Applicability of the GDPR to the data processing activities carried out by the non-EU controllers and processors

University of Turku
Faculty of Law
Anna Naumchuk
Master's thesis
MDP in Law and Information Society
May 2020

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

UNIVERSITY OF TURKU

Faculty of Law

ANNA NAUMCHUK:

Applicability of the GDPR to the data processing activities carried out by the non-EU controllers and processors

Master's thesis, 95 p.

Master's Degree Programme in Law and Information Society

May 2020

Broadening the scope of EU data protection law due to the entering into force of the General Data Protection Regulation has made many companies review their data processing practices. Especially changes have affected the non-EU entities which appeared to be pursued under the new Regulation for the activities that only yesterday were outside the territorial scope of law.

This master's thesis aims at providing the comprehensive analysis of the conditions under which a non-EU controller or processor will be subject to the GDPR. For this purpose, it analyzes the grounds for the GDPR applicability from the non-EU controllers' and processors' perspective.

Besides provision of the theoretical background regarding various concepts and processing activities, the work pays considerable attention to the practical side of the matter. It presents diverse examples of the GDPR applicability to the non-EU operators, including both the situations where certain evidences are sufficient to invoke the Regulation and, by contrast, those which are missing appropriate grounds.

In addition, the paper is an attempt to fill up the gaps, which the EDPB has not addressed in the Guidelines on the territorial scope, and, where possible, to provide the probable solutions to the existing issues.

Keywords: *non-EU controller, non-EU processor, data protection, GDPR applicability, territorial scope, establishment in the Union, targeting, offering of goods and services, monitoring*

TABLE OF CONTENTS

BIBLIOGRAPHY

Literature

Barlag, Charlotte, *Anwendungsbereich der Datencshutz-Grundverordnung* in: Roβnagel, Alexander (ed.), *Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts (1st edition)*. Baden-Baden: Nomos (NomosPraxis), 2017, 108-118

Jay, Rosemary – Malcolm, William – Parry, Ellis et al., *Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition)*. London: Sweet & Maxwell, 2017. (Jay 2017)

Plath, Kai-Uwe (Hrsg.), *BDSG/DSGVO. Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG (2. Auflage)*. Köln: Otto Schmidt, 2016. (Plath 2016)

Skouma, Georgia – Leonard, Laura, *On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection* in: Gutwirth, Serge – Leenes, Ronald – de Hert, Paul (eds.), *Reforming European Data Protection Law*. Springer Science+Business Media Dordrecht, 2015, 35-60. (Skouma – Leonard 2015)

Svantesson, Dan Jerker, *Territorial scope* in: Kuner, Christopher – Bygrave, Lee A. – Docksey, Christopher (eds.), *Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)* – non-final draft commentaries, 2019, 1-18. (Svantesson 2019)

Ustaran, Eduardo, *The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach* in: Ismail, Noriswadi – Yong Cieh, Edwin Lee (eds.), *Beyond Data Protection. Strategic Case Studies and Practical Guidance*. Springer-Verlag Berlin Heidelberg, 2013, 135-156. (Ustaran 2013)

Voigt, Paul – von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer International Publishing AG, 2017. (Voigt – von dem Bussche 2017)

Wisman, Tijmen H. A. *Privacy, data protection and e-commerce* in: Lodder, Arno R. – Murray, Andrew D. (eds.), *EU Regulation of E-commerce: A Commentary*. Cheltenham: Edward Elgar Publishing, 2017, 349-382

Articles

Alich, Stefan – Voigt, Paul, Mitteilsame Browser – Datenschutzrechtliche Bewertung des Trackings mittels Browser-Fingerprints, Computer und Recht, Vol. 28, Issue 5 (2012), 344-348. (Alich – Voigt 2012)

Azzi, Adèle, The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation, Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 9, Issue 2 (2018), 126-137

Bygrave, Lee A. Determining Applicable Law pursuant to European Data Protection Legislation. Computer Law & Security Report, Vol. 16 (2000), 252–257

de Hert, Paul – Czerniawski, Michal, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, Vol. 6, No. 3 (2016), 230-243. (de Hert – Czerniawski 2016)

Granmar, Claes G. Global applicability of the GDPR in context. Available at: <www.diva-portal.org/smash/get/diva2:1274839/FULLTEXT01.pdf>. 14 January 2019 – last updated. (Granmar 2019)

Gömann, Merlin, The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement. Common Market Law Review, Vol. 54 (2017), 567-590. (Gömann 2017)

Karaduman, Ozan, The General Data Protection Regulation: Achieving Compliance for EU and non-EU Companies. Business Law International, Vol. 18, No 3 (2017), 225-232

Kartheuser, Ingemar – Schmitt, Florian, Der Niederlassungsbegriff und seine praktischen Auswirkungen. Anwendbarkeit des Datenschutzrechtes eines Mitgliedstaats auf ausländische EU-Gesellschaften. 6(4) Zeitschrift für Datenschutz (2016), 155-159

Korff, Douwe, The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service, 19 August 2019). Available at SSRN: <www.ssrn.com/abstract=3439293>. (Korff 2019)

Moerel, Lokke, The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? International Data Privacy Law (2011), Vol. 1, No. 1, 28-46

Safari, Beata A., Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. Seton Hall Law Review, Vol. 47 (2017), 809-848. (Safari 2017)

Schonhofen, Sven – Detmering, Friederike, Territorial applicability of the GDPR. New EU data protection law also to apply to non-EU organizations. Business Law Magazine, Vol. 1 (2018), 3-5

Svantesson, Dan Jerker B. Pammer and Hotel Alpenhof – ECJ decision creates further uncertainty about when e-businesses "direct activities" to a consumer's state under the Brussels I Regulation. Computer Law & Security Review, Vol. 27 (2011), 298-304. (Svantesson 2011)

Tene, Omer – Wolf, Christopher, Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation. The Future of Privacy Forum White Paper, 2013

Case law

Court of Justice of the European Union

CJEU, Case 168/84, Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt, 4 July 1985

CJEU, Case 196/87, Udo Steymann v Staatssecretaris van Justitie, 5 October 1988

CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014. (Google Spain case)

CJEU, Case C-191/15, Verein für Konsumenteninformation v Amazon EU Sàrl, 28 July 2016. (Verein für Konsumenteninformation case)

Opinions of Advocates General of the CJEU

Opinion of Advocate General Cruz Villalón, delivered on 25 June 2015, Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság. (Opinion of Advocate General Villalón)

Opinion of Advocate General Jääskinen, delivered on 25 June 2013, Case C-131/12, Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González. (Opinion of Advocate General Jääskinen)

Opinion of Advocate General Trstenjak, delivered on 18 May 2010, Case C-585/08, Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Case C-144/09, Hotel Alpenhof GesmbH v Oliver Heller. (Opinion of Advocate General Trstenjak)

EU Legislation

Agreement on the European Economic Area, 13 December 1993

Consolidated version of the Treaty on the Functioning of the European Union, 26 October 2012, 2012/C 326/01. (TFEU)

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters – no longer in force. (Brussels I Regulation)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). (Directive on electronic commerce)

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. (DPD; Data Protection Directive)

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services

Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (GDPR; Regulation)

Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)

Materials from the EU data protection bodies

Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC. Available at: <www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>

European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Version 2.0, 12 November 2019. (EDPB Guidelines)

The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019. Available at: <www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>

The Information Commisioner's Office, Enforcement Notice to AggregateIQ Data Services Ltd ("AIQ"), The Data Protection Act 2018, Part 6, Section 149, dated 24 October 2018. Available at: <www.ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf>. (The First Enforcement Notice to AIQ, dated 24 October 2018)

The Information Commisioner's Office, Enforcement Notice to AggregateIQ Data Services Ltd ("AIQ"), The Data Protection Act 2018, Part 6, Section 149, dated 6 July 2018. Available at: <www.ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf>

The Information Commissioner's Office, Information rights and Brexit Frequently Asked Questions, 29 January 2020. Available at: <www.ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf>

The Information Commissioner's Office, Intention to fine Marriott International, Inc. more than £99 million under GDPR for data breach, 9 July 2019. Available at: <www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/>

Opinions, guidelines and other documents from the Article 29 Working Party

WP29, EU General Data Protection Regulation, General Information Document, 12 February 2018. Available at: <www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614208>

WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN, WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018

WP29, Opinion 1/2008 on data protection issues related to search engines, 00737/EN, WP 148, adopted on 4 April 2008

WP29, Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN, WP 169, adopted on 16 February 2010. (WP29, Opinion 1/2010 on the concepts of "controller" and "processor")

WP29, Opinion 8/2010 on applicable law, 0836-02/10/EN, WP 179, adopted on 16 December 2010. (WP29, Opinion 8/2010 on applicable law)

WP29, Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, 176/16/EN, WP 179 update, adopted on 16 December 2015. (WP29, Update of Opinion 8/2010 on applicable law)

WP29, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final, WP 56, adopted on 30 May 2002. (WP29, Working document on processing on the Internet by non-EU based web sites)

Other official materials from the European Union

Council of Europe, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum, adopted 23 November 2010

Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]

Official publications

Department of Official Language, President's Order, 1960, Copy of Notification No. 2/8/60-O.L. (Ministry of Home Affairs), 27 April 1960. Available at: <www.rajbhasha.gov.in/en/presidents-order-1960>

Johnson, Boris, UK / EU relations: Written statement – HCWS86 of 3 February 2020. Available at: <www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2020-02-03/HCWS86/>

The European Free Trade Association, General Data Protection Regulation (GDPR) entered into force in the EEA, 19 July 2018. Available at: <www.efta.int/EEA/news/General-Data-Protection-Regulation-GDPR-entered-force-EEA-509576>

Online sources

All of the world's top-level domains, 18 June 2019 – last updated. Available at: <www.norid.no/en/om-domenenavn/domreg/>

BBC News, .london web domain name goes on sale for first time, 29 April 2014. Available at: <https://www.bbc.com/news/uk-england-london-27193725>

Bird & Bird, Guide to the General Data Protection Regulation, May 2020 version, 26 May 2020 – last visited. Available at: <www.twobirds.com/~/media/pdfs/gdpr-

pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>. (Bird & Bird, Guide to the General Data Protection Regulation)

Complaint under Article 77(1) GDPR, noyb Case Nr: C-07/18, 18 January 2019. Available at: <www.noyb.eu/wp-content/uploads/2019/01/Netflix_Complaint_geschw%C3%A4rzt.pdf>

Complaint under Article 77(1) GDPR, noyb Case Nr: C-14/18, 18 January 2019. Available at: <www.noyb.eu/wp-content/uploads/2019/01/YouTube_Complaint_geschw%C3%A4rzt.pdf>

Complaint under Article 77(1) GDPR, noyb Case Nr: C-16/18, 18 January 2019. Available at: <www.noyb.eu/wp-content/uploads/2019/01/Amazon_Complaint_geschw%C3%A4rzt.pdf>

Complaint under Article 77(1) GDPR, noyb Case Nr: C-17/18, 18 January 2019. Available at: <www.noyb.eu/wp-content/uploads/2019/01/AppleMusic_Complaint_geschw%C3%A4rzt.pdf>

Country-code top-level domains with commercial licenses, 17 May 2020 – last edited. Available at: <www.en.wikipedia.org/wiki/Country_code_top-level_domains_with_commercial_licenses>

European Union, EU languages, 20 May 2020 – last published. Available at: <www.europa.eu/european-union/about-eu/eu-languages_en>

European Union, Use of the euro outside the euro area, 16 December 2019 – last published. Available at: <www.europa.eu/european-union/about-eu/euro/use-euro-outside-euro-area_en>

European Union, Which countries use the euro, 1 February 2020 – last published. Available at: <www.europa.eu/european-union/about-eu/euro/which-countries-use-euro_en>

Hill, Rebecca, Washington Post offers invalid cookie consent under EU rules – ICO, 19 November 2018. Available at: <www.theregister.co.uk/2018/11/19/ico_washington_post/>

Hunton Andrews Kurth, Centre for Information Policy Leadership, Comments by the Centre for Information Policy Leadership on the European Data Protection Board's "Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)" Adopted on 16 November 2018, 18 January 2019. Available at: <www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_edpbs_territorial_scope_guidelines.pdf>

IANA Report on the Delegation of the .eu Top-Level Domain, March 2005. Available at: <www.iana.org/reports/2005/eu-report-05aug2005.pdf>

ICANN, Resources for Country Code Managers. Glossary: Country-code top-level domain, 26 May 2020 – last visited. Available at: <www.icann.org/resources/pages/cctlds-21-2012-02-25-en>

Information Commissioner's Office's letter to WP Company LLC, 11 October 2018. Available at: <www.mega.nz/#!mkISAIrb!xrior2Ffk7C_ILuNTqa9uPhuzMYPUjU19FSwfZTFrqM>

International Calling Codes, 26 May 2020 – last visited. Available at: <www.internationalcitizens.com/international-calling-codes/>

LinkedIn Marketing Solutions, Market to who matters, 26 May 2020 – last visited. Available at: <www.business.linkedin.com/marketing-solutions>

LinkedIn Sales Solutions, LinkedIn Sales Navigator, 26 May 2020 – last visited. Available at: <www.business.linkedin.com/sales-solutions/sales-navigator>

Linklaters, The General Data Protection Regulation: A survival guide – Version 2.0, 13 December 2018. Available at: <www.linklaters.com/en/insights/publications/2016/june/guide-to-the-general-data-protection-regulation>, p. 8

List of Internet top-level domains. Geographic top-level domains, 23 May 2020 – last edited. Available at: <www.en.wikipedia.org/wiki/List_of_Internet_top-level_domains#Geographic_top-level_domains>

Make Way for youtu.be Links, 21 December 2009. Available at: <www.youtube.googleblog.com/2009/12/make-way-for-youtube-links.html>

Marriott International headquarters and office locations. Available at: <www.craft.co/marriot-international/locations>

Meisinger, Jeremy, Weltimmo v. Hungarian Data Protection Authority: EU Rules on What It Means To Be "Established" in a Jurisdiction, 2 December 2015. Available at: <www.securityprivacyandthelaw.com/2015/12/weltimmo-v-hungarian-data-protection-authority-eu-rules-on-what-it-means-to-be-established-in-a-jurisdiction/>

Netflix, Spotify & YouTube: Eight Strategic Complaints filed on "Right to Access", 18 January 2019. Available at: <www.noyb.eu/access_streaming/>

New Guidance on the GDPR's Territorial Scope – Are You Covered?, 30 November 2018. Available at: <www.debevoise.com/insights/publications/2018/11/new-guidance-on-the-gdprs-territorial-scope>

Privat24 home page, 26 May 2020 – last visited. Available at: <www.next.privat24.ua/>

Rouse, Margaret, top-level domain (TLD), April 2009 – last updated. Available at: <www.searchapparchitecture.techtarget.com/definition/top-level-domain-TLD>

The full list of generic TLDs can be found here: Generic top-level domains (gTLD), 18 June 2019 – last updated. Available at: <www.norid.no/en/om-domenenavn/domreg/#gtld>

LIST OF ABBREVIATIONS

APPA	Asia Pacific Privacy Authorities
Brexit	"British exit" (refers to the UK's withdrawal from the EU)
ccTLD	country-code top-level domain
CCTV	closed-circuit television (video surveillance)
CJEU	Court of Justice of the European Union
clTLD	city-level top-level domain
CNIL	Commission Nationale de l'Informatique et des Libertés (The French Data Protection Authority)
DPD	Data Protection Directive
EDPB	European Data Protection Board
EEA	European Economic Area
EFTA	European Free Trade Association
EU	European Union
GDPR	General Data Protection Regulation
IANA	The Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICO	The Information Commissioner's Office (The UK Data Protection Authority)
Inc.	Incorporated
IP	Internet Protocol
LLC	limited liability company
Ltd	limited

RFID	radio frequency identification
TFEU	Treaty on the Functioning of the European Union
TLD	top-level domain
UK	The United Kingdom of Great Britain and Northern Ireland
US	The United States of America
Wi-Fi	‘Wireless Fidelity’
WP29	The Article 29 Working Party

I. INTRODUCTION

1.1. Topicality

Broadening the scope of EU data protection law due to the entering into force of the General Data Protection Regulation *(hereinafter – GDPR)* has made many companies review their data processing practices. Especially changes have affected the non-EU entities which appeared to be pursued under the new Regulation for the activities that only yesterday were outside the territorial scope of law.

In comparison with the Data Protection Directive *(hereinafter – DPD)*[1], the GDPR has substantially extended grounds for the applicability to the non-EU controllers and processors. The GDPR explains such enlargements in the scope of applicability with the need "to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation"[2]. Among major changes, one can find the law extension to the non-EU processors. Also, under the establishment principle, the place of processing has become irrelevant. What is more, the Regulation provides two fundamentally new grounds for the applicability to the non-EU operators – offering of goods or services and behavioral monitoring – united under the targeting principle.

All these novelties complement the already existing establishment principle and add new conditions, or, if assessing from the non-EU-entities' perspective, issues. To a non-EU controller or processor, which has subsidiaries in the Union, the said 'improvements' seem to bring a lot more confusion than certainty. As regards those entities which are not established in the EU, the situation is not a bit better since all their data processing activities are now potential triggers of the targeting principle to them. Furthermore, while broadening the scope of the GDPR application, the legislator has not even addressed the notions of a non-EU controller and a non-EU processor. So, the non-EU operators are in need of clarity with regard to all the mentioned issues.

Being a starting point in the application of the whole GDPR in principle, Article 3 Sections 1 and 2 have to be the first thing that the non-EU controllers and processors

[1] 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, Article 4(1)

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 23

consult[3], because if Article 3 GDPR is not applicable to them, then it stands no reason checking whether they comply with the other provisions. Therefore, it is important to closely examine all the grounds that may invoke application of the GDPR to the non-EU entities.

Aiming at clarifying the criteria established in the Regulation, the European Data Protection Board *(hereinafter – EDPB)* has issued general Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)[4], which contemplate the applicability of the GDPR provisions to various actors – both the EU and the non-EU ones. Despite casting light upon various aspects, Guidelines are abundant in inaccuracies and inconsistencies with the text of the Regulation. Also, they are silent about many practical moments and do not step aside from the straightforward scenarios. Nevertheless, they remain in fact the only official interpretation from the public authority on the matter at stake.

