of their users when they have given a permission. The purpose seems to be connecting the users with the contacts who are also using Snapchat or Twitter. It does not fulfil the criteria for necessity, since it cannot be considered to be the least restrictive option for connecting users of Twitter or Snapchat inside the service. When address book containing information of non-user, is uploaded to Twitter or Snapchat, personal data of non-user is processed at least to the extent that the service provider recognizes that the person is not a user of the service. The service providers do not even claim in their privacy policies that the address book information would be necessary in order to connect the users of the service. Hence, the requirement of necessity is not met.

Third step of the balancing test is the evaluation of the legitimate interest and necessity of processing against the fundamental rights and freedoms of the data subject and the impact of the processing to them.[109] The SNS providers' legitimate business interest have been established earlier but the collecting of non-user personal data lacks the necessity, thus it cannot pass the balancing test. As the necessity is required by law, the processing cannot be based on legitimate interest without necessity. Besides, the controller must consider the reasonable expectations of the

[108] *Data Policy*. Facebook. Accessible: https://www.facebook.com/policy.php 14 February 2019, *Data Policy*. Instagram. Accessible: https://help.instagram.com/155833707900388 14 February 2019.
[109] Kamara, de Hert, *supra nota* 72, p 332.

data subject, which means that the processing of the personal data should have been foreseeable.[110] A person who does not use SNSs could reasonably expect that he will not be tracked by SNS provider whose service he is not using. It is also burdensome for the user of these services that there is no possibility to use the service without revealing someone else's personal data, which is the case with WhatsApp. Taking into consideration the broad user basis the evaluated SNS providers have, it is almost impossible not to be tracked by them.

Even though, in the cases Belgian Commission for the Protection of privacy versus Facebook Inc.[111] the tracking of non-users via cookies was much more extensive than the tracking of non-users through address books, SMS log and call log history, the outcomes were similar when assessing the legal basis for processing non-user personal data. In both present and the Belgian cases there were problems with the transparency relating to the purpose of collecting and processing the data and the valid consent of the data subject.[112] Even though, the decision by Belgian court is not directly applicable, it shows how a similar situation has been legally examined. It may be deduced from the judgement of the Belgian court that the non-user personal data should not be based on legitimate interest but rather on the informed consent of the data subject.

The processing of non-user personal data does not pass the balancing test not only because it is not necessary but because the processing is not in balance with the data subjects' rights to privacy and data protection. The non-user does not benefit from the collection of his personal data in any way and cannot determine himself whether he wants to disclose his personal data with these SNS providers or not. Considering that their business models are based on collecting personal data and selling that data to other businesses, consequently the SNS providers are financially benefiting from the collection of the personal data of the non-users at the cost of the non-users' privacy, which makes it highly unproportionate. If the data was not be valuable to the service providers, there would not be a reason for collecting such data. In addition, non-users are not connected to the contract between the user and the service provider in any way, therefore the processing of their personal data does not make much sense. The SNS providers' legitimate interest override the non-user's right to privacy and data protection. For these reasons, the processing of non-user personal data cannot be based on legitimate interest of the controller.

[110] Kamara, de Hert, *supra nota* 72, p 334.
[111] Nederlandstalige rechtbank van eerste aanleg Brussel, 2015/57/C, 09.11.2015; Nederlandstalige rechtbank van eerste aanleg Brussel, AR 2016/153/A, 16.02.2018.
[112] Nederlandstalige rechtbank van eerste aanleg Brussel, AR 2016/153/A, 16.02.2018, p 34.

3. PROPOSALS

The processing of non-user personal data, by the SNS providers evaluated in this paper, lacks the legal ground under the GDPR. The most suitable legal ground for processing non-user personal data would be processing based on informed consent of the non-user. The SNS providers cannot outsource the duty to ask for consent to the users because the SNS providers are accountable for demonstrating the compliance. In practice however, the SNS providers cannot ask the consent from the non-users, since it would require processing of the non-user personal data prior the consent. EPrivacy Directive also prohibits the direct marketing by automated calling systems without the prior consent.[113] Therefore, the SNS providers cannot contact the non-users without the non-users themselves requesting the processing of their personal data.

Processing of non-users' personal data violates data subject's rights and basic principles relating to the processing of personal data. The processing of non-users' personal data violates "the right to be informed of processing"[114], since the non-users are not informed about the processing of their personal data nor the transfer of the non-users' data to third countries. Consequently, the non-users cannot exercise "the right of access"[115] since they are not aware of the processing activities and cannot demand access. The data subjects cannot be expected to contact every SNS provider and demand access to their personal data, in order to find out who are processing their personal data and who are not. The non-users cannot demand "the right to erasure of their data"[116] for the same reasons as they cannot demand access. The request for erasure would not even matter in the case of WhatsApp, who frequently collects the address book information. Since the non-users are not providing personal data to the SNS provider and cannot effectively exercise the control over their personal data, since someone else is providing it to the SNS providers. Thus, they cannot exercise their "right to restriction the processing"[117]. The applications by design enables the wrongful processing of personal data since non-user personal data should not be collected the very

[113] OJ L 201, 31.7.2002 art 13 sec. 1.
[114] OJ L 119, 4.5.2016 art 14.
[115] OJ L 119, 4.5.2016 art 15.
[116] OJ L 119, 4.5.2016 art 17 sec. 1(d).
[117] OJ L 119, 4.5.2016 art 18 sec. 1(b).

beginning. The processing is unlawful, goes beyond what is relevant or necessary and lacks the transparency thus violating the principles relating to processing.[118] For above-mentioned reasons, Twitter, Snapchat, Facebook, WhatsApp and Instagram should terminate the illegitimate processing of non-user personal data in the EU, meaning the processing of address book, call and SMS log history information containing non-user data. As well as they should delete the collected non-user personal data from their databases.

It seems that many practices which would not be acceptable in the real-life business policies are somehow acceptable in the internet. For example, if a courier service would demand its customers to disclose all addresses of the customer's friends when sending a parcel, it would be convenient for the courier service, as they would know the addresses beforehand and the customer would only have to tell the name of the recipient. Still, it seems unlikely that anybody would agree to it. Why it would be acceptable to demand it on internet? Yet, it seems to be a common practice among the biggest SNS providers. It is not the question of inadequate legislation anymore. In fact, as shown in this paper the GDPR prohibits such practice and in theory protects the non-user's right to privacy and data protection. However, the problem seems to be on a pragmatic level. An individual cannot effectively defend his rights against big SNS providers. Instead, collective actions should be taken in order to truly make a change in the privacy policies of the SNS providers. As it is the duty of the Data Protection Authorities to monitor the compliance of the controller with the GDPR, more active intervention would be needed. Data Protection Authorities are also able to impose administrative fines to the controllers who infringe the GDPR and therefore more capable to protect the rights of individuals.[119]

[118] OJ L 119, 4.5.2016 art 5
[119] OJ L 119, 4.5.2016 art 83.

CONCLUSION

The aim of the paper was to evaluate from the perspective of the GDPR the lawfulness of collecting and processing of non-user personal data by a few major SNS providers, namely Twitter, Snapchat, Facebook, WhatsApp and Instagram. The hypothesis of the paper was that the practice of collecting non-user personal data is unlawful.

In the first part of the paper, the compliance of privacy policies was assessed with the legal requirements of the GDPR relating to the data subject's rights and principles relating to the processing of personal data. Multiple infringements and potential risks were mentioned in the assessment. The data subjects were unable to fully exercise their rights mainly because they were not informed of their personal data being processed by the SNS providers, nor they were aware that their data would be transferred outside of the EU. The processing of non-user personal data was nothing but transparent and the basis for processing such data was not mentioned in the privacy policies. The privacy policies had overall vague wordings and the purpose for processing was not defined well enough. There were also issues with data minimisation, since the processing did not seem necessary and the privacy by default principle as the applications collected personal data which they should not be collecting.