1.2. Research aims and research question

This study aims at, first of all, analyzing the grounds for the GDPR applicability from the non-EU controllers' and processors' perspective, notably, in isolation from the EU actors, where possible. Secondly, it intends to focus on the practical side of the matter by providing diverse examples of application that would allow drawing the line between what evidences are sufficient for the applicability of the GDPR and what are not weighty enough. Thirdly, the study will try to fill up the gaps that the EDPB has not addressed and, where possible, provide the probable solutions to the existing issues.

Therefore, on the basis of the aforesaid, this thesis is going to answer the following research question:

Under what conditions will a non-EU controller or processor be subject to the GDPR?

1.3. Limitations of the paper

In spite of being an attempt of considering various situations when the GDPR will apply to the data processing activities carried out by the non-EU controllers and processors, this study does not address the cases where the non-EU entities are pursued under the

[3] Svantesson, Dan Jerker, *Territorial scope* in: Kuner, Christopher – Bygrave, Lee A. – Docksey, Christopher (eds.), *Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)* – non-final draft commentaries, 2019, 1-18, p. 8

[4] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Version 2.0, 12 November 2019

GDPR by virtue of public international law (Article 3(3)) since such example of application states the obvious and goes far beyond the scope of data protection field.

Also, the paper covers neither the questions of transfers to the third states nor the enforcement issues since the said cases, though involve the non-EU controllers and processors, however, concern situations where the applicability of the GDPR is already established and uncontested.

1.4. Research methods

The methods used in this paper are conditional on the research question stipulated above. Taking into account that the legislative act underlies the whole study and serves as the main source of research, the *doctrinal method* was chosen to conduct the analysis of the respective provisions of the GDPR. Also, it was used to examine the case law on the matter and various advisory documents form the public authorities, such as guidelines, opinions and recommendations.

Both core chapters of the thesis were examined following the same steps based on the *structure* of the respective parts of Article 3 GDPR. First, there was provided general overview of the principle laid down into the law provision and its key concepts, thereby introducing general *theoretical background*. Second step included breaking down the analyzable provision into as small elements as possible and examining each of them separately; when few elements were studied in detail, then it was possible to consider them in combination with each other, gradually layering new details onto them. When theoretical background was researched enough, *practical situations* were added as the completion phase in order to contemplate various issues of applicability to the non-EU entities. Thus, step by step both criteria of the GDPR applicability were examined.

Also, the study applied *interbranch legal method*, particularly, in two cases: for comparison of the concept of establishment in data protection law and in company law, and for retracing interconnections of the concept of directing activities in consumer protection field with the concept of targeting in data protection law.

Additionally, *historical and legal method* was applied in order to demonstrate the development of the concept of targeting within the legal doctrine, which originated from the context of consumer contracts in Brussels I Regulation and appear to be embedded nowadays in data protection field.

1.5. Structure of work

The thesis consists of four main structural parts.

Chapter I "Introduction" introduces the topic to a reader and defines the problematic aspects that lack clarity. Also, it determines the limitations of the paper, explains the methods used in the research process and describes the structural components of the paper. Finally, in extra paragraph, it prepares reader for the main part of work by presenting the key notions of the study.

The structure of thesis is conditional on the composition of the researched sections in Article 3 GDPR. Therefore, the pivot of work consists of just two but extensive chapters.

Chapter II "Applicability of the establishment principle (Article 3(1) GDPR)" examines what 'being established in the Union' means, provides conditions for the establishment test, determines how to ascertain the links between an EU establishment with its non-EU parent company, and considers various scenarios of applicability depending on the status of the operator.

Chapter III "Applicability of the targeting principle (Article 3(2) GDPR)" explains both subjective and objective constituents of the targeting criterion, specifies at what point in time data subjects are considered to be in the Union, provides conditions for the targeting test, and exemplifies which activities refer to offering of goods and services and which demonstrate monitoring of the data subjects' behaviour.

Chapter IV "Conclusions" answers the research question and summarises the findings and final observations.

1.6. The notions of a non-EU controller and a non-EU processor

For the purposes of this paper and before turning to the discussion on the matter which starts in the next chapter, it is utterly important to define who (or what) a non-EU controller and a non-EU processor stand for. This will allow setting the limits of the paper and distinguishing the non-EU controllers and processors from the EU ones.

The GDPR does not provide for the definitions of either a non-EU controller or a non-EU processor. Nevertheless, these notions are implicitly presented in the text of the Regulation in a somewhat different way – "a controller or a processor *not established in*

the Union"[5] (emphasis added). Even though it seems obvious from the above that a non-EU controller is a controller not established in the Union, and a non-EU processor is, accordingly, a processor not established in the Union, however, this needs to be further clarified.

The GDPR is *the European Union regulation* which means that it is binding and directly applicable in all 27 Member States of the EU[6]. Also, starting since 20 July 2018, it is a part of the national legal systems of Iceland, Liechtenstein and Norway[7] by virtue of the Agreement on the European Economic Area[8] which extended the EU's single market to the non-EU member parties. The respective decision to incorporate the GDPR into the EEA Agreement was adopted by the EEA Joint Committee[9]. Hence, the GDPR is applicable not only on the territory of the EU Member States, but also on the territory of three more EEA states, namely Iceland, Liechtenstein and Norway. Therefore, even though the GDPR refers to the Union and its Member States throughout the text, it is necessary to bear in mind that in most cases this should be interpreted as a reference to the EEA states as well[10].

Taking into consideration the aforesaid, it is not right to assert that a non-EU controller or processor is just the one which is not established in the EU. Thus, similarly to how the GDPR defines a 'controller' and a 'processor'[11], it is suggested to render non-EU controller as the natural or legal person, public authority, agency or other body *which is established in the state other than the EU Member State or the EEA state*[12], and which, alone or jointly with others, determines the purposes and means of the processing of personal data. By analogy, it is suggested to render non-EU processor as a natural or legal person, public authority, agency or other body *which is established in the state*

[5] *See* Recitals 23, 24, 25, 80, 122, Articles 3(2), 3(3), 27 GDPR

[6] Consolidated version of the Treaty on the Functioning of the European Union, 26 October 2012, 2012/C 326/01, Article 288

[7] The European Free Trade Association. General Data Protection Regulation (GDPR) entered into force in the EEA, 19 July 2018. Available at: <www.efta.int/EEA/news/General-Data-Protection-Regulation-GDPR-entered-force-EEA-509576>

[8] Agreement on the European Economic Area, 13 December 1993

[9] Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]

[10] Granmar, Claes G. Global applicability of the GDPR in context. Available at: <www.diva-portal.org/smash/get/diva2:1274839/FULLTEXT01.pdf>. 14 January 2019 – last updated, p. 3

[11] Article 4 (7, 8) GDPR

[12] It is not advisable to unite 'the EU Member State' and 'the EEA state' under the common denominator which is 'the EEA states', though all EU Member States are also the EEA states, since such formulation may run counter to the scope of the GDPR as *the EU regulation* in the first place, and it may clash with the wordings used in the Regulation in the second place.

other than the EU Member State or the EEA state[13], and which processes personal data on behalf of the controller. This way, it would be precisely ascertained that a non-EU controller or processor is the one established in any state, except the EU Member States and other three EEA states. Namely all those third states are covered by this paper.

To avoid confusion with the wordings in the GDPR and in this thesis, the terminology used in the paper will be the same as in the text of the GDPR, for instance, use of 'in the Union' and 'Member States' when referring to the EU. However, at all times, this will implicate additionally 'in Iceland, Liechtenstein and Norway'.

With respect to the UK and its recent withdrawal from the EU *(hereinafter – Brexit)* which took place on 31 January 2020, few points ought to be highlighted here. On the one hand, the GDPR is the EU regulation directly applicable to *Member States of the EU*, and since the UK has left the Union and, thus, lost the status of a Member State, so the Regulation should not apply to the UK anymore. If that was the case, this would allow rendering the UK as the third state right after Brexit. On the other hand, however, as the ICO stated, the GDPR will continue to apply to the UK till the end of the year 2020 which is conditional on the transition period[14]. This means that since the UK keeps on abiding the Regulation during the transition period, it has to be regarded as though it was a Member State. According to the ICO, when the transition period is over, the GDPR will discontinue applying to the UK[15]. There are opposite views as to what happens next: the ICO considers that the Regulation will be incorporated into the UK law as the so-called 'UK GDPR'[16]; however, Boris Johnson, the Prime Minister of the UK, alleges that the UK will "develop separate and independent policies" in various areas, including data protection[17]. In any case, even if the ICO is right and the GDPR will be incorporated into the UK legislation, this will not change the fact that the UK is the non-EU state. So, starting from 1 January 2021, it will be possible to affirmatively ascertain that the UK is the third state in relation to the EU. As it follows, all the respective findings of this paper will be applicable to the UK as well since the UK's controllers and processors will become the non-EU ones.

---

[13] *Ibid*

[14] The Information Commissioner's Office, Information rights and Brexit Frequently Asked Questions, 29 January 2020. Available at: <www.ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf>, p. 1

[15] *Ibid*, p. 2

[16] *Ibid*, p. 1

[17] Johnson, Boris, UK / EU relations: Written statement – HCWS86 of 3 February 2020. Available at: <www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2020-02-03/HCWS86/>

II. APPLICABILITY OF THE ESTABLISHMENT PRINCIPLE (ARTICLE 3(1) GDPR)

2.1. The establishment principle

The establishment principle is a starting point of determining whether a non-EU controller or processor is subject to the GDPR. Anticipating things, in case the establishment principle cannot be applied, the next step will be checking the applicability of the targeting principle[18].

According to the establishment principle, the choice of applicable law depends on the place where an entity is established[19]. It is stipulated in Article 3(1) on the territorial scope of the GDPR which states the following: *"This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."*[20] As it follows, the actual place of processing activities does not affect the applicability of the GDPR, – instead, the location of the establishment matters.

On the surface, it may seem that the provision has nothing to do with applicability to the non-EU based entities, and only the closing wording 'in the Union *or not*' indicates the extraterritorial effect. However, the case is somewhat different. Despite its vague formulation, the provision foresees a broad scope of possible subjects, including, but not limited to, the non-EU subjects, i. e., the non-EU controllers and processors. Notably, Article 3(1) GDPR in the first place is oriented towards the EU entities, and only after closer consideration it appears to be a comprehensive provision encompassing the EU based as well as the *non-EU based* entities.

In order to apply the establishment principle, it is necessary, first, to determine whether a non-EU controller or processor is established through an establishment in the Union, and, second, to check whether the personal data is processed in the context of the activities of the said EU establishment. So, following this order, the questions will be contemplated in detail hereinafter.

[18] *See* Chapter III. Applicability of the targeting principle (Article 3(2) GDPR)
[19] Voigt, Paul – von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer International Publishing AG, 2017, p. 24
[20] Article 3(1) GDPR

2.2. An establishment of a non-EU controller or processor in the Union

2.2.1. Types of connections between controllers, processors and their establishments

Before considering under what conditions a non-EU legal entity will have an establishment in the Union, it is necessary to inquire into theoretical part as to what kinds of connections may occur between establishments and their parent companies.

In general, a controller or a processor may have one, several or many establishments, or no establishment. To be more precise, in the latter case, both notions coincide since a company appears as an establishment in relation to itself. For the purposes of this chapter, only instances with at least two establishments are of interest – when one establishment is outside the EU and another one is within the EU.

The main company (more common 'parent company' or 'parent firm') is at the same time the 'main establishment' (or 'primary establishment'), while its subsidiary companies ('subsidiaries' or 'daughter companies') are 'secondary establishments' (or 'affiliated establishments'). So, in order to stipulate that a non-EU entity has an establishment in the Union, there has to be the following arrangement of facts: the main establishment is in the non-EU state, and the affiliated establishment is in the EU Member State. If, for instance, the situation is *vice versa*, i. e., the primary establishment is in the Union and the secondary establishment is in the third state, then the given example concerns the EU parent company which has an affiliated establishment in the third state. Of course, the GDPR applies to such situation, however, that is not covered by this paper.

A good example of the right arrangement of facts for the application of Article 3(1) GDPR can be found in the real case. On July 9 2019, the UK Information Commissioner's Office (ICO) announced about its intention to impose a fine in the amount of £99,200,396 against *Marriott International, Inc.* for violation of the GDPR[21]. The case concerned the cyber incident during which guest records related to residents of all EEA states were exposed[22]. Despite the fact that *Marriott International, Inc.* was headquartered in the United States, the said data breach fell under the GDPR since the

[21] The Information Commissioner's Office, Intention to fine Marriott International, Inc. more than £99 million under GDPR for data breach, 9 July 2019. Available at: <www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/>

[22] *Ibid*

company was established in the Union as well through its office in the UK[23] (at that time – the EU Member State). Therefore, the establishment principle applied.

An establishment of

Article 3(1) GDPR prescribes that an establishment concerned has to be an establishment *of* either a controller or a processor in the Union[24]. Granmar suggests interpreting the provision in question on the basis of its literal construction and therefore considers that, in the event of a non-EU entity, 'an establishment of' will be the non-EU controller's or processor's affiliated person in the Union[25]. Moreover, elaborating on this suggestion, the scholar states that if the processing is conducted in the context of the activities of an undertaking which belongs to the same group of undertakings as a non-EU entity, the GDPR will not apply since in this case the undertaking will not be considered the non-EU entity's establishment[26]. So, according to Granmar, 'an establishment of' should indicate the relationship of belonging to or possession of the non-EU entity.

However, such a literal construction is too narrow and does not reflect the real meaning of the provision. As it is shown hereinafter in paragraph 2.5.4 of the paper, under certain circumstances, a processor in the EU may be regarded as an establishment of a non-EU controller. That is to say, despite the fact that there are two separate entities in question, the establishment of one company may be considered as an establishment of another. Thus, 'an establishment of' indicates rather a certain *connection* between two parties than the fact of belonging one to another.

2.2.2. The concept of establishment

Indubitably, 'establishment' is a central notion in the whole Article 3 GDPR since it defines the scope of territorial approach of the Regulation. Despite the notion's significance, the GDPR does not provide for a definition of 'establishment' specifically for the goals of Article 3 GDPR and, moreover, does not include it into the 'Definitions' section, however, places it into recitals in the preamble to the GDPR. On the one hand, such approach to composing a legislative act is not surprising since both the same definition and placement in the document were in the DPD, and the GDPR repeats its

[23] Marriott International headquarters and office locations. Available at: <www.craft.co/marriot-international/locations>
[24] Article 3(1) GDPR
[25] Granmar 2019, p. 27
[26] *Ibid*

predecessor in much. On the other hand, taking into consideration how much the legislator has enlarged the 'Definitions' section of the GDPR in comparison with the DPD, and how important the scope of establishment is for the application of the whole Regulation, it seems unreasonable to leave the definition of establishment in recitals again.

Though, here is how recital 22 in the preamble to the GDPR construes it: *"[e]stablishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."*[27] That is to say, a non-EU controller or processor will be considered to have an establishment in the Union, if it exercises on the territory of the Union an effective and real activity through stable arrangements, regardless of its legal form. Supposedly, all the mentioned conditions are met, and a non-EU controller or processor has an establishment in the Union, in that case, as a general rule, it will be pursued under Article 3(1) GDPR.

The CJEU in its judgments has helpfully interpreted the notion of 'establishment' within the meaning of EU data protection law. This is particularly important since not every notion of 'establishment' can be applicable here due to being different in other branches of law (for instance, company law), or in standard practice when a company is established there where it is physically headquartered[28]. Nevertheless, it should be observed that the notion of 'establishment' within the meaning of EU data protection law originates from the general definition of 'establishment' and has adopted "stable and continuous basis" of activity[29] from it.

The case law of the CJEU on the aforesaid matter is based on the interpretations of the DPD, thus, can be applied to the GDPR respectively. For instance, in *Weltimmo case*, the Court concluded that the concept of establishment is flexible and must be interpreted apart from a formalistic approach, according to which entities are considered to be established only in the place of registration[30]. Indeed, in a modern information world, such formalities as registration of a branch play minor role; on the contrary, the real

[27] Recital 22 GDPR

[28] Meisinger, Jeremy, Weltimmo v. Hungarian Data Protection Authority: EU Rules on What It Means To Be "Established" in a Jurisdiction, 2 December 2015. Available at: <www.securityprivacyandthelaw.com/2015/12/weltimmo-v-hungarian-data-protection-authority-eu-rules-on-what-it-means-to-be-established-in-a-jurisdiction/>

[29] CJEU, Case C-55/94, Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano, 30 November 1995, para 25

[30] CJEU, Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, 1 October 2015, para 29

activities of a branch and their factual effects matter. Thus, lack of a registered office in the Union does not preclude a non-EU entity from having an establishment there within the meaning of EU data protection law. Upon reversion, the place of registration does not necessarily mean the same as the place of establishment, though usually serves an indicator for an establishment[31]. For example, in *Weltimmo case*, the company was registered in Slovakia, however, the Court ruled that it was actually established in Hungary due to conducting business activities there[32]. Thus, it is possible that a non-EU company can have a formally registered branch in the Union, however, that branch will not be considered an establishment within the meaning of EU data protection law. All the above illustrated mismatches happen due to the prevailing role of the real activities (will be discussed in paragraph 2.2.5 of the paper further) which exactly determine the establishment.

While the CJEU has fixed that the notion of 'establishment' is broad[33] and flexible[34], and in every case it adheres to this opinion by means of providing more and more all-embracing meaning of the notion, the EDPB warns that interpretation of 'establishment' cannot be boundless[35]. For instance, a non-EU entity cannot be admitted to have an establishment in the Union based solely on the fact that its website can be accessed from one of the Member States[36]. Indeed, accessibility of the website is just an attainment of the digital age – everyone who has access to the Internet can normally reach any web-page (with the exception of some restrictions). Quite another situation will be if a non-EU entity purposefully targets the EU data subjects through its website[37], – then the accessibility of the latter has to be evaluated in connection with other facts of the case. However, in any event, mere accessibility of the website from the Union cannot lead to an establishment *per se*.

2.2.3. The establishment test

In order to determine whether a non-EU controller or processor has an establishment in the Union, it is necessary to apply the establishment criteria, i. e., the stability of the arrangements and the real and effective exercise of activities in the Union[38].

[31] Voigt – von dem Bussche 2017, p. 24
[32] Weltimmo case, paras 9, 33
[33] Gebhard case, para 25
[34] Weltimmo case, para 29
[35] EDPB Guidelines, p. 7
[36] CJEU, Case C-191/15, Verein für Konsumenteninformation v Amazon EU Sàrl, 28 July 2016, para 76
[37] *See* Chapter III. Applicability of the targeting principle (Article 3(2) GDPR)
[38] Weltimmo case, para 29

Additionally, as Advocate General Villalón noted in his Opinion in *Weltimmo case*, and later it was supported by the Court, the establishment criteria "must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned"[39], especially when the entity in question provides services only on the Internet[40]. Thus, the establishment test offered by the Court consists of the following steps:

1) determining whether an activity is executed through stable arrangements;
2) determining whether the activity is real and effective;
3) evaluating the activity in the light of its nature and the services provided.

It is worth noting that in its Guidelines on the territorial scope of the GDPR, the EDPB emphasizes on the need to determine an establishment in the Union on a case-by-case basis and to take into consideration the specific facts of the case[41]. Such a vague in its wording advice, on the one hand, does not provide for the concrete guidance, however, on the other hand, leaves room for analysis and warns that there are no straightforward answers yet.

Nevertheless, this paper will follow the existing establishment test as it is. So, when all three steps are done, questions are answered in the affirmative and the specific details of the case are taken into account, then it is possible to consider that a non-EU controller or processor has an establishment in the Union. The above specified steps are examined in the next paragraphs.

2.2.4. Stable arrangements

In an establishment, activities are carried out through stable arrangements. The legal form of arrangements is not decisive in respect to the application of the establishment criteria[42], – the legislator stipulates that directly and defines *stability* as a determinant factor instead. In essence, whatever to call a non-EU entity's establishment on the territory of the Union, – whether a branch, an office or a subsidiary, – it will, in any case, *represent* its non-EU parent company in the Union, and, in that sense, this is enough to show a link between the establishment in the Union and the non-EU parent company. It is important to note that an establishment does not necessarily need to have

[39] Opinion of Advocate General Cruz Villalón, delivered on 25 June 2015, Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, para 32
[40] Weltimmo case, para 29
[41] EDPB Guidelines, p. 7
[42] Recital 22 GDPR

a legal personality[43], which allows applying the broad concept of establishment – the non-formalistic one.

Supposedly, a non-EU controller or processor decided not to have an establishment in the Union in order to avoid applicability of the GDPR to its processing activities, – it simply does not establish a branch nor a subsidiary company in any of the Member States and believes that this way it is not pursued under the GDPR. However, lack of a formally established, i. e., registered, arrangement, as shown in paragraph 2.2.2 of the paper hereinbefore, does not exclude the existence of an establishment in the Union in terms of EU data protection law[44]. Moreover, whether a non-EU entity considers itself being established within the Union or not, is not decisive in that respect.

Quite another situation would be if a non-EU entity *indeed* does not have *any* stable arrangement or representation in the Union, – neither registered, nor factual, – that potentially could be considered as its establishment. In such case, there would be no grounds for the application of establishment principle.

Notably, an employee or an agent of a non-EU entity does not necessarily have to originate from the third state where the main establishment is in order to be considered its establishment in the Union; rather, it can be any resident or company from the Union which was hired specifically for the purposes of the non-EU main establishment. For instance, this will be the case when, as shown hereinafter in paragraph 2.5.4 of the paper, an EU-based processor may be considered as an establishment of a non-EU controller in the Union. Furthermore, even having an appointed consultant in the Union may lead to a full-fledged establishment there with all respectful consequences[45].

Stability of the arrangements

Arrangements must be stable – that is what the legislator alleges, however, how to measure stability remains unclear. Some guidance on this issue is found in *Gebhard case*, in which the Court ruled that the activity has to be evaluated in the light of, first of all, its duration and, second, with regard to "its regularity, periodicity and continuity"[46]. According to Villalón, the key feature of the stable arrangements is "a factor of

[43] WP29, Opinion 8/2010 on applicable law, 0836-02/10/EN WP 179, adopted on 16 December 2010, p. 11
[44] EDPB Guidelines, pp. 6-7
[45] Granmar 2019, p. 33
[46] Gebhard case, para 27

permanence"[47]. Therefore, putting altogether the listed interpretations, it is possible to infer that the regular activities performed through the arrangements on a continuous and permanent basis, without specified time frame, confirm the stability of arrangements. By contrast, limited period of performance indicates rather a service than a stable activity[48].

As Korff rightly observed, "a travelling person is unlikely to constitute an "establishment""[49]. This example pictures to oneself an agent of a foreign company who travels around the EU in InterCity trains and advertises to passengers some goods or services that his or her company provides and, at the same time, the agent collects the contact details of the passengers in order to monthly send them the company's newsletters. It is not that a person cannot be considered an establishment, – on the contrary, this is quite possible. However, the problem with a travelling agent lays in arrangement being not stable *a priori*, at least on the basis that it does not have a fixed location.

Regarding the degree of stability, it has to be estimated, first, in view of the nature of an arrangement's economic activities and, second, the services provided by that arrangement[50]. Voigt has provided an example showing that when a non-EU entity's office in the Union "develops customer relationships", it is deemed to have "a considerable degree of stability that qualifies the office as 'establishment'"[51]. Why in the exemplified instance the activity was understood to have a *considerable* degree of stability, remains unclear, though. The problem is that there is no unambiguous answer regarding under what circumstances certain activities are stable enough and on which conditions they are insufficient. The EDPB seems to ensure oneself against any risks and did not take care of drawing a borderline between 'sufficient' and 'insufficient' stability. Probably, the reason for that is, broadly speaking, that stability is always relative: what is sufficiently stable in one case, might be not stable enough to be rendered establishment in another. Until there is the case law with striking examples which clearly illustrate when stability is rendered 'sufficient' or 'insufficient', its real

[47] Opinion of Advocate General Villalón, para 28
[48] This indirect conclusion is inferred on the basis of: CJEU, Case 196/87, Udo Steymann v Staatssecretaris van Justitie, 5 October 1988, paras 6(1), 16
[49] Korff, Douwe, The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service, 19 August 2019). Available at SSRN: <www.ssrn.com/abstract=3439293>, p. 6
[50] Weltimmo case, para 29
[51] Voigt – von dem Bussche 2017, p. 25

meaning will remain a riddle. So, for the time being, there is no other better guidance than that the degree of stability always has to be evaluated on a case-by-case basis.

Returning to the nature of activities, they can, roughly speaking, be divided into offline and online activities. For both types, the activity must contribute to the data processing. In case of the offline activities, everything is more or less clear since the existence of an arrangement is *real* and obvious: usually, there is a physical location of an establishment through an office or a branch, a post address, the representatives and so forth. The situation is different when online activities are in question. Then a 'burden of proof' depends on the circumstances of the case, and, as stated hereinbefore, there is no clear algorithm for determining the degree of stability.

Provision of services online

The EDPB has extended the concept of establishment for online organisations even further in comparison with the existing case law on the matter by stating that when it comes to such an activity as the provision of services online, "the threshold for "stable arrangement" can actually be quite low"[52]. Providing services over the Internet excepts some features attributable to an establishment in its typical image, for instance, real estate, infrastructure, assets, representatives etc. – some of them can be missing since they do not have an influence on the effective provision of services online.

The Article 29 Data Protection Working Party *(hereinafter – WP29)* considers the definition of 'established service provider' relevant for the purposes of data protection law[53]. Thus, according to recital 19 in the preamble to Directive on electronic commerce, "the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place *where it pursues its economic activity*"[54] (emphasis added). Basically, this means that if an arrangement of a non-EU controller or processor offers services exclusively on the Internet and it offers or administrates its services in the Union, the arrangement can amount to an

[52] EDPB Guidelines, p. 6

[53] WP29, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final, WP 56, adopted on 30 May 2002, p. 8

[54] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Recital 19

'establishment'[55]. In support of the above specified definition, the WP29 clarifies that the fact of using the web servers located in place 'A' does not change the fact that a company is still established in place 'B' where it conducts the activities or where it is registered[56]. Furthermore, as already discussed hereinabove, a non-EU controller or processor cannot be considered to have an establishment in the Union merely in terms of the fact that its website is accessible from one of the Member States[57]. Therefore, indeed, the place where a non-EU company providing services via the Internet pursues its economic activities will define its stable arrangements there and, thus, the establishment.

On 21 January 2019, the Restricted Committee of the CNIL (Commission Nationale de l'Informatique et des Libertés – the French Data Protection Authority) issued the heaviest GDPR sanction so far – a 50 million euros fine against *Google LLC* for violating the GDPR, notably, for lack of transparency, information and effective consent[58]. According to the facts of the case, *Google LLC* is a company with a registered office in the United States, and one of its subsidiaries is based in France – *Google France SARL*[59]. Thus, the latter appears as the establishment of the *Google LLC* in the Union. Formally, that is so, however, as specified above, the company providing services over the Internet is established there where it pursues economic activity. In this context, it is worth mentioning that *Google* has developed, *inter alia*, the operating system for Android mobile terminals which numbered 27 million users in France[60]. This allows the conclusion that *Google* pursued economic activities through its French subsidiary, therefore, the given fact defines France as the place of establishment of the *Google's* EU subsidiary.

Another striking example concerns a series of complaints filed against big corporations that provide streaming services, four of which are headquartered in the United States. They are *Amazon*, *Apple*, *Netflix* and *YouTube*. The said complaints were filed on 18

[55] Kartheuser, Ingemar – Schmitt, Florian, Der Niederlassungsbegriff und seine praktischen Auswirkungen. Anwendbarkeit des Datenschutzrechtes eines Mitgliedstaats auf ausländische EU-Gesellschaften. 6(4) Zeitschrift für Datenschutz (2016), 155-159, pp. 155, 158 in: Voigt – von dem Bussche 2017, p. 24

[56] WP29, Working document on processing on the Internet by non-EU based web sites, p. 8

[57] Verein für Konsumenteninformation case, para 76

[58] The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019. Available at: <www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>

[59] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC. Available at: <www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>, paras 1, 2

[60] *Ibid*, paras 3, 4

January 2019 by *noyb* ("none of your business") – a European non-profit organisation for privacy enforcement[61]. It accused the said companies of violation of the right of access guaranteed by the GDPR. So far as the streaming companies have the European subsidiaries in the Member States – *Amazon* in Luxembourg[62], *Apple* in the Republic of Ireland[63], *Netflix* in the Netherlands[64] and *YouTube* in Austria[65] (due to *Google LLC* being *YouTube's* parent company) – the complaints were submitted against the respectful European establishments. Even though the complaints are currently under investigation, there is no doubt that the said companies administrate the services of their US parent companies in the Union and therefore are established in the EU within data protection law. Thereby this makes filing of the complaints against them possible under the GDPR.

It would be unreasonable with respect to the provision of services online not to contemplate the issue of whether a website would qualify as a stable arrangement[66]. So, to answer this question, it is necessary again to appeal to the Directive on electronic commerce. It directly stipulates that "[t]he presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider"[67]. As it follows, even though being to some extent relevant to the technological constituent of a service provider, a website itself cannot be considered as the stable arrangements. Moreover, as it was noted above, the place of establishment of a service provider "is not the place at which the technology supporting its website is located"[68]. Putting Ustaran's observation into the context of the paper[69], it is possible to infer that a non-EU entity with a website in the Union, however, pursuing its economic activity in, e. g., Belarus, will not be pursued under the GDPR since it will not be established in the Union within the meaning of data protection law.

---

[61] Netflix, Spotify & YouTube: Eight Strategic Complaints filed on "Right to Access", 18 January 2019. Available at: <www.noyb.eu/access_streaming/>

[62] Complaint under Article 77(1) GDPR, noyb Case Nr: C-16/18, 18 January 2019. Available at: <www.noyb.eu/wp-content/uploads/2019/01/Amazon_Complaint_geschw%C3%A4rzt.pdf>

[63] Complaint under Article 77(1) GDPR, noyb Case Nr: C-17/18, 18 January 2019. Available at: <www.noyb.eu/wp-content/uploads/2019/01/AppleMusic_Complaint_geschw%C3%A4rzt.pdf>

[64] Complaint under Article 77(1) GDPR, noyb Case Nr: C-07/18, 18 January 2019. Available at: <www.noyb.eu/wp-content/uploads/2019/01/Netflix_Complaint_geschw%C3%A4rzt.pdf>

[65] Complaint under Article 77(1) GDPR, noyb Case Nr: C-14/18, 18 January 2019. Available at: <www.noyb.eu/wp-content/uploads/2019/01/YouTube_Complaint_geschw%C3%A4rzt.pdf>

[66] Ustaran, Eduardo, *The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach* in: Ismail, Noriswadi – Yong Cieh, Edwin Lee (eds.), *Beyond Data Protection. Strategic Case Studies and Practical Guidance*. Springer-Verlag Berlin Heidelberg, 2013, 135-156, p. 142

[67] Directive on electronic commerce, Article 2(c)

[68] *Ibid*, Recital 19

[69] Ustaran 2013, p. 143

Bygrave confirmed the view that a website is unlikely to qualify a stable arrangement, nevertheless, as the scholar noted, it would be quite possible to prove the execution of real and effective activities of an establishment by means of a website, if the latter is interactive[70]. This way, it is clear that a website as such has a dual nature – on the one hand, it cannot be singled out as a separate stable arrangement, however, on the other hand, an establishment becomes established *through* the mentioned website. The logic behind this is comprehensible, i. e., why a website cannot be considered as a stable arrangement as such. However, the whole confusion sits uncomfortably with the concept of establishment.

Some light on the stated issue was cast by Granmar. He has defined the situation which occurred in *Weltimmo case* as the recognition of "a composite establishment consisting of the online presence […] and a stable offline arrangement through an appointed representative"[71]. Thus, in this example, the website was considered the argument of *Weltimmo* pursuing economic activities in Hungary. However, only the representative qualified to a stable arrangement.

Through stable arrangements

It is worth noting that the wording '*through* stable arrangements' was framed so not without purpose. Basically, it stipulates that a non-EU controller or processor is established in the Union *by the use of* its stable arrangements and exercises activity there also *by the use of* its stable arrangements. So, stable arrangements appear as *the means*. Of course, they can have a legal form of a branch, a subsidiary etc. However, if that branch or subsidiary does not serve as the means (e. g., appears as a controlled undertaking, instead) for the non-EU parent company for the purpose of fulfilling the above mentioned tasks, or, moreover, if it does not contribute to the processing of personal data, then it will not be considered an establishment in the Union, at least within the meaning of data protection law. Therefore, 'to be established in the Union through stable arrangements' and 'to have a controlled undertaking in the Union' is not the same[72].

[70] Bygrave, Lee A. Determining Applicable Law pursuant to European Data Protection Legislation. Computer Law & Security Report, Vol. 16 (2000), 252–257, sec. 4, p. 9
[71] Granmar 2019, p. 31
[72] *Ibid*

Human and material resources

In the case law of the CJEU, there was repeatedly confirmed[73] that a stable arrangement envisages that "both the human and technical resources necessary for the provision of the services are permanently present"[74]. Now, when a non-formalistic approach of determining the place of establishment is admitted as a guiding star, the human and technical resources go yet a greater way.

The WP29 has provided felicitous practical examples of resources that can constitute stable arrangements. It has given an opinion that when effective and real activities take place in an office, the latter will be deemed material resource through which the establishment operates. Even in case of a one-person office, it will still qualify as a resource since the office is "actively involved in the activities in the context of which the processing of personal data takes place"; and such involvement goes beyond just a representative function.[75] It is right that quantitative aspects, such as how many employees are appointed to an EU establishment, do not affect applicability of the establishment principle.

As for other material resources, the WP29 has clarified that a server or a computer cannot be considered as an establishment, arguing that they are just instruments for data processing[76]. They are. However, Advocate General Villalón thinks somewhat differently about that. He states that "[i]n some circumstances, an agent who is permanently present, equipped with little more than a laptop computer", can be deemed acting with a sufficient degree of stability[77]. Admittedly, by stating that, he meant a person whose equipment and probably software go beyond an average user's computer. On condition that a computer is not the only resource being assessed in the context of availability of stable arrangements, it is possible to infer that a computer (or any other data processing equipment) can actually lead to a stable arrangement. The essential takeaway here is that there must be a combination of *both* human and material resources presented – the computer needs to be operated by someone. Regarding the abovementioned 'some circumstances', Villalón emphasizes that, when evaluating

[73] *See*, e. g., CJEU, Case C-390/96, Lease Plan Luxembourg SA v Belgian State, 7 May 1998, para 24; CJEU, Case C-73/06, Planzer Luxembourg Sàrl v Bundeszentralamt für Steuern, 28 June 2007, para 54; CJEU, Case C-605/12, Welmory sp. z o.o. v Dyrektor Izby Skarbowej w Gdańsku, 16 October 2014, para 58

[74] CJEU, Case 168/84, Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt, 4 July 1985, para 18

[75] WP29, Opinion 8/2010 on applicable law, pp. 11-12

[76] *Ibid*, p. 12

[77] Opinion of Advocate General Villalón, para 34

human and technical resources, it is necessary to consider peculiarities of legal entities offering services on the Internet and undertake *in concreto* analysis of each situation.[78]

Besides technical resources which are directly involved in the processing activities of personal data, there are some other examples of material resources found in the case law. For instance, in *Weltimmo case*, a letter box and a bank account in Hungary were, indubitably, regarded as the material resources, even though the Court did not state that directly[79]. Together with the legal representative who was the human resource, the letter box and the bank account constituted the stable arrangements of *Weltimmo* in Hungary and, thus, the establishment there.