The second part of the paper evaluated the applicable lawful basis for processing non-user personal data. There are six legal bases for processing non-user personal data but three of them were only evaluated briefly since they were not suitable bases for processing. Processing based on vital interest could not be used since there was no vital interest. Processing based on performance of a task carried out in the public interest was not suitable because there was not such a task which the SNS providers were carrying out. Neither processing based on legal obligation was suitable since the SNS providers do not have a legal obligation, which would require the collection of non-user personal data. Processing based on consent was evaluated, but the SNS providers cannot rely on it mainly because the consent is not given by the non-user himself. The SNS providers cannot rely on performance of a contract even though there is a contract between the user and the service provider, as the contract would have to be between the service provider and the non-user. The

legitimate interest of the SNS provider was not acceptable ground for processing either, since the processing of non-user personal data was not necessary and overall, was not in balance with the non-user's right to privacy. The hypothesis was proven as there was not a legal ground, which the SNS provider could not rely when processing non-user personal data, as a consequence the processing of such personal data is unlawful.

In third section of the paper, proposals were made based on the findings of the paper. Firstly, the SNS providers could process non-user personal data only if it was initiated by the non-user. Secondly, Twitter, Snapchat, Facebook, WhatsApp and Instagram have to stop processing non-user personal data and delete the already collected non-user personal data. Thirdly, more active intervention from the side of Data Protection Authorities is needed, in order to ensure the compliance of the GDPR and protection of fundamental rights and freedoms of data subjects.

LIST OF REFERENCES

Scientific books

1. *EU Internet Law: Regulation and Enforcement*. (2017). /Eds. T-E. Synodinou, P. Jougleux, C. Markou, T. Prastitou. Nicosia: Springer.

2. Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU.* Vol. 31. Brussels: Springer.

3. Kelleher, D., Murray, K. (2018). *EU Data Protection Law.* 1st ed. London: Bloomsbury Professional.

4. Kuner, C. (2007). *European Data Protection Law: Corporate Compliance and Regulation.* 2nd ed. Oxford: Oxford University Press.

5. *New European General Data Protection Regulation: A Practitioner's Guide Ensuring Compliant Corporate Practice.* (2018). /Eds. D. Rücker, T. Kugler. Baden-Baden: C. H. Beck, Hart, Nomos.

6. *Reforming European Data Protection Law.* (2015). /Eds. S. Gutwirth, R. Leenes, P. de Hert. Vol. 20. Brussels: Springer.

7. Voigt, P., von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st ed. Berlin: Hamburg: Springer.

Scientific articles

8. Balboni, P., Cooper, D., Imperiali, R., Macenaite, M. (2013). Legitimate interest of the controller New data protection paradigm: legitimacy grounded on appropriate protection. – *International Data Privacy Law*, Vol. 3, No. 4, 244-261.

9. Blume, P. (2012). Will it be a better world? The proposed EU Data Protection regulation. – *International Data Privacy Law*, Volume 2, Issue 3, 130-136.

10. Borghi, M., Ferretti, F., Karapapa, S. (2013). Online data processing under EU law: a theoretical framework and empirical evidence from the UK. – *International Journal of Law and Information Technology*, Vol. 21, No. 2, 109-153.

11. Castelluccia, C. (2012). Behavioural Tracking on the Internet: A Technical Perspective. – *European Data Protection: In Good Health?* (Eds.) S. Gutwirth, R. Leenes, P. de Hert, Y. Poullet. Brussels: Springer, 21-33.

12. Esteve, A. (2017). The business of personal data: Google, Facebook and privacy issues in the EU and the USA. – *International data privacy law*, Vol. 7, No. 1, 36-47.

13. Ferretti, F. (2014). Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights. – *Common Market Law* Review, Vol. 51, Issue 3, 843-868.

14. Gil Gonzalez, E., de Hert, P. (2019) Understanding the legal provisions that allow processing and profiling of personal data – an analysis of GDPR provisions and principles. – *ERA Forum*, 1-25.

15. Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., Leucci, S. (2018). Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR – *European Data Protection Law Review*, Vol. 4, 168-189

16. Kamara, I., de Hert, P. (2018). Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. – *The Cambridge Handbook of Consumer Privacy*. (Eds.) E. Selinger, J. Polonetsky, O. Tene. Cambridge: Cambridge University Press, 321-352.

17. Kerber, W. (2016). Digital markets, data, and privacy: competition law, consumer law and data protection. – *Journal of Intellectual Property Law & Practice*, Vol. 11, No. 11, 856-866.

18. Maxwel, W. J. (2015). Principles-based regulation of personal data: the case of 'fair processing'. – *International Data Privacy Law*, Vol. 5, No. 3, 205-216.

19. Truyens, M. (2016). No More Cookies for Unregistered Facebook Users in Belgium: Belgian Data Protection Legislation Applies to Facebook. – *European Data Protection Law Review*, Vol. 2, Issue 1, 135-140.

20. van Ooijen, I., Vrabec, H. U. (2018). Does the GDPR Enhance Consumers' Control over Personal Data?: An Analysis from a Behavioural Perspective. – *Journal of Consumer Policy,* 1-17. Accessible: https://doi.org/10.1007/s10603-018-9399-7, 13 March 2019.

21. Warren, S., Brandeis, L. (1890). The Right to Privacy. – *Harvard Law Review*, Vol. IV, No. 5, 193-220.

22. Zuiderveen Borgesius, F. J. (2015). Personal data processing for behavioural targeting: which legal basis?. – *International data privacy law*, Vol. 5, No. 3, 163-176.

23. Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C., Helberger, N. (2017.) Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. – *European Data Protection Law Review*, Vol. 3, Issue 3, 353-368.

EU and international legislation

24. 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, OJ L 281, 23.11.1995, p. 31-50

25. 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), OJ L 201, 31.7.2002, p 37-47

26. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p.1-88

Court decisions

27. Court decision, 6.11.2003, Lindqvist, C-101/01, EU:C:2003:596.

28. Court decision, 13.05.2014, Google Spain and Google, C-131/12, EU:C:2014:317.

29. Nederlandstalige rechtbank van eerste aanleg Brussel, 15/57/C, 09.11.2015.

30. Hof van beroep Brussel, 2016/KR/2, 29.06.2016.

31. Nederlandstalige rechtbank van eerste aanleg Brussel, 2016/153/A, 16.02.2018.

Other sources

32. Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. – *Digital Investigation*, Vol. 11, Issue 3, 201-213.

33. Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (WP259), 28.11.2017

34. Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC (WP217), 09.04.2014.

35. *Data Policy.* Facebook. Accessible: https://www.facebook.com/policy.php 14 February 2019.

36. *Data Policy.* Instagram. Accessible: https://help.instagram.com/155833707900388 14 February 2019.

37. Eagel, N., Pentland, A. S., Lazer, D. (2009). Inferring friendship network structure by using mobile phone data. – *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 106, No. 36, 15274-15278.

38. *How can I manage contact uploading with the Facebook app?* Facebook Help center. Accessible: https://www.facebook.com/help/355489824655936?helpref=faq_content 10 March 2019.

39. *Privacy Policy.* Snapchat. Accessible: https://www.snap.com/en-US/privacy/privacy-policy/#european-union-users 14 February 2019.

40. *Privacy Policy.* Twitter. Accessible: https://twitter.com/en/privacy 14 February 2019.

41. *Privacy Policy.* WhatsApp. Accessible: https://www.whatsapp.com/legal/?eea=1#privacy-policy 14 February 2019.

42. Van Bael & Bellis. (2016) Facebook Wins Privacy Appeal before Belgian Court of Appeal. – *Van Bael & Bellis on Belgian Business Law*, Vol. 2016, No. 7, p 7-8, Accessible: https://www.vbb.com/media/Insights/BE_07_16.pdf , 16 March 2019.