Representative as a stable arrangement

As shown above, a representative should be qualified as the human resources. Developing this consideration, the WP29 has specified that "even a simple agent may be considered as a relevant establishment if his presence in the Member State presents sufficient stability"[80]. That is to say, the actual position in the company of a representative is not decisive – the idea is that such a person has to *represent* the non-EU controller or processor in the EU. Villalón supported the statement and added that a sole agent's stability has to be assured by "the presence of the human and technical resources necessary for the provision of the specific services concerned"[81]. This way, it is once again confirmed the unity of the human and material (technical) resources required for the ascertainment of stable arrangements.

The dual meaning of a 'representative'

There is an issue with the dual meaning of a 'representative' in the context of interpretation of the Regulation. The difference is considerable for the right applicability of the GDPR. That is why it will be contemplated here in detail.

According to the meaning introduced in the Regulation, 'representative' is a natural or legal person established in the Union and designated by the non-EU controller or processor in writing[82] in cases specified in Article 3(2) GDPR[83], i. e., targeting or

[78] Opinion of Advocate General Villalón, para 34
[79] Weltimmo case, para 33
[80] WP29, Opinion 8/2010 on applicable law, p. 12
[81] Opinion of Advocate General Villalón, para 42
[82] Article 4(17) GDPR
[83] Article 27(1) GDPR

monitoring of data subjects in the Union. So, this kind of a 'representative' is a specially appointed one in the precisely defined by the GDPR cases.

The other 'representative' is, roughly speaking, a *factual* representative that does not necessarily have to be designated in writing, and such a person is a representative by virtue of executed duties. The person in question may be an agent of the non-EU entity, its employee, consultant etc., who *de facto*, *inter alia*, *represents* the non-EU controller or processor on the territory of the EU. That was the case in *Weltimmo*, where the representative Mr Benkö served as a point of contact between the data subjects and the company, as well as he represented the company in the judicial and administrative proceedings[84]. The CJEU found those facts the satisfactory evidence and ruled that even the presence of one representative may be sufficient to form a stable arrangement[85]. The EDPB confirmed this, observing that the availability of at least one employee or agent of the non-EU controller or processor in the Union may be equated to a stable arrangement on condition that there is a "sufficient degree of stability" in that employee's or agent's actions[86]. Hence, a representative may lead to a stable arrangement and, thus, to an establishment of the non-EU entity.

Following the logic, the representative within the meaning of Article 4(17) GDPR might constitute a stable arrangement as well. Gömann claims that the requirement to appoint a representative, in accordance with Article 27 GDPR, might lead to a stable arrangement, which, in turn, would trigger the establishment clause of Article 3(1) GDPR so that the latter would be "likely to even absorb the remaining field of application of the two alternatives posed under Article 3(2)"[87]. However, that is not the case.

Anticipating the forthcoming issues with wrong interpretation and, thus, application of the concept of representative, the EDPB warned that a representative designated pursuant to Article 27 GDPR "does not constitute an "establishment" of a controller or processor *by virtue of article 3(1)*"[88] (emphasis added). In practice, this means that the presence in the Union of a representative appointed on the basis of Article 27 GDPR cannot be used in proving the existence of a stable arrangement and, consequently, an

[84] Weltimmo case, para 33
[85] *Ibid*, para 30
[86] EDPB Guidelines, p. 6
[87] Gömann, Merlin, The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement. Common Market Law Review, Vol. 54 (2017), 567-590, p. 575
[88] EDPB Guidelines, p. 23

EU establishment of the non-EU controller or processor. The reason is obvious: if it could be used so, then there would be a great deal of confusion since every time when a representative would be designated by virtue of Article 27 GDPR, this would lead to an establishment in the EU and, hence, to the application of Article 3(1) GDPR instead of Article 3(2) GDPR, which, in turn, would make the existence of the latter pointless.

2.2.5. The effective and real exercise of activity

The CJEU has ruled that the notion of 'establishment' "extends to any *real and effective activity* – even a minimal one – exercised through stable arrangements"[89] (emphasis added). It came to such a conclusion in *Weltimmo case*, which dealt, in particular, with determining the meaning of 'establishment'. Many facts of the case allow ascertaining what kinds of activities may speak in favour of the real and effective activities, in other words, which facts may prove the affirmative of an establishment. Of course, the case does not cover all possible scenarios that may occur, however, provides a useful interpretation of the concept of establishment in practice. Since the case abounds in important and influencing details, it will be closely contemplated here.

In the case, *Weltimmo s. r. o.* was a company registered in Slovakia, thus, it was established there within the meaning of company law, however, as shown hereinbefore, this is not the same as to be established within the meaning of data protection law. Despite having a registered office in Slovakia, *Weltimmo* did not conduct any activities there – it ran a business only in Hungary. The fact that the company had never engaged in business activities in the place of registration may indicate that it was *ab origin* set up to run a business in another state[90]. Probably, that was the case in *Weltimmo*, nevertheless, the motives are not decisive here. Thus, being a Slovak company registered in Slovakia within the meaning of company law was, in fact, the only connecting link between *Weltimmo* and Slovakia.

The rest of the facts confirm *Weltimmo's* strong ties with Hungary. Firstly, as mentioned above, *Weltimmo* ran its business in Hungary, i. e., the activities took place there, not in Slovakia. Secondly, the company executed the activities through the websites which dealt exclusively with Hungarian properties. That is to say, activities were expressly oriented to the Hungarian market. The company conducted processing of personal data relating to the property's owners and published such data on its websites

[89] Weltimmo case, para 31
[90] Svantesson 2019, p. 7

in the form of advertisements. The latter were subject to fees after one month of publication. The language of the websites was Hungarian which indicates that the service addressed the customers in Hungary. The facts of the case do not provide the information about the extension of the domain names used for *Weltimmo's* websites to run. This could serve as one more link either to the activities in Hungary, if an extension was ".hu", or to the activities in Slovakia, if it was ".sk". At any rate, the language of the website is a more important determinant, and in the analysed case it was Hungarian. Thirdly, one of the owners of *Weltimmo* resided in Hungary and was at the same time the company's representative on the territory of Hungary. The representative served as a contact point between *Weltimmo* and customers, administered recovering debts from clients and introduced the company in the legal matters, in other words, fulfilled all range of functions that representatives normally do. Also, the representative had an address in Hungary, as the register of companies proved. Fourthly, *Weltimmo* had a post box in Hungary for company's business purposes and opened a bank account for managing debts collection. Such a customer-oriented approach is an additional evidence that *Weltimmo*, bag and baggage, functioned in Hungary.[91]

It follows from all the aforesaid that *Weltimmo* had a comparatively weak connection with Slovakia and, by contrast, conducted its activities in Hungary. The CJEU singled out particularly few arguments as the weightiest ones: running the property dealing websites regarding properties in Hungary, the use of Hungarian as the language of the websites and fees applicable to advertisements after one month[92]. The Court concluded that the named factors constituted the effectiveness and real exercise of activities by *Weltimmo*, so far as the activities were "mainly or entirely directed" at Hungary[93]. The point is that in order to be considered real and effective, the activities must contribute to data processing and occur in the place of stable arrangements (in this case, in Hungary) so that altogether to constitute an establishment there. The same rule applies to the establishments in the Union of the non-EU entities.

Granmar noted that the "Court seems to suggest that all kinds of economic activities in relation to a business constitute a "real and effective activity" of a controller running a website"[94]. It is difficult to say, how the Court would rule, if there were another circumstances of the case. Most likely, practically any kind of activities exercised in an

[91] Weltimmo case, paras 13, 16, 33
[92] *Ibid*, para 32
[93] *Ibid*, paras 41, 66(1)
[94] Granmar 2019, p. 31

establishment may be considered as related to the activities of the parent company, especially when a local establishment serves as a link between the customers, i. e., data subjects, and the main establishment – the data controller.

Notably, the threshold for activity can be quite low. The wording "even a minimal one" allows admitting that the mere running of the website in the context of the activities of an establishment, as that was the case in *Weltimmo*, may suffice to conclude effectiveness and real exercise of activities. There are no limitations as to what can assert the real and effective activity of an establishment. Generally speaking, it can be everything which either confirms or refutes the existence of certain facts. In that respect, *Weltimmo* is just an example of what circumstances of the case may be taken into consideration when ascertaining the existence of an establishment.

As Wisman has noted, obviously, the addressed population – people residing in Hungary – was decisive in the given example[95]. The formulation 'real and effective' itself provides for an activity that creates tangible consequences from a legal perspective, is capable of producing a result and changing the rights and obligations of subjects. So, in order to be real and effective, the activity needs to influence the legal reality and to have an object, for instance, in the case in point, the Hungarian population.

With respect to a representative, a post box and a bank account in Hungary, they were, indubitably, regarded as the affirmative of stable arrangements in Hungary, even though the Court did not state that directly. In a stable arrangement, they appear as the resources: a representative is a human resource and a post box and a bank account are material resources of an entity. The named examples of stable arrangements cannot be used separately in confirmation of real and effective exercise of activities since they are not actions as such, though are always in a close connection with the latter ones; they are instruments by means of which the activities become real and effective. For example, a bank account itself does not create any legal consequences, however, when it is used as an instrument for recovering debts from customers, the bank operations occur. The same logic applies to having a representative, a post box etc. – they may serve as the means of activities only when they are used in a respective way that makes activities happen.

[95] Wisman, Tijmen H. A. *Privacy, data protection and e-commerce* in: Lodder, Arno R. – Murray, Andrew D. (eds.), *EU Regulation of E-commerce: A Commentary*. Cheltenham: Edward Elgar Publishing, 2017, 349-382, p. 368

Advocate General Villalón noted in his Opinion that there are also other factors which may indicate the real and effective nature of the activities, namely, "the place from where the data was uploaded, the nationality of the data subjects, the place of residence of the owners of the undertaking responsible for the data processing, and the fact that the service provided by that data controller is directed at the territory of another Member State"[96]. However, the Court ruled clearly that the nationality of the data subjects is irrelevant[97], and the given principle was specified in the GDPR[98]. So, as a matter of fact, the nationality of the data subjects cannot be of consequence for the purposes of determining the real and effective activities and an establishment in whole. As regards the other listed probable factors, they truly may indicate the real and effective nature of the activities of a non-EU entity's establishment, if taken into account together with other circumstances of the case.

Granmar disagreed with the Court's judgment by arguing that since the legal representative "was not involved in the company's core business", and he "did not assist the Slovak client to provide online advertisements for real estate in Hungary", *Weltimmo* cannot be considered conducting the real and effective activity in Hungary through its representative[99]. There is some kernel of good sense in Granmar's argument. Assuming he meant that the representative fulfilled, though related, but not the same tasks, as the data controller in Slovakia, thus, representation 'through' could not occur. However, it seems unreasonable that the representative was supposed to exercise identical functions since his tasks were *ab origin* different from the data controller's ones. Moreover, the representative actually contributed to the activities of the data controller. The Court has established that the representative was "responsible for recovering the debts *resulting from that activity* and for representing the controller in the administrative and judicial proceedings *relating to the processing of the data concerned*"[100] (emphases added). So, undoubtedly, the activities exercised by the representative, in particular, contributed to the company's core business substantially enough to conclude that the real and effective activities were carried out in Hungary. The most important takeaway here is that the activities exercised in an establishment in the Union must be related to the data processing activities of the parent company. The

[96] Opinion of Advocate General Villalón, paras 42, 72(1)
[97] Weltimmo case, para 66(1)
[98] Recitals 2, 14 GDPR
[99] Granmar 2019, p. 31
[100] Weltimmo case, para 66(1)

issue of this relatedness is contemplated in more detail in section 2.3 of the paper hereinafter.

To sum up the outcome of *Weltimmo case* at this point, the Court established that *Weltimmo* executed the real and effective exercise of activities, and those activities were exercised by means of stable arrangements. Also, it took into account that the activities in question were conducted through the websites, thus, the entity provided services over the Internet. Finally, the Court came to a conclusion that overall this ascertains the existence of *Weltimmo's* establishment in Hungary within the meaning of data protection law[101]. This way, the Court demonstrated how the establishment test can be met and created the precedent for EU businesses, as well as non-EU businesses which process personal data.

2.3. Processing in the context of the activities of an EU establishment

2.3.1. Applicability of the concept of processing in the context of the activities of an EU establishment

When the establishment test is checked, and it is confirmed that a non-EU controller or processor has an establishment which exercises real and effective activity through stable arrangements in the Union, then it is possible to proceed to the next step – checking whether the personal data is processed *in the context of the activities of* the said EU establishment[102]. Thereby it will be determined whether Article 3(1) GDPR can be applied. Anticipating things, it is important to note that if a non-EU entity has an establishment in the Union, however, does not carry out processing in the context of the activities of that establishment, Article 3(1) GDPR will not apply to such processing[103].

According to recital 22 in the preamble to the GDPR, the Regulation applies to any processing that is performed in the context of the activities of the respective establishment[104]. The GDPR itself does not provide any clues as to how to define when the processing takes place 'in the context of' and not otherwise. In this respect, Jay suggests undertaking analysis of "the nature of the activities which are directed from the

[101] Weltimmo case, para 33
[102] EDPB Guidelines, p. 7
[103] *Ibid*, p. 11
[104] Recital 22 GDPR

establishment and the relationship of those activities with the relevant processing in question"[105].

A non-EU controller or processor will be subject to the GDPR every time when the processing is performed in the context of the activities of its respective establishments[106]. As Jay specified regarding particularly a controller, it will continue to be responsible "even if the actual processing is conducted by a processor and/or takes place elsewhere"[107]. On the surface, it may seem that a non-EU controller bears more responsibility than a processor, however, obviously, the aforementioned observation derives from the controlling and organizational nature of a controller and from the fact that a processor acts "on behalf of the controller"[108].

As it follows from the case law on the matter, the wording 'in the context of the activities of an establishment' cannot be construed restrictively[109]. Therefore, it is not possible to conclude that the concept at stake, for instance, equates to 'processing *within* the activities of an establishment'[110], or to apply it merely "to the specific business model of search engine operators"[111], as it was in *Google Spain case*. At the same time, it would be wrong to construe the concept too broadly and infer that any establishment in the Union, even the one having "the remotest links to the data processing activities" of a non-EU controller or processor, will invoke the application of Article 3(1) GDPR to that processing[112]. Elaborating on this statement, the EDPB reiterates the WP29[113] and clarifies that "some commercial activity" carried out by a non-EU controller or processor in the Union may be outside the scope of the processing of personal data by this entity[114]. Indeed, commercial activities do not necessarily embody data processing activities, which, in turn, means that those commercial activities are not done in the context of data processing. In such case, they cannot be deemed as covered by data

[105] Jay, Rosemary – Malcolm, William – Parry, Ellis et al., *Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition)*. London: Sweet & Maxwell, 2017, section 4-028
[106] EDPB Guidelines, p. 7
[107] Jay 2017, section 4-028
[108] Article 4 (7, 8) GDPR
[109] CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014, para 53; Weltimmo case, para 25
[110] Granmar 2019, p. 33
[111] WP29, Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, 176/16/EN WP 179 update, adopted on 16 December 2015, p. 5
[112] *Ibid*, p. 5; EDPB Guidelines, p. 7
[113] *Ibid*, p. 5
[114] EDPB Guidelines, pp. 7-8

protection law. Therefore, with respect to data processing activities, they should be considered separately from the commercial activities.

2.3.2. Role of an EU establishment in the data processing

The processing in the context of the activities of an EU establishment can, generally speaking, occur in two cases: first, if the relevant data processing is being done by the EU establishment itself, or, second, if "the establishment is otherwise 'inextricably linked'" to the personal data processing activities of the non-EU parent entity[115]. So, the applicability of the 'in the context of' criterion depends on the role which an EU establishment plays in the data processing.

In the first case, when an EU establishment carries out processing of personal data itself, it will be considered processing in the context of the activities of *that* EU establishment, i. e., in the context of its own activities. So, as this scenario would be rather simple, there is no need to go further into details.

As for the second case, when an EU establishment does not conduct processing itself, however, may be deemed being inextricably linked to the activities of the non-EU controller or processor in some other ways than processing, this example requires thorough analysis.

In Update of Opinion 8/2010 on applicable law, the WP29 alleged that if there is an inextricable link ascertained, "the EU law will apply to that processing by the non-EU entity, *whether or not* the EU establishment *plays a role* in the processing of data"[116] (emphasis added). So, on the basis of the lexical construction, the WP29 conceded that the EU establishment may not play a role in the data processing. It is worth mentioning that the Opinion was adopted after the judgment in *Google Spain case* and, thus, reflects the outcome of the case.

Resuming the judgment in *Google Spain case*, the EDPB noted that the EU law will apply to the inextricably linked activities of an EU establishment and its non-EU parent company "even if that local establishment *is not* actually *taking any role* in the data processing itself"[117] (emphasis added). As it follows, the EDPB took the same view as

[115] Korff 2019, p. 47
[116] WP29, Update of Opinion 8/2010 on applicable law, p. 5
[117] EDPB Guidelines, p. 8

the WP29 had done before and interpreted the function of the Spanish establishment as 'not taking any role in processing'.

Unlike quoted above data protection authorities, Advocate General Jääskinen deemed that the establishment, nevertheless, "*plays a relevant role* in the processing of personal data if it is linked to a service involved in selling targeted advertisement"[118] (emphasis added). As it follows, an establishment *has to play* a relevant role in processing, for all that. In confirmation of his words, Jääskinen made reference to the earlier adopted Opinion 1/2008 of the WP29.

In the mentioned Opinion 1/2008 on data protection issues related to search engines, the WP29 explained that 'in the context of the activities of an establishment' implies that the establishment has to "play a relevant role in the particular processing operation"[119]. It has also provided few felicitous examples which are put here with insignificant changes, however, without losing their sense. So, an establishment in the Union will be considered playing a relevant role in data processing, if it is, for instance, "responsible for relations with users of the search engine" in a particular EU state. In this case, the establishment is representing the interests of its parent company, therefore, such a role can be deemed considerable. Another example is about the EU establishment which observes the law enforcement requests prescribed by the EU data protection authorities. Why this will be the case is obvious – complying with the prescriptions will directly affect the non-EU parent company since the establishment in the Union is its subsidiary. One more instance contemplates a search engine provider that establishes an office in the Union which "is involved in the selling of targeted advertisements" to the residents of a particular Member State.[120] The said instance is, obviously, drawn from one of the *Google cases*, so it will be returned to further for closer analysis.

To sum up, taking into account the examples of when an establishment would 'play a role' and on the basis of what circumstances of the case the WP29 and the EDPB concluded that it may *not* play a role, it seems that the data protection authorities merely lost consistency in formulations since the examples do not contradict one another. Apparently, by stating that playing a role is not required, they actually meant that the processing does not necessarily have to be done by an establishment itself, though it

[118] Opinion of Advocate General Jääskinen, delivered on 25 June 2013, Case C-131/12, Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González, para 65
[119] WP29, Opinion 1/2008 on data protection issues related to search engines, 00737/EN, WP 148, adopted on 4 April 2008, p. 10
[120] *Ibid*

may be carried out so. Therefore, it is considered that *playing a relevant role* by the EU establishment in data processing carried out by a non-EU entity is actually *an essential requirement*, and it should be understood in a different way than 'to perform processing by the EU establishment itself'.

As already mentioned, it was established by Court in *Google Spain case* that the processing does not necessarily have to be done *by* the said establishment itself in order to be considered as carried out in the context of its activities[121], – or rather it *can* be done by, however, there is no such requirement. Granmar supported this view and turned attention to the other crucial point: if there is an establishment *'of'* the non-EU entity in the Union, then it does not matter for the applicability of the GDPR, whether the said establishment processes the data itself or it does not fulfil any processing activities[122]. Returning to *Google Spain case*, the Spanish establishment merely sold advertising space on the search engine, and it did not conduct any processing activities, – the latter were carried out by parent company Google Inc.[123] In *Weltimmo case*, the legal representative in Hungary executed various duties, however, publication of personal data on the website and invoicing were not among them[124]. Nevertheless, in both cases, the Court concluded that there occurred processing in the context of the activities of the establishment[125]. The reasons for that will be discussed further hereinafter.

Granmar passed an opinion that "it would be more convincing to apply the GDPR only when […] an establishment in the Union is *actually involved in the data processing*"[126]. It is difficult to disagree with scholar. Indeed, if an EU establishment would take part in factual processing, its activity would be less problematic from the perspective of proving its involvement and establishing all that relationship between the non-EU entity and the establishment. However, that is not typically the case, – usually, the EU establishments of the non-EU parent companies play a minor role and do not process data themselves, therefore, if not the 'in the context of' formula, it would be impossible to connect establishments in the Union with their parent companies and data processing standing behind them.

[121] Google Spain case, para 52
[122] Granmar 2019, p. 34
[123] Google Spain case, para 51
[124] Weltimmo case, paras 33, 35, 36
[125] Google Spain case, paras 55, 100(2); Weltimmo case, paras 38, 41, 66(1)
[126] Granmar 2019, p. 34

2.3.3. An inextricable link between the activities of an EU establishment and the data processing carried out by a non-EU controller or processor

Providing more specific guidance concerning the meaning of 'in the context of the activities of an EU establishment', the EDPB suggests following its recommendations. The first one envisages conducting analysis of the relationship between a non-EU controller or processor and its EU establishment, the second one – determining whether the latter is involved in revenue-raising in the Union[127]. What consolidates both criteria is that there has to be shown the existence of an inextricable link between the activities of an establishment in the Union and the data processing carried out by a non-EU entity. The listed criteria are discussed hereinafter.

a) the relationship between a non-EU controller or processor and its EU establishment

As stated above, even if a non-EU establishment does not process data itself, it still may be inextricably linked in some other way to the personal data processing activities of its non-EU parent entity. Admittedly, in general, the idea of the 'link' is not a novelty to the EU data protection law since 'in the context of the activities of an establishment' was presented in the DPD as well. However, the concept of the *inextricable* link is new to the EU data protection law – it was introduced in *Google Spain case*. Indubitably, the concept is going to be extensively used in the forthcoming cases, but so far as it was invoked first in *Google Spain case*, the latter will be contemplated closely as an example.

In *Google Spain case*, *Google's* establishment located in Spain did not conduct any processing activities[128]. It acted as a commercial agent for its parent company *Google Inc.* which was established in the United States. The Spanish establishment was intended to promote and facilitate the sale of advertising space, which was offered by the parent company, on the territory of Spain.[129] Taking into consideration the mentioned facts, the Court concluded that the activities of the Spanish establishment and the US parent company were inextricably linked. It argued that "the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable" and, in addition, the same engine served as the means of

[127] EDPB Guidelines, p. 8
[128] Google Spain case, para 62
[129] *Ibid*, paras 43, 55

carrying out the said activities[130]. Moreover, as the Court noted, the fact that the search results and the advertisements were displayed on the same page, was the absolute evidence of the link between the activities in question[131]. In fact, there occurred the interdependency which caused the inextricable link between the EU establishment and the non-EU parent company. As follows from the judgment, there has to be a connection between the economic activity of the EU establishment and the data processing carried out by the non-EU entity.

As the WP29 later clarified, it was found that the advertising activities performed by Spanish establishment were "linked to the business model of Google" since the advertising corresponded to the results which the search engine supplied[132]. If not the activities of *Google Spain*, which were relating to the advertising space, *Google Inc.* would gain less profits; conversely, if not the engine, the EU establishment would not be able to promote and sell the advertising space which, in turn, brings profit to *Google Inc.* and so forth. As Advocate General Jääskinen noted in his Opinion, the establishment appeared "as the bridge for the referencing service to the advertising market" in Spain[133]. Therefore, as shown, the activities between the Spanish establishment and the US company were indeed inextricably linked. This allowed the conclusion that the processing of data was conducted in the context of the commercial and advertising activities of the EU establishment on the territory of Spain[134].

The most important takeaway in the analyzed case is that even if an EU establishment does not carry out any data processing operations itself, its other activities can still trigger the applicability of Article 3(1) GDPR to the data processing on the basis of being otherwise inextricably linked to the data processing operations of the non-EU parent company.

A much alike example took place in a so-called *Facebook Fan Page case* in which the processing activities were carried out jointly by *Facebook Inc.* (a US-based parent company) and *Facebook Ireland* (based in the Republic of Ireland respectively). There was one more *Facebook* entity involved – *Facebook Germany* – an establishment that

[130] *Ibid*, para 56
[131] *Ibid*, para 57
[132] WP29, Update of Opinion 8/2010 on applicable law, p. 3
[133] Opinion of Advocate General Jääskinen, para 67
[134] Google Spain case, paras 57, 100(2)

was "responsible for the promotion and sale of advertising space"[135] activities which rendered *Facebook's* services at issue profitable. As Advocate General Bot noted, "the Facebook Group almost completely depends on the sale of advertising space"[136], therefore, the business success of *Facebook* depended much on the activities of German establishment. Taking the said facts into consideration, the CJEU held that the advertising activities of German establishment that brought income to *Facebook* and the data processing carried out jointly by *Facebook Inc.* and *Facebook Ireland* were inextricably linked[137].

As the WP29 noted, if it is established that "there is an inextricable link between the activities of an EU establishment and *the processing* of data carried out by a non-EU controller, EU law will apply to *that processing* by the non-EU entity"[138] (emphasis added). Korff deems that the italicized wordings 'the processing' and 'that processing' have to be interpreted "as referring to a specific processing operation"[139]. This is an utterly relevant observation since it allows to draw an important conclusion – when it is established that the processing is carried out in the context of the activities of the EU establishment, Article 3(1) GDPR will apply only to *that particular processing operation*, or, possibly, to the series of processing operations, if the inextricable link occurs in relation to all of them. In confirmation of his words, Korff adds that if it was not the case, the Court would have held that the EU data protection law applies to the processing with respect to "people using its [*Google's*] browser from outside the EU" as well, however, the Court ruled that the law applies only to the processing regarding users from Spain[140]. Indeed, the Court tried the case regarding particular processing operations, and therefore only *those* operations were taken into account when determining the existence of the establishment in Spain.

[135] Opinion of Advocate General Bot, delivered on 24 October 2017, Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the presence of Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht, para 94
[136] *Ibid*, ref. 63
[137] CJEU, Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein V Wirtschaftsakademie Schleswig-Holstein GmbH, interveners: Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht, 5 June 2018, para 60
[138] WP29, Update of Opinion 8/2010 on applicable law, p. 5
[139] Korff 2019, p. 8
[140] *Ibid*

b) an EU establishment involved in revenue-raising in the Union

Just the same as the inextricably linked activities discussed above, the 'revenue-raising in the Union' is a new concept to the EU data protection law, and it originates from the judgment in *Google Spain case*. In essence, it envisages that an EU establishment raises revenue in the EU, and *that* is sufficiently inextricably linked to the individuals in the Union and to the data processing conducted outside the EU by a non-EU entity so that potentially it may confirm that the processing is being done in the context of the activities of the EU establishment[141].

Returning to *Google Spain case*, the activities regarding promotion and selling of advertisements by the Spanish establishment were admitted by the Court as "the means of rendering the search engine at issue economically profitable"[142]. As it follows, the fact of making profit in the Union was considered sufficient to connect it with the data processing activities of *Google Inc.* so that to constitute inextricably linked activities.

As already mentioned hereinbefore, the search results and the advertisements were displayed on the same page[143]. On the basis of that fact, the WP29 emphasized that *Google's* activities were unseparable from the revenue raised from advertising[144], – that is what guided the Court in rendering its decision. Indeed, the word 'unseparable' is probably the most felicitous one to define what being 'inextricably linked' means.

As stated above, the revenue-raising by an EU establishment has to be inextricably linked to the *individuals in the Union* as well. Following the Opinion of Advocate General Jääskinen[145], the Court noted that one of the requirements of concluding that there takes place data processing in the context of the activities of an EU establishment is that the latter "orientates its activity towards the inhabitants of that Member State[146],,[147]. At some point, this has something in common with the targeting principle which is not applicable in the given case. However, actually, the 'link to the individuals in the Union' has to be construed as the confirmation of the real and effective exercise of activities (discussed in paragraph 2.2.5 of the paper hereinbefore). This seems to be

[141] EDPB Guidelines, p. 8
[142] Google Spain case, para 56
[143] *Ibid*, para 57
[144] WP29, Update of Opinion 8/2010 on applicable law, pp. 3-4
[145] Opinion of Advocate General Jääskinen, paras 68, 138(1)
[146] As for now, this should be interpreted broadly, that is to say, *in Google Spain case*, the Member State concerned was Spain, however, in the context of this paper it has to be read as 'the Union' meaning any Member State or the whole European Union.
[147] Google Spain case, para 100(2)

reasonable since all the elements of the establishment test are interconnected and, in fact, one and the same element can be used for the consideration of various steps of the establishment test.

There are certain activities of the EU establishments that will most likely fall under 'inextricable link' condition – in the first place, it is all kinds of activities that concern the EU sales offices, i. e., promotion or selling of advertising, marketing directing at the EU residents[148], commercial prospection[149] and so forth. Why namely those activities, is obvious, – they enable bringing profit to the parent companies established outside the Union.

2.4. Geographical location pursuant to Article 3(1) GDPR

Under Article 3(1) GDPR, as the EDPB rightly observed, the geographical location matters in respect of the place of establishment of a controller or a processor and their establishments, if any in the Union; by contrast, it is unimportant concerning the place of processing and the location of data subjects whose personal data is being processed[150]. It is necessary to discuss this closer in the context of the paper.

2.4.1. The place of establishment of a controller or a processor

In general, a controller or a processor, notably its primary establishment, can be established either in the Union, or in the third state. Since this paper deals only with the non-EU controllers and processors, the geographical location is, in this case, important in establishing that a non-EU entity has its main establishment outside the Union.

2.4.2. The place of a controller's or a processor's establishment, if any in the Union

Once it is concluded that a controller or a processor is established in the third state, then, for the purposes of Article 3(1) GDPR, it is necessary to check whether a non-EU entity has a business presence in the Union that can constitute an EU establishment. Thus, the geographical location matters also when determining the fact of a proper representation in the Union.

---

[148] Bird & Bird, Guide to the General Data Protection Regulation, May 2020 version, 26 May 2020 – last visited. Available at: <www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>, p. 7
[149] EDPB Guidelines, pp. 8-9
[150] *Ibid*, p. 10

2.4.3. The place of processing

It is directly stipulated in Article 3(1) GDPR that the Regulation applies "regardless of whether the processing takes place in the Union or not"[151]. That is to say, the GDPR will apply to the data processing irrespective of the *actual place of processing*, though, under the stipulation that all other conditions specified in Article 3(1) GDPR and contemplated hereinbefore are met. Therefore, even in case of the non-EU entities, it does not matter whether the processing occurs in the Union or in the third state. The really important thing is to prove that the processing takes place *in the context of the activities* of a non-EU establishment. So, as just shown, the place of processing does not affect the applicability of Article 3(1) GDPR.

2.4.4. The location of data subjects

The location of data subjects whose personal data is being processed is not important under the provision in question. Therefore, the data subjects can be either on the territory of a Member State or on the territory of any other third state. In the instance exemplified by the EDPB, the data subjects were located in three African states, and the processing of their data was carried out by the company established in France; since the location of data subjects does not matter, Article 3(1) GDPR would apply to such processing[152]. It is worth emphasizing that the location of data subjects is an unimportant feature in the cases where Article 3(1) GDPR applies. By contrast, the location of data subjects will be taken into account under conditions stipulated in Article 3(2) GDPR which will be discussed further.

2.5. Special cases of application of the establishment principle to the non-EU controllers and processors

2.5.1. Differentiated approach in the application of the establishment principle to the non-EU controllers and processors

The GDPR applies to both non-EU controllers and non-EU processors. However, the ascertained applicability of the Regulation, for instance, to the non-EU controller does not automatically invoke the applicability to the processor within the same processing operation, and *vice versa*. Therefore, the EDPB has laid stress on that and clarified in its Guidelines on the territorial scope of the GDPR.

[151] Article 3(1) GDPR
[152] EDPB Guidelines, p. 9

According to the EDPB, the applicability of the Regulation has to be considered separately for a controller and a processor for each activity (as was already noted hereinbefore) and each processing operation[153]. Korff expounds this by making an example in which the same entity appears as the data controller in one processing operation, however, its role changes to joint controller or even data processor in another operation[154]. This is particularly true for "complex arrangements between different entities including groups of companies"[155]. Indeed, in the given example, all sorts of interconnections and capacities may occur between the entities.

The EDPB asserts that the GDPR provides for "different and dedicated provisions or obligations" applicable to controllers and processors[156]. However, it is not exactly so. With respect to processor's obligations, they are set out substantially in Article 28 GDPR[157]. As regards obligations related to controllers, they are not singled out, so far as effectively all the GDPR provisions apply to them, except for those which are exclusively applicable to processors.

2.5.2. Application of the establishment principle to the non-EU joint controllers

As Korff has rightly observed, the EDPB had not addressed joint controllers in respect of the application of the establishment principle to them[158]. Albeit joint controllers are basically controllers, and thereby the respectful GDPR provisions will apply to them, however, the nature of interrelation between joint controllers deserves separate consideration.

To redress this omission, it is necessary to turn first to the definition. It implies that joint controllers are "two or more controllers [that] jointly determine the purposes and means of processing"[159]. On closer inspection, pursuant to the WP29, joint control occurs when, firstly, there are at least two different controllers, secondly, they act jointly in respect of the specific processing operation and, thirdly, those controllers determine "*either the purpose or* those essential elements of *the means* which characterize a controller"[160] (emphasis added). As it follows, in joint control, a controller does not

[153] EDPB Guidelines, p. 10
[154] Korff 2019, p. 25
[155] *Ibid*, p. 49
[156] EDPB Guidelines, p. 10
[157] Article 28 GDPR
[158] Korff 2019, p. 23
[159] Article 26(1) GDPR
[160] WP29, Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN, WP 169, adopted on 16 February 2010, p. 19

have to participate in defining *both* the purposes and means of processing, rather, it is important that actions of joint controllers concern one and the same processing operation. This specification seems to be reasonable since it lays stress that the allocation of responsibilities between controllers may indeed be of all kinds, and one controller may be responsible only for a minor part of a data processing operation.

The WP29 further clarifies that the level of participation of the controllers "may take different forms and does not need to be equally shared", that is to say, joint controllers may share determining all purposes and means together or decide who is doing which part of it[161]. For this purpose, the GDPR prescribes that in order to comply with the obligations placed upon them, joint controllers have to "in a transparent manner determine their respective responsibilities" in the form of an arrangement between them[162], which is likely to be done in a written way[163]. Such requirement aims at determining allocation of obligations and, thus, responsibilities of each controller when it comes to the specific processing operation.

In practice, different controllers may be responsible for the data processing "at different stages and to different degrees"[164]. For instance, in *Fashion ID case*, the CJEU admitted that *Fashion ID* acted together with *Facebook Ireland* as joint controllers in regard to determining the purposes and means of "the collection and disclosure" of the personal data, however, with respect to all "subsequent operations involving the processing […] by *Facebook Ireland* after their transmission to the latter", *Fashion ID* was not acknowledged to be a controller[165]. That is to say, in everything what concerns the subsequent operations, only *Facebook Ireland* appeared as a data controller. Therefore, as just shown, the level of participation of controllers in each processing operation has to be evaluated in the light of specific facts of the case.

As Advocate General Bot rightly noted, 'joint' responsibility is not the same as 'equal' responsibility[166]. In this sense, 'jointly' stands for 'together with', and nothing more. This observation was met with support in a number of the CJEU's judgments which reiterated that "the existence of joint responsibility does not necessarily imply equal

[161] WP29, Opinion 1/2010 on the concepts of "controller" and "processor", p. 19
[162] Article 26(1) GDPR
[163] Korff 2019, p. 23
[164] WP29, Opinion 1/2010 on the concepts of "controller" and "processor", p. 22
[165] CJEU, Case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, interveners: Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, 29 July 2019, para 76
[166] Opinion of Advocate General Bot, para 75

responsibility of the various operators involved in the processing of personal data"[167]. To put it differently, if there are, for instance, two joint controllers at stake, and it is ascertained that controller 'A' is considered to be pursued under the GDPR with respect to three specific processing operations, this does not mean that the fact of joint control would lead to controller 'B' being responsible for the same three operations. By contrast, controller 'B' may be responsible, for example, only for two out of three operations if it acted as a controller regarding those two ones. Since controller 'A' appeared as a controller in all three cases, it will be subject to the GDPR controller obligations on the basis of three episodes. As regards controller 'B', it acted jointly with controller 'A' in two cases, therefore, the GDPR controller obligations apply to it on the grounds of those two processing operations. To conclude, the GDPR controller obligations apply to joint controllers separately and in view of contribution of each of them to the specific processing operation or its part.

2.5.3. A controller subject to the GDPR uses a non-EU processor (the indirect application through Article 28 GDPR)

Quite often, a controller and a processor involved in the same processing operation or a set of processing operations are on the opposite sides of the EU, that is to say, one of them is based in the Union and another one outside the Union. Obviously, in such cases, the applicability of the GDPR to them will vary on the basis of the establishment principle.

Supposedly, a controller with an EU establishment decided to use a processor who is not established in the Union. In this case, the controller will be subject to the GDPR due to being established in the EU and processing in the context of its EU establishment's activities. However, as regards the non-EU processor, the situation is not that straightforward as it may seem on the surface. That is to say, the non-EU processor, even though not being established in the Union, will not avoid the application of the Regulation to it.

In this respect, the EDPB stipulates that the controller will have "to ensure by contract or other legal act that the processor processes the data in accordance with the GDPR", namely complies with the GDPR processor obligations set out in Article 28(3)

[167] *See* Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein case, para 43; CJEU, Case C-25/17, Tietosuojavaltuutettu, intervening parties: Jehovan todistajat — uskonnollinen yhdyskunta, 10 July 2018, para 66; Fashion ID case, para 70

GDPR[168]. This is not a requirement made-up by the EDPB since, indeed, the Regulation provides for a provision which states that "[p]rocessing by a processor shall be governed by a contract or other legal act under Union or Member State law"[169]. So, basically, the EDPB has interpreted how the said provision has to be put into practice. Since the provision in question does not specify whether it concerns the processors in the Union or outside the Union, it results from this that the requirement concerns all processors, irrespectively of the place of establishment.

Why namely the controller has to ensure that the non-EU processor is obliged by contract or other legal act to abide by the GDPR provisions, lies in the controller's own obligation to use only 'reliable' processors. This means that the processor has to be able "to implement appropriate technical and organisational measures" that would ensure the processing in conformity with the GDPR[170]. As a result, the non-EU processor will "become *indirectly subject*"[171] through Article 28 GDPR to some processor obligations on account of the contract or other legal act (emphasis added). In this sense, the non-EU processor's legal status becomes effectively the same as if it was the EU-based processor. If considering whether this is right or wrong approach, many would incline to choose 'right' since, first of all, not imposing the obligations on the non-EU processor would put the EU individuals' rights at risk; secondly, if conclusion of the contract or other legal act bothers the non-EU party, its analogue can always be found on the EU market of processors instead.

It is worth noting that in the case at issue the data processing has to be carried out by the non-EU processor's establishment based outside the EU. If, for instance, the non-EU processor has establishments both in the Union and outside the Union, and if the processor is going to use one of its EU establishments for the processing activities ordered by the EU controller, "then GDPR processor obligations would apply directly to the processor"[172]. As regards such multinational data processors, Korff suggests that the processor's obligations required under the Regulation should be stipulated in a "standard overall contract – typically referred to as a Master Services Agreement […], or in a separate addendum to that contract"[173]. It seems that such an agreement would be a more practical solution than every time concluding a contract with the EU controllers.

[168] EDPB Guidelines, p. 11
[169] Article 28(3) GDPR
[170] Article 28(1) GDPR
[171] EDPB Guidelines, p. 11
[172] Korff 2019, p. 31
[173] *Ibid*, p. 32

Moreover, it would demonstrate the non-EU company's desire to comply with the GDPR.

2.5.4. A controller not subject to the GDPR uses an EU processor (providing a processing service)

There will be quite another situation if a non-EU controller that is not subject to the GDPR decides to choose an EU-based processor to carry out processing on its behalf. With respect to the non-EU controller, it will not be pursued under the GDPR on the stipulation that it neither conducts processing in the context of the activities of its EU establishment (if there is any) – thereby Article 3(1) GDPR is dismissed, – nor targets individuals in the Union in either form – Article 3(2) GDPR falls away as well[174]. Of course, if other circumstances at place, i. e., the opposite to the mentioned above ones, the GDPR controller obligations may apply. However, commonly, in the straightforward scenario, there are no grounds for the application of the controller obligations to the non-EU controller.

As regards the EU processor in the case at stake, it will be subject to the GDPR processor obligations on the basis of being established in the Union and carrying out processing in the context of the activities of that EU establishment[175]. In other words, the Regulation will apply so far as all the conditions stipulated in Article 3(1) GDPR regarding the EU processor are met.

As shown above, the applicability of the establishment principle to the EU processor does not actuate the applicability to the non-EU controller, which is notably the opposite effect to the situation discussed in paragraph 2.5.3 of the paper hereinbefore. The fact of the matter is that the non-EU processor, though being itself subject to the GDPR, has neither the obligation nor the right to impose the GDPR obligations on the non-EU controller. As the EDPB noted, "[b]y instructing a processor in the Union, the controller not subject to GDPR is not carrying out processing "in the context of the activities of the processor in the Union""[176], otherwise, the effect would vary. That is to say, each of the parties remains to conduct processing in the context of its own activities.

[174] EDPB Guidelines, p. 11
[175] *Ibid*, p. 12
[176] *Ibid*

Moreover, "the processor is merely *providing a processing service* which is not "inextricably linked" to the activities of the controller"[177] (emphasis added). The relationship which occurs between two entities is defined by the EDPB as the relationship of the client company and the processor[178]. To put it even more simply, one company, – the client, – hires another company, – the contractor, – to carry out the processing service on its behalf. In view of this, it seems that the legal relationship at issue lies more in the field of contract law than the data protection law, thereby there is no wonder that the GDPR cannot be applied to the client company established in the third state.

The EU processor being pursued under the GDPR will most likely have to deal with the personal data collected "in a non-GDPR-compliant manner"[179] since the data was first processed by the non-EU controller which probably did not follow the GDPR provisions. Therefore, in order to not to run risks of breaking the law, the EU processor should ensure, for instance, by contractual means that the other party provides data for processing within the law[180]. Such a contract would regulate the relationship 'client – processor'. The need to settle a contract comes from the EU processor's obligation for its own part to process "under Union or Member State law"[181], despite the fact that the non-EU controller is not subject to the GDPR.

An EU-based processor as an establishment of a non-EU controller

The EDPB has passed an interesting opinion, though without further explanation, that "a processor in the EU should not be considered to be an establishment of a data controller within the meaning of Article 3(1) *merely by virtue of its status as processor on behalf of a controller*"[182] (emphasis added). On a strict reading, this means that there may be the cases where the fact of using the EU processor will be equated with having an establishment in the Union. However, what other conditions are implicated the EDPB has not specified.

Korff deems that in this case the EU processor has to do something more than merely data processing on behalf of the non-EU controller: the EU processor's activities must

[177] EDPB Guidelines, p. 12
[178] *Ibid*, p. 10
[179] New Guidance on the GDPR's Territorial Scope – Are You Covered?, 30 November 2018. Available at: <www.debevoise.com/insights/publications/2018/11/new-guidance-on-the-gdprs-territorial-scope>
[180] *Ibid*
[181] Article 28(3) GDPR
[182] EDPB Guidelines, p. 10

be ""inextricably linked" – read: essential to – the non-EU controller organisation", for instance, to revenue-raising[183]. So, the logic is the same as when showing that the processing is being conducted in the context of the activities of an establishment in the Union. Consequently, if the EU processor is acknowledged to be the non-EU controller's establishment in the Union, this means that the non-EU controller is established in the EU and, moreover, processes data in the context of the activities of the said establishment. As a result, the GDPR will apply to the non-EU controller.

Indeed, the given example may be the case, moreover, it may be the only possible case since the concept of establishment in the Union does not envisage the existence of other applicable grounds. Furthermore, from the practical perspective, the given scenario looks rather feasible: the processor may indeed carry out processing activities to the extent that it contributes to the revenue-raising by the controller. This example confirms the observations made in paragraph 2.2.4 of the paper hereinbefore, when stating that an EU company which was hired specifically for the purposes of the non-EU entity, may be considered as an establishment in the Union. Thereby, as shown above, the non-EU controller may be applicable to the GDPR controller obligations due to having the establishment, though through the EU processor, in the Union, and the given case may occur only if the EU processor's activities are considered inextricably linked to the processing carried out by the non-EU controller. Under other circumstances, the GDPR will not apply to the non-EU controller.

[183] Korff 2019, p. 9

III. APPLICABILITY OF THE TARGETING PRINCIPLE (ARTICLE 3(2) GDPR)

3.1. The targeting principle

Even if a non-EU entity is not established in the Union, the GDPR can still apply to it. In contrast to the establishment principle that is applicable to both the EU companies and the non-EU ones, the targeting principle is oriented purely towards the controllers and processors that are not established in the Union. To put more specifically, it also focuses on those non-EU entities which do not process personal data in the context of the activities of their EU establishments (if such are available)[184]. In any event, the applicability of the targeting principle may be possible on precondition that the establishment principle is not applicable. Therefore, it seems reasonable to start checking the targeting test (contemplated below) after it is found impossible to apply the establishment principle.

The targeting criterion is underlaid by the principle of *lex loci solutionis*, pursuant to which the choice of law is defined by the place where the "*contractual performance* is being offered"[185]. To put it into the context of the matter at stake, the territory of the EU will be the place where the data subjects are targeted, therefore, the law of the Union will be decisive, and the Regulation will apply. Notably, in order to fully convey the meaning of the given criterion, it is suggested to use term 'the marketplace rule'[186] as opposed to the principle of *lex loci solutionis*. Even though both terms are practically synonyms, 'the marketplace' often refers to 'virtual marketplace', thus, includes broader range of targeting activities, in particular online-related matters of targeting the EU data subjects[187]. Due to the said feature, 'the marketplace rule' better reflects the information society legal reality.

The targeting principle is stipulated in Article 3(2) GDPR and reads as follows: *"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

[184] WP29, Opinion 8/2010 on applicable law, p. 30
[185] Voigt – von dem Bussche 2017, p. 26
[186] Schonhofen, Sven – Detmering, Friederike, Territorial applicability of the GDPR. New EU data protection law also to apply to non-EU organizations. Business Law Magazine, Vol. 1 (2018), 3-5, p. 4
[187] *Ibid*

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."[188]

As it follows, the Regulation envisages two alternative categories of activities, – offering of goods or services and monitoring, – which, if performed by a non-EU controller or processor, will invoke the application of Article 3(2) GDPR. It is utterly important for the applicability of the targeting principle that the mentioned activities concern individuals exactly in the EU.

3.2. The concept of targeting

In order to define the scope of targeting, it is necessary to inquire into a question of where 'targeting' originates from and the evolution of the understanding of the given concept. This will allow determining not only what the processing activities are related to, but also what those activities are aimed at.

The predecessor of the GDPR – the DPD dating from 1995 – did not contain any reference to targeting or related notions so far as the grounds for the applicability of the DPD to the non-EU entities were based on the use of equipment criterion[189]. So, the concept of targeting in the GDPR has other origin.

The first mentioning of the 'directing activities to the Member States' took place in the context of consumer contracts in Brussels I Regulation[190]. Later, in Rome I, there was confirmed the consistency with Brussels I Regulation regarding the 'directed at' test with respect to consumer contracts; also, there was used for the first time, notably, in the same context, the notion of '*targeting* activities at the Member State'[191]. Thus, the regulation Rome I identified 'directing' and 'targeting' of activities as the same concepts. The Brussels I Regulation's successor, which has repealed it in 2012, reiterated the existing 'directed at' test without elaborating on the issue at stake[192], thereby remaining the meaning of the concept unamended. Furthermore, Advocate General Trstenjak in her Opinion in *Pammer and Hotel Alpenhof joined cases* used an

[188] Article 3(2) GDPR
[189] Article 4(1)(c) DPD
[190] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters – no longer in force, Article 15(1)(c)
[191] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), Recital 24
[192] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), Article 17(1)(c)

example illustrating that the "use of websites to target advertising to nationals of other Member States" is a criterion sustaining directing of activities[193]. As it follows, if 'directing' can be shown by means of 'targeting', the given concepts are mutually complementary. To conclude at this point, the concept of targeting originates from the consumer protection field where 'directing at' and 'targeting to' have close meanings or are even used as synonyms.

The WP29 has suggested in its Opinion 8/2010 on applicable law to take targeting criterion used in consumer protection field as a basis for future legislation in relation to the non-EU controllers. In the WP29's view, this "would bring additional legal certainty to [the non-EU] controllers as they would have to apply the same criterion for activities which often trigger the application of both consumer and data protection rules"[194]. Indubitably, if the Opinion was adopted some years later, it would have concerned the non-EU processors as well. At this point, there are two important takeaways: first, the WP29 has initiated launching of the targeting criterion into data protection law, second, it has acknowledged that unification of consumer and data protection rules is necessary with regard to the controllers (and probably processors) not established in the Union. Furthermore, the way the WP29 has exemplified targeting allows concluding that 'directing activities to' is a form of targeting: "targeting could consist of: […] services explicitly accessible or *directed to* EU residents"[195] (emphasis added). So, unlike consumer protection, data protection field regards 'targeting' and 'directing' activities as the whole and its part. In other words, 'directing' means to target, however, 'targeting' may have many other forms.

The WP29's recommendations named above concerning the non-EU entities were taken into consideration and were finally embodied in Article 3(2) GDPR. Notably, the Regulation itself mentions 'targeting' only once throughout the whole document with respect to the data subjects in the Union[196], however, does not do so with regard to the criteria provided in Article 3(2) GDPR. In this respect, the Regulation does not provide clear understanding as to whether it supports the WP29's views concerning the concept of targeting or whether it has different vision.

[193] Opinion of Advocate General Trstenjak, delivered on 18 May 2010, Case C-585/08, Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Case C-144/09, Hotel Alpenhof GesmbH v Oliver Heller, para 36
[194] WP29, Opinion 8/2010 on applicable law, p. 31
[195] *Ibid*
[196] Recital 122 GDPR

Aiming at assisting Asia Pacific Privacy Authorities (APPA) to understand the requirements of the GDPR, the WP29 has issued a document in which it explained that the Regulation, in particular, applies to the non-EU controllers and processors "*that target* individuals in the EU *by offering* goods and services […] *or that monitor* the behavior of individuals in the EU"[197] (emphases added). As Svantesson noted, the most important thing about this explanation is the "specific inclusion of the phrase 'target individuals in the EU'"[198]. Indeed, what the WP29 has done is that it has clearly and directly named the main feature of activities covered by Article 3(2) GDPR – *targeting*, – which, as noted above, was not done by the Regulation. Notably, on a strict reading, it looks like the WP29 has referred 'offering goods and services' to the forms of targeting, however, has separated 'monitoring' as if has not considered the latter as a form of targeting. It seems that such formulation was not really implied by the WP29 since it does not meet support in the rest of the document.

Finally, the EDPB in the Guidelines on the territorial scope of the GDPR unambiguously refers to the targeting criterion as the common denominator for the activities set out in Article 3(2) GDPR. That is to say, the EDPB uses 'targeting' as a general term which designates both 'offering goods and services' and 'monitoring the behaviour'[199]. The said activities may appear in various forms, as will be shown hereinafter in the paper. Nevertheless, irrespectively of the form, the activities must have features attributable to 'targeting' in order to invoke application of the targeting principle.

Indubitably, 'targeting' was chosen by the EDPB to name the respective principle so not without purpose – it to the best advantage characterizes the scope of the activities concerned. Indeed, what consolidates 'offering of goods and services *to*' together with 'monitoring the behaviour *of*' is the data subjects in the Union *to whom* the said activities are *directed*. Notably, the EDPB Guidelines is the first document of the data protection authority after the WP29's Opinion 8/2010 on applicable law which contemplates the concept of directing activities. The EDPB deems that even though the concept of directing activities is not the same as offering of goods or services, it still may be used to assess "whether goods or services are offered to a data subject in the

[197] WP29, EU General Data Protection Regulation, General Information Document, 12 February 2018. Available at: <www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614208>
[198] Svantesson 2019, p. 8
[199] EDPB Guidelines, p. 13

Union"[200]. That is to say, 'directing' appears as a form of conducting 'offering' and therefore may indicate the targeting character of activities. In spite of the fact that the concept of directing activities originates from consumer protection field where it has close meaning with 'targeting', in data protection law the case is different.

Furthermore, by directing activities, the non-EU controllers or processors set themselves a task to reach certain goals, i. e., to target the EU individuals. To put it differently, the concept of targeting characterizes not only the scope of the nature of the activities, i. e., *targeting as an activity*, but also defines the subjective component of the non-EU entities which is to reach the data subjects in the Union – *targeting as a goal*. Given subjective component will be discussed further in more detail.

3.3. The targeting test

In order to determine whether a non-EU controller or processor directs its activities at the data subjects in the Union, it is necessary to apply the targeting criteria. The test offered by the EDPB does not introduce any additional conditions to those stipulated in Article 3(2) GDPR. However, as mentioned above, it seems necessary to improve the algorithm provided by the EDPB. Thus, it is suggested to check the applicability of the targeting principle following such steps:

1) checking the applicability of the establishment principle[201] – if impossible to apply, then proceeding to the next steps set out in this test;
2) determining whether the processing of personal data concerns the data subjects who are in the Union;
3) determining whether the processing is related to either the offering of goods or services or to the monitoring of data subjects' behaviour within the Union[202].

As appears from the above, the processing is a central determinant in the targeting test. It creates a two-way connection between the targeting activities, – offering of goods or services and monitoring, – and the data subjects in the Union. If at least one out of three specified elements is missing, the targeting test will not be passed.

Practical application of the targeting test can be illustrated with a real case based on the GDPR. On 11 October 2018, the UK Information Commissioner's Office (ICO) issued

[200] EDPB Guidelines, p. 17
[201] *See* 2.2.3. The establishment test
[202] EDPB Guidelines, p. 14

a written warning against the US-based newspaper *The Washington Post* regarding its cookie consent practices[203]. According to the complaint raised with the ICO, in order to get access to the website of the newspaper, a user in the EU had to "either accept cookies or to pay for a full subscription to the service"[204]; in the latter case, cookies and tracking would be, of course, switched off. The ICO took the view that under mentioned circumstances the "consent cannot be freely given and is invalid" since there was no alternative presented to users which would at the same time exclude fees and cookies[205]. In the given case, Article 3(2)(a) GDPR was applicable to *The Washington Post* so far as the US company did not have any business presence in the Union, however, intentionally offered its subscription services to the EU individuals.

Presumably, there are no grounds found for the application of the establishment criteria. So, this chapter will contemplate the targeting test omitting the first step.

3.4. Data subjects in the Union

Notably, 'data subjects who are in the Union' is the cornerstone of the whole Article 3(2) GDPR. It is an equally important condition under both alternative types of processing activities envisaged by the targeting principle – offering of goods or services as well as monitoring of behaviour. Thus, whether Article 3(2) GDPR is applicable to the specific processing activity directly depends on whether targeted data subjects are located in the Union.

3.4.1. Unlimited scope of a data subject

First of all, it is necessary to define what categories of data subjects are protected under the Regulation and, consequently, the targeting of whom will trigger the application of the targeting principle.

Broadly speaking, the Regulation grants protection to all individuals who are in the Union in relation to the processing of their personal data. It applies irrespectively of the nationality, place of residence[206], citizenship or any other data subject's legal status[207].

---

[203] The information about the warning is missing on the ICO's official website since it was not an enforcement action or so. Therefore, *see*, for instance, Hill, Rebecca, Washington Post offers invalid cookie consent under EU rules – ICO, 19 November 2018. Available at: <www.theregister.co.uk/2018/11/19/ico_washington_post/>

[204] Information Commissioner's Office's letter to WP Company LLC, 11 October 2018. Available at: <www.mega.nz/#!mkISAIrb!xrior2Ffk7C_ILuNTqa9uPhuzMYPUjU19FSwfZTFrqM>, p. 1

[205] *Ibid*, p. 2

[206] Recital 14 GDPR

[207] EDPB Guidelines, p. 15

Thereby the targeting principle may concern the hereupon listed categories of data subjects: EU citizens, non-EU citizens, stateless persons, refugees, asylum seekers – everyone who resides in the Union. In addition, it encompasses all other individuals who do not reside, but happen to be temporarily in the territory of the EU, such as cross-border commuters, visitors, tourists or even travellers in transit. For instance, a resident of Lugano (Switzerland) who travels on weekdays to visit his parents in Como (Italy), will enjoy protection under the Regulation whenever his personal data is being processed while he is in the territory of Italy. As it follows, the scope of a data subject is not limited to any legal status defining a physical person. Therefore, in the context of Article 3(2) GDPR, the only significant circumstance is that the data subject in question is located within the Union.

3.4.2. Spatial scope of stay in the Union

In general, to be located in the Union in terms of spatial scope means that a data subject is "physically present"[208] within the EU. Notably, the duration of the physical presence is not decisive – it can, roughly speaking, last one hour while a traveller is changing the plane at the airport of Munich, but the most important thing is that the processing of the traveller's personal data takes place at some point of time during those sixty minutes of staying in the EU.

It should be reminded here what is implied when referring to the wording 'in the Union'. As previously noted in paragraph 1.6 of the paper hereinbefore, the GDPR is binding not only in all 27 Member States of the Union, but also on the territory of three more EEA states, namely Iceland, Liechtenstein and Norway. Hence, the same understanding should be applied when contemplating Article 3(2) GDPR. That is to say, the wordings 'data subjects (who are) in the Union' as well as 'behaviour within the Union' should be understood broadly and therefore mean referring to the EU Member States along with Iceland, Liechtenstein and Norway.

Online being in the Union

As regards the scope of stay in the Union in *online* environment, Gömann deems that it is not clear when an online behaviour of a data subject is considered to occur within the

[208] Linklaters, The General Data Protection Regulation: A survival guide – Version 2.0, 13 December 2018. Available at: <www.linklaters.com/en/insights/publications/2016/june/guide-to-the-general-data-protection-regulation>, p. 8

Union and when not[209]. Indeed, 'being in the Union online' is a problematic notion since it requires setting out how legal EU borders correlate with the online ubiquity. Obviously, the latter is a much broader notion: if an online behaviour can take place in the Union, then it appears from this that some other online behaviour can occur in the third state. Therefore, in order to show that the online behaviour takes place namely in the EU and not somewhere else, there has to be a certain connection with the Union.

In this respect, Gömann flatly discards "the place of Internet access or the location of the servers processing the information" as the possible solutions[210], however, does not provide any probable suggestions instead. With respect to the location of the servers, it indeed does not matter at all since, according to the GDPR, the place of processing is irrelevant for the applicability of the Regulation[211].

However, as concerns the place of Internet access, it is difficult to agree with Gömann. It seems that namely this link would be capable of connecting the data subjects and the Union. Every time when an individual accesses the Internet, his or her location is identified by servers, and even though that location is read as just an IP address, it allows determining practically an exact physical location of that data subject. Thus, even in the cases of online behaviour, the data subjects must be physically present in the Union, notably when accessing the Internet.

Granmar suggests that it should not matter where the Internet is accessed from, – whether from any of the EU Member States (which is true since in such case a data subject is in the Union), or whether "from the place in a third country" alleging that otherwise there would be "inconsistency in the Union legal order if the GDPR could not be invoked only because the website was accessed from a place in a third country"[212]. Actually, the last part sits uncomfortably with the concept of being located in the Union. Bearing in mind that the scholar implies in the first place the EU citizens in the given example, some kernel of good sense can be found here, i. e., how come that the EU citizens are not granted protection under the GDPR if they access the Internet from outside the Union, while the Regulation has such a far-reaching effect worldwide. Nevertheless, it is so. Accessing the Internet from the Union requires being physically present in the EU.

[209] Gömann 2017, p. 587
[210] *Ibid*
[211] Article 3(1) GDPR
[212] Granmar 2019, p. 39

3.4.3. Temporal scope of stay in the Union

The temporal component is no less important than the spatial one discussed above. However, its application is not that obvious. As Granmar noted, clear understanding of when exactly the data subjects have to be present within the EU allows determining the burden of proving resting on the non-EU controller or processor[213].

The EDPB suggests that the data subjects' being in the Union has to be evaluated "at the moment when the relevant trigger activity takes place, i. e. at the moment of offering of goods or services or the moment when the behaviour is being monitored", and adds that the duration of the said targeting activities does not matter[214]. On the surface, it may seem that the guidance rephrases the text of Article 3(2) GDPR and states the obvious. However, construing it this way, the EDPB actually raises more questions than provides the answers.

First of all, it is unclear, what exactly is implicated by "the relevant trigger activity" which defines when the data subjects have to be in the Union. Under the assumption that it is 'the *targeting* activity' meant, then there should have been 'offering' and *'monitoring'* activities specified in the explanatory part of the guidance coming after 'i. e.' This way, it would have been shown that the said activities *target* the data subjects in the Union, but have not led to the processing yet. As it follows, the wording 'the behaviour is being monitored' implies that the processing is already being carried out, which is in advance as compared to 'offering of goods or services' that does not necessarily envisage the processing (this issue is contemplated further in the paper). Thus, it is unlikely that the EDPB implied 'targeting activities'.

Alternatively, if there were 'the *processing* activities' implicated, then this would have been more logical since the GDPR applies to the *processing* of personal data, – not to the targeting activities as such. Anyway, even in such case, the provided guidance was not formulated correctly. There should have been 'at the moment of *processing related to* the offering of goods or services' stipulated as the suitable point in time. In regard to the monitoring activities, the way how it was construed by the EDPB, – 'the moment when the behaviour is being monitored', – expresses to the best advantage that the processing is being conducted. On the basis of the discussed above, it appears that the

[213] Granmar 2019, p. 39
[214] EDPB Guidelines, p. 15

data subjects' 'being in the Union' has to be evaluated at the moment when the processing related to the relevant targeting activity takes place.

'Stay in the Union' and monitoring

Monitoring as such consists of the targeting and the immediate data processing which happens at the same time as the targeting activity. Thereby the moment of targeting and the moment of data processing concur, i. e., happen simultaneously. For this reason, the exact time when a specific processing operation occurred is easy to determine.

In essence, targeting becomes monitoring only when it is accompanied by data processing. Conversely, if personal data of a data subject in the Union was not processed, this means that the data subject was not monitored. Thus, the subsequent processing after targeting is an essential condition.

Based on the above, for the applicability of Article 3(2) GDPR on the basis of monitoring, there need to be two conditions met: first, a non-EU controller or processor monitors the behaviour of a data subject in the Union, i. e., targets a data subject and processes the data subject's personal data, second, the data subject is physically present in the Union. So, in case of monitoring, the moment when the behaviour is being monitored indeed determines the time of stay of the data subject in the Union.

'Stay in the Union' and offering

Another situation will be when considering offering of goods and services. The fact of the matter is that the moment of offering of goods or services is *not a data processing yet*. There is no doubt that offering is a form of targeting and, thus, envisages the latter. However, offering as such does not necessarily include processing, and that changes a lot.

It is worth reminding that the GDPR is oriented largely towards online activities, however, it applies also to the *offline ones*. Therefore, offering of goods or services may occur also outside the scope of information society world. In real life, an offer of goods or services may be made in the form of various outdoor advertising, including even the publicity-mast advertising. For instance, a private language school located in China offers online language courses for the residents of Poland, and the school orders the placement of respective advertisements on the billboards in the biggest cities of Poland. Indubitably, individuals residing in Poland will be targeted by Chinese school, however,

unless they provide their personal data to the said school for the purposes of, say, enrolment to the courses, their data will not be processed. Thus, targeting occurs, however, this does not trigger the processing of data.

As regards offering of goods or services *online*, in fact any offering will additionally invoke processing of personal data. The mere publication of an advertisement will target certain groups of individuals, depending on other circumstances of the case. It is not even required that a data subject has to accept an online offer aimed at him or her in order to cause the initiation of the processing of his or her data – the mere visit of the website will lead to the processing of at least the IP address of the visitor for the statistical purposes. Therefore, on the Internet, processing is unavoidable.

As shown hereinbefore, offering as a targeting activity in general is possible even when the subsequent data processing does not take place. Such offer which does not draw after it the data processing will not invoke the application of Article 3(2) GDPR since the Regulation requires that the conditions of territorial scope are accompanied with the conditions of material scope present, i. e., the data processing must take place[215]. Therefore, the EDPB's suggestion stating that the data subject's 'being in the Union' has to be evaluated at the moment of offering of goods or services is quite perfunctory and cannot be applied literally. Moreover, 'aiming at' is not enough since the subsequent processing is required. It would be more precise to state that as regards offering, the data subject's stay in the Union has to be evaluated at the moment when the processing activity *related to* an offer of goods or services takes place.

Thereby for the applicability of Article 3(2) GDPR on the basis of offering, the following conditions must be fulfilled: first, a non-EU controller or processor offers goods or services to a data subject in the EU, second, the data subject is physically present in the Union, third, the data processing takes place when the data subject is in the EU. This way, it is stressed that offering and processing are, though related, but separate activities, and to invoke the targeting principle, it is important that the data subject is located in the Union not when the offer is made, but when the processing related to the offer is carried out.

[215] Article 2(1) GDPR

3.4.4. Temporal applicability of the targeting principle

The data subjects' time of stay in the Union is a determinant which assists with defining the exact time when the targeting principle is applicable. To put it differently, it specifies at what point in time a non-EU controller or processor becomes pursued under Article 3(2) GDPR.

As stated above, targeting itself does not always envisage data processing, namely monitoring includes processing of personal data at all times, however, offering may either come before the subsequent processing or not lead to the latter. Therefore, it is utterly important to define when the data processing is considered to be commenced.

In terms of the definition of 'processing', it can be "any operation or set of operations which is performed on personal data or on sets of personal data"[216]. As a result, a non-EU controller or processor is subject to the GDPR every time when it carries out processing operations related to data subjects in the Union. However, it would be too imprecise to allege that the time of the data processing defines when the targeting principle is applicable. The reason for that is that such conclusion would mean that all the conditions, including the data subjects' stay in the Union, would need to be met during various stages and forms of processing in order to apply the targeting principle.

In practice, this would lead to such an absurd situation when a resident of the EU becomes deprived of his or her right to protection under the GDPR for the period of being outside the Union[217] and obtains it back when returning home; respectively, as concerns the non-EU controller or processor, it would be out of responsibility for the data processing while the data subject is outside the Union. Thus, 'time of the data processing' as a concept implying all respective forms of processing is too broad to use it for determining the commencement of processing.

Returning to the operations which can be carried out on personal data, 'collection' is a fundamental one since it serves as a basis for all the subsequent operations. Indeed, before being used, altered, analysed etc., data has to be collected first. Thus, without the stage of 'collection' the other processing operations would be impossible. In terms of

[216] Article 4(2) GDPR
[217] Plath, Kai-Uwe (Hrsg.), *BDSG/DSGVO. Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG (2. Auflage)*. Köln: Otto Schmidt, 2016, Art. 3, rec. 14 in: Voigt – von dem Bussche 2017, p. 28

this observation, "*the time of the collection* (in a broad sense) of the data is decisive"[218]. Since that very moment of data collection the non-EU controller or processor becomes pursued under Article 3(2) GDPR. With respect to other processing operations which go after the collection, they must be fulfilled in accordance with the Regulation[219], irrespectively of whether the data subject concerned is still located in the territory of the EU or has left it and will never come back.

In this context, it is obvious that the wording of Article 3(2) GDPR about the data subjects in the Union should not be interpreted restrictively – instead, it should be implicated that the data subjects have to be located within the EU only at the moment of collection of their personal data. That would be enough for the application of the targeting principle.

3.5. Offering of goods or services to data subjects in the Union

3.5.1. The notion of goods and services

While the GDPR stipulates that it applies to the processing activities that are related to the offering of goods and services[220], it does not explain, – either for the purposes of Article 3(2)(a) GDPR, or for the Regulation in general, – which exactly goods and services are implied. Such explanation would be of assistance especially in the context of data processing activities in online environment which the GDPR is particularly intended for.

In Safari's view, the mentioned terms should be sought for in the TFEU[221]. Though indirectly, the latter provides for the definition of 'goods' as "products originating in Member States [or] products coming from third countries which are in free circulation in Member States"[222]. So, for the purposes of Article 3(2)(a) GDPR 'goods' should be understood as any kind of products originating typically from the non-EU states, or, less sparsely, though still possibly, from the Member States, and that are offered by the non-EU entities to data subjects in the Union. For example, an online shop based in the Republic of Korea sells cosmetics of Korean brands and offers delivery to the EU.

[218] Plath 2016, Art. 3, rec. 14 in: Voigt – von dem Bussche 2017, p. 28
[219] *Ibid*
[220] Article 3(2) GDPR
[221] Safari, Beata A., Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. Seton Hall Law Review, Vol. 47 (2017), 809-848, p. 838
[222] Article 28(2) TFEU

With regard to 'services', the TFEU defines them as activities either of an industrial or commercial character, or activities of craftsmen or professions, that "are normally provided for remuneration"[223]. Since the Regulation does not set out any limitations as to the scope of services concerned, it seems that all mentioned forms of services through activities may take place on behalf of the non-EU controllers and processors.

For instance, *LinkedIn*[224] embraces at least two groups of services – activities of the commercial character, such as marketing and sales, and, additionally, activities related to the professions[225]. As for today, it offers advertising services 'Sponsored content', 'Sponsored inmail', 'Text ads' and 'Dynamic ads' that aim at promotion businesses with the help of *LinkedIn*[226]. Another product, which is called '*LinkedIn* Sales Navigator', serves to "target the right buyers"[227] and, as a result, score big business successes faster. While activities of the commercial character are very common on the Internet, activities of the professions are less known. Safari deems that this form of services manifests itself through *LinkedIn* creating proper environment where employers and potential employees can find one another and take advantage of such interaction[228]. Thus, as just shown, the services offered by the non-EU entities may take the shape of various activities as soon as the receiver of the offer benefits from it somehow or other.

Notably, with respect to remuneration which the TFEU considers as typically following the service, the GDPR goes further and prescribes that it applies to the processing "irrespective of whether a payment of the data subject is required"[229]. This way, the Regulation stresses on the broad range of services covered by its application – services for a fee along with free ones which the information society environment is so abundant in. Svantesson is of the opinion that extension of the GDPR to free of charge goods and services is significant in the online environment[230]. Barlag takes the same view and notes that it is principally oriented towards international companies which offer their

[223] Article 57 TFEU
[224] *Note* that *LinkedIn* is used here as an example to demonstrate the *forms of services* only; it does not concern the issue of targeting principle in general discussed in the given chapter. Despite the fact that *LinkedIn* is a company headquarted in the US, it has three establishments in the Union, therefore, most likely, the establishment principle will apply to its processing activities.
[225] Safari 2017, p. 839
[226] LinkedIn Marketing Solutions, Market to who matters, 26 May 2020 – last visited. Available at: <www.business.linkedin.com/marketing-solutions>
[227] LinkedIn Sales Solutions, LinkedIn Sales Navigator, 26 May 2020 – last visited. Available at: <www.business.linkedin.com/sales-solutions/sales-navigator>
[228] Safari 2017, p. 840
[229] Article 3(2)(a) GDPR
[230] Svantesson 2019, p. 10

services on the Internet[231]. Indeed, the change aims at paying attention to the fact that not only offering of those goods and services that are *subject to fee* must be accompanied with processing in the GDPR-compliant manner, but also those goods and services that *do not require payment* by a data subject in the Union.

The GDPR repeatedly refers to one of the types of services – the information society services[232], however, does not define their place among the services offered by the non-EU controllers and processors. In this respect, the EDPB helpfully confirms that 'offering of services' implicates the information society services as well[233]. According to Directive (EU) 2015/1535, an information society service is any service provided "at a distance, by electronic means and at the individual request of a recipient of services"[234]. So, basically, information society services encompass all sorts of services that can be sent by the non-EU controllers and processors and received by data subjects in the Union by means of the Internet or other types of connections enabling provision of services at a distance, that is to say, "by wire, by radio, by optical means or by other electromagnetic means"[235]. As it follows, provision of information society services is not restricted by the means of transmission of data in their typical image, i. e., the Internet.

3.5.2. Offering requirements

a) offering has to be specific

There are certain general criteria indicating that a non-EU controller or processor intentionally targets data subjects in the Union by offering goods or services to them. In the first place, this will be the case when the EU individuals are specified, distinguished[236], categorized, referred to a certain group of people or some other way specifically mentioned so that it is clear enough that a non-EU entity targets namely those customers who are located in the Union[237]. For instance, formulations like 'youth

[231] Barlag, Charlotte, *Anwendungsbereich der Datencshutz-Grundverordnung* in: Roβnagel, Alexander (ed.), *Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts (1st edition)*. Baden-Baden: Nomos (NomosPraxis), 2017, rec. 18 in: Voigt – von dem Bussche 2017, p. 26
[232] *See*, e. g., Article 8 GDPR
[233] EDPB Guidelines, p. 16
[234] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, Article 1(1)(b)
[235] *Ibid*, Article 1(1)(b)(ii)
[236] EDPB Guidelines, p. 19
[237] Recital 23 GDPR

from the Nordic countries', 'guides and scouts of the EU', 'German and Polish volleyball teams' and so forth, if used by the non-EU entities in the description of goods and services they provide, will clearly confirm that namely those groups of individuals in the Union are intentionally targeted from the third country.

Another general indication of the EU-oriented offering is connected to the specific targeting through advertising[238]. In the given example, not individuals are a determining factor, but a place or territory in the Union – country, city, college, park, gym, library, concert hall etc., – any location where a non-EU controller or processor can place an advertisement of its goods or services. Even though this criterion of intentional offering differs from the one discussed above, however, the result is the same – the attained goal to reach data subjects in the Union. As just shown, in both instances, the criterion of *specific offering* served as a determinant – the specifically mentioned EU individuals or the specific advertising in the EU territory.

By contrast, the less specific offering is, the less probably it will be ascertained as targeting individuals in the EU. For instance, a job offer on the Internet that is directed at 'candidates with good command of English' undoubtedly concerns not only native speakers in the Union, but everyone who meets the requirement. For the reason of being too general, the said requirement cannot serve indication of the intentional targeting of the EU data subjects[239].

Even if considering some other EU language which is not that common as English, for instance, Greek, the outcome will not change much. Apparently, the lion's share of people speaking Greek live in Greece and Cyprus, however, an offer without any connection to territory and targeting job seekers 'with good command of Greek' concerns at the very least and in particular the Greek-speaking diaspora from all around the world. Thereby even having obvious *ex facte* connection with the Union is often not enough to prove targeting. Consequently, the criterion will be dismissed at all times if it is too general and does not allow connecting it exclusively with the EU.

b) offering needs to be accompanied with the processing related to it

Even if targeting the distinguished individuals in the Union with subsequent processing of their personal data, it does not necessarily invoke application of Article 3(2)(a) GDPR. This may particularly be the case when the processing of the employees'

[238] EDPB Guidelines, p. 19
[239] *Ibid*

personal data is under consideration. Therefore, the situations which involve personal data of the employees deserve separate consideration, especially with regard to those employees that are "highly mobile"[240], for instance, due to business trips. Notably, it does not mean that in this context employees have to be rendered as a special category of data subjects – quite the reverse, they should be treated like any other data subjects, irrespective of legal status. However, the nature of the processing activities that concern the personal data of the employees requires deeper analysis.

In the instances on the matter provided by the EDPB, one of which concerned the US employees on a business trip to the EU countries and the other one – residents of the EU whose employer located in Monaco, the processing in both cases was considered as "specifically connected to persons on the territory of the Union"[241]. Indeed, the processing activities conducted by the employer companies concerned the concrete data subjects, and the latter were physically present in the EU Member States. So, apparently, the condition of targeting of the distinguished individuals in the Union was met.

With respect to the processing activities conducted by the non-EU employers, they constituted solely the employment-related purposes, such as salary payments and human resources management. Despite having the processing at place and despite targeting specific data subjects in the Union, there was no offer of a service to the said data subjects established. As the EDPB underlined, the processing at stake did not "relate to an offer of a service to those individuals, but rather [was] part of the processing necessary for the employer to fulfil its contractual obligation and human resources duties"[242]. Indeed, 'being away on business' cannot be equated to 'being offered a service', or, to put it even more differently, 'being *offered to go* on a business trip' (meaning that it is an honour for an employee due to being chosen among other co-workers) still will not be regarded as an 'offer of a service', – the employee will act within his or her professional duties. The same logic applies to salary which *de facto* is a reward for doing work. Thus, for the reasons discussed above, the targeting test was not passed.

---

[240] Hunton Andrews Kurth, Centre for Information Policy Leadership, Comments by the Centre for Information Policy Leadership on the European Data Protection Board's "Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)" Adopted on 16 November 2018, 18 January 2019. Available at:
<www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_edpbs_territorial_scope_guidelines.pdf>, p. 12

[241] EDPB Guidelines, pp. 16, 18

[242] *Ibid*, pp. 16-17

The analysed cases cast light upon some unobvious details and remind about already contemplated ones. First of all, the targeting test, as shown in paragraph 3.3 of the paper hereinbefore, requires, in particular, that processing must *relate to an offer* of goods or services. Also, data processing can take place in connection with one of the legitimate grounds[243] that allow it happen, e. g., performance of a contract, however, not relate to an offering of goods or services. Finally, processing of personal data related to employment matters does not foresee *per se* any offers of goods or services to the employees, therefore, it cannot invoke application of Article 3(2)(a) GDPR.

c) offering has to target individuals in the Union *ab origin*

Although much has already been discussed about the data subjects in the Union in subchapter 3.4 of the paper hereinbefore, few more words need to be said in the context of offering, especially offering of services. The thing is that the provision of services and the concomitant data processing usually consist of repeated episodes, unlike the provision of goods. Therefore, provision of a service can be time-spaced which leads to various circumstances at different stages.

Arguably, any processing related to an offer of a service that takes place in the EU is subject to the Regulation on the basis of targeting principle. Obviously, it cannot be so. One of the reasons lies in the initial location of individuals that were targeted by the non-EU controller or processor. If the data subjects were offered a service outside the Union, and the said service was directed exclusively to the residents of the non-EU countries, then, even in case of their subsequent visit of the Union and the use of that service from the territory of the EU, the offer will remain targeting the non-EU individuals. The possibility of continuing to use the service in the Union does not change the fact that the service still targets individuals in the third states only. In such case, an important factor is that the targeted data subjects remain the same – no new ones from the EU added.

Moreover, even though the targeted individuals that came to the EU become in fact ‘individuals in the Union’, i. e., the category which is necessary for the applicability of the targeting principle, however, the GDPR will not apply to such processing since there was no preceding intentional targeting of individuals in the Union. By contrast, there

[243] Article 6(1) GDPR

occurred targeting of data subjects *outside* the Union, and this fact is unchangeable irrespective of the subsequent entering the EU by the said individuals.[244]

A typical illustration of such case may be banking sphere. For instance, Ukrainian bank *Privatbank* offers 147 various services through its application *Privat24*[245]. In order to use the application, an individual needs to have a bank account in *Privatbank*. So, only those who have such bank accounts are targeted by the offer, namely residents of Ukraine. When a user of application goes on vacation to the EU, he or she continues using the application on his or her mobile phone. The processing related to such offer of service will not become subject to Article 3(2)(a) GDPR since the offer was *ab origin* directed only at customers from Ukraine.

With respect to offering of goods, such situation is improbable (though not impossible) since goods as such are intended for one-time provision, thus, they normally are not supplied partly outside the EU first and then complemented within the EU. Nevertheless, if the circumstances happen to be as just described, the outcome will remain the same as in case of offering of services – the offer directed at individuals in the third states will not invoke the targeting principle, even if the targeted data subjects enter the Member States of the Union.

d) offering requires intention

Recital 23 in the preamble to the GDPR explains that a non-EU controller or processor will be considered offering goods or services to data subjects in the EU under the stipulation that "it is *apparent* that the controller or processor *envisages offering* services to data subjects in one or more Member States in the Union"[246] (emphases added). In fact, this should mean that the Regulation applies only when a non-EU entity *intends* to offer goods or services to data subjects in the EU. However, the way the legislator has stipulated that in recital 23 does not allow making such straightforward conclusions.

To understand better the logic behind the analysed guidance from the recital, the case law on the matter should be addressed. In *Pammer and Hotel Alpenhof joined cases*, the CJEU observed that it is necessary to determine availability of the "evidence demonstrating that the trader *was envisaging* doing business with consumers […] in the

[244] EDPB Guidelines, p. 15
[245] Privat24 home page, 26 May 2020 – last visited. Available at: <www.next.privat24.ua/>
[246] Recital 23 GDPR

sense that it *was minded* to conclude a contract with those consumers"[247] (emphases added). Obviously, most of the elements provided in the given judgment were adopted and embodied into the GDPR. However, one which is utterly important – evidence demonstrating intention – was not included into the text of the Regulation. One may argue that referring to the wording "it is apparent …" is an equivalent of 'evidence', however, what is apparent or is not so depends on one's subjective perception, unlike what constitutes evidence is determined by law. Therefore, it is suggested that by rephrasing the CJEU's judgment, which indubitably was taken as a basis for the respective guidance in the GDPR, its real meaning was distorted, thus, it is not possible to rely on recital 23 in full.

As Svantesson rightly observed, by stating that the non-EU controller or processor has *to envisage offering*, the legislator had made "the focus on subjective targeting, as opposed to objective targeting"[248]. In scholar's opinion, such formulation implies nothing else but "what is in the mind of the controller or processor that matters" by contrast with whether targeting takes place objectively[249]. Indeed, measuring the non-EU controllers' or processors' intention of offering in a way of relying on their forethoughts and considerations is quite unreasonable and far from the legal approach that requires factual reasoning. Therefore, bearing in mind the GDPR's goals and principles, it is suggested to interpret given recommendation not literally, but broadly.

The idea of objective targeting was also supported by Granmar who stressed on the need to rely on objective facts and not on "the actual state of mind of a person"[250]. Objective targeting implies that offering activities include an objective intention of the non-EU operator to direct its activities to data subjects in the Union, and this intention is manifested through *objective evidences* (contemplated closely in paragraph 3.5.3 of the paper). Thus, what the non-EU entity indeed envisaged is not decisive, moreover, it cannot be determined or checked objectively. On the contrary, the absence of evidences showing the intention to offer will speak of the impossibility to apply the targeting principle.

By contrast to the requirement stating that the offering has to be made intentionally in order to apply Article 3(2)(a) GDPR, the *unintentional* offering will not, respectively,

[247] CJEU, Joined Cases C-585/08 and C-144/09, Peter Pammer v Reederei Karl Schlüter GmbH & Co KG, and Hotel Alpenhof GesmbH v Oliver Heller, 7 December 2010, para 76
[248] Svantesson 2019, p. 11
[249] *Ibid*
[250] Granmar 2019, p. 37

invoke the provision in question. With regard to this observation, the EDPB has added an interesting note to the finalized version of the Guidelines in which it states that if "goods or services are inadvertently or incidentally provided" to data subjects in the Union, the Regulation will not apply to the respective processing[251]. Basically, it means that even though the processing of personal data occurred, however, on condition that there was no intention to target, the non-EU entity will not fall under the GDPR.

On the one hand, this, indeed, may be the case if, for example, a website of the non-EU controller or processor is accessible from the Member State and, by virtue of that, the website was accessed and a service was provided to the data subject located within the Union. However, since there was no intention to offer services to the individuals in the EU, the mere accessibility will not lead to application of the targeting principle. That is what the EDPB most likely implicates by referring to the situations when goods or services are provided unintentionally or accidentally.

On the other hand, the mentioned above observation from the EDPB does not seem to clarify anything or solve an issue. On the contrary, it raises even more issues. First of all, it exempts the non-EU controllers and processors from liability if they prove that the provision of goods or services took place unintentionally. As noted hereinbefore, this matter cannot be checked objectively. So, the non-EU entities are going to invoke the exemption every time when willing to escape the applicability of the targeting principle to them. Secondly, the grounds of exemption from liability – "inadvertently or incidentally provided" goods or services – create a loophole on default as long as the existence of the said grounds greatly depends on whether the non-EU entities themselves acknowledge the intention of offering. This is an additional argument for why the objective targeting including all respective objective evidences should have been focused on by the legislator and should always be checked in practice in order to determine whether Article 3(2)(a) applies to the processing.

3.5.3. Objective evidences of directing activities at the individuals in the Union

As previously noted, the concept of directing activities should be consulted when evaluating the evidences of offering goods or services to the data subjects in the Union[252]. Furthermore, in support of the given approach, Granmar suggests that in times of universal digitalization the concept of offering goods or services should mean the

[251] EDPB Guidelines, p. 18
[252] *Ibid*, p. 17

same as "directing commercial offers to consumers", implicating that the majority of offers are commercial[253]. Putting it this way, commercial offering equates to promotion which, in turn, brings it closer to targeting as a goal. Therefore, evidences used in the concept of directing of activities can be capable of affirming 'offering of goods or services' too, however, with a proviso.

First of all, judgment in *Pammer and Hotel Alpenhof joined cases*, which is a mine of information about evidences of directing and due to this should be consulted as the main and original source, was answering the question regarding activities directed *via a website*[254], while offering of goods and services, pursuant to Article 3(2)(a) GDPR, is *not limited* to the Internet offers. Secondly, as Advocate General Trstenjak has inferred in her Opinion, Article 15(1)(c) of Brussels I Regulation[255], which was interpreted by the CJEU in the cases mentioned above, implies that "an undertaking must direct its activities to a particular Member State and not to a particular group of consumers"[256]. By contrast, under Article 3(2)(a) GDPR, the activities are being directed to data subjects in the Union which can be defined particularly as a group of people, though referring to the whole Member State is not excluded.

As appears from the above, the GDPR has wider scope of application in comparison with *Pammer and Hotel Alpenhof joined cases*, i. e., it is applicable both to online and offline activities. In addition, unlike the interpreted provision, the Regulation allows directing activities not only to a certain Member State (meaning its residents) but also at certain groups of people within the Union. These observations allow inferring that practically all indices of directing that were addressed in the judgment as well as in Opinion of Advocate General can to certain extent be applicable to concept of offering within the meaning of Article 3(2)(a) GDPR, though the EDPB has selected not all of them to include into Guidelines.

Furthermore, there may be other evidences of directing the existence of which is conditional on objective impossibility to foresee everything, so, in any case, the list of indices is not exhaustive[257]. It is worth noting that the availability of just one evidence may be insufficient to ascertain a non-EU controller's intention of offering goods or

[253] Granmar 2019, pp. 36-37
[254] Pammer and Hotel Alpenhof joined cases, para 24(2)
[255] Article 15(1)(c) Brussels I Regulation: "[..] the contract has been concluded with a person who […] directs such activities to that Member State or to several States including that Member State […]"
[256] Opinion of Advocate General Trstenjak, para 82
[257] Pammer and Hotel Alpenhof joined cases, para 93

services to individuals in the Union, nevertheless, it will depend on the facts of a concrete case[258]. So, as a general recommendation, it is suggested that the more factors of offering are ascertained, the better. In the following paragraphs, this paper will contemplate possible evidences of directing, however, due to the limits of the paper, only those indices which require deeper analysis will be discussed in detail.

a) the use of a language or a currency of one or more EU Member States

If a non-EU controller uses on its website a language or a currency of one or more Member States of the Union, this fact may indicate that the said non-EU entity directs its activities to the EU data subjects. Ideal example of such evidence would be a language that is official only in one EU Member State and nowhere else, and spoken by relatively few people[259], such as Estonian or Latvian.

The use of a language or a currency can be put into effect either by means of writing the website in the particular language, i. e., the website's interface is available to users in certain language, or provision of the facility with the help of which the EU currency or EU Member State language can be switched to[260]. In addition to the said attributes, offering may be expressed through "the possibility of ordering goods and services"[261] or "making and confirming the reservation" using the said language and currency[262].

The use of a language

The EDPB's clarification that a language or a currency has to be "*other than that* generally used *in the trader's country*"[263] (emphases added) is inaccurate and too generalized since it suggests languages and currencies of *any* third countries with respect to the non-EU entity's country, including EU Member States, however, not only them. Thus, for the sake of clarity, it seems more rational to shift stress onto the condition that a language or a currency must be, first, of one of the EU Member States, and only then, second, different from that generally used one in the country where the non-EU entity is established. However, as will be shown hereinafter, the second condition may sometimes be absent.

[258] EDPB Guidelines, p. 18
[259] Opinion of Advocate General Trstenjak, para 82
[260] *Ibid*, para 83
[261] Recital 23 GDPR
[262] Pammer and Hotel Alpenhof joined cases, para 93
[263] EDPB Guidelines, p. 18

In the event when a generally used in a non-EU country language coincides with a language of the European Union, it becomes difficult to show the non-EU controller's intention of targeting individuals in the EU. For instance, in India, English has status of the subsidiary official language[264], while in the EU, English is one of the official languages in Malta and Ireland[265]. It appears from this that the Indian controller may potentially be considered directing its activities at data subjects in Malta or Ireland without being aware of it. However, the legislator has envisaged such situation by stating that "the use of a language generally used in the third country where the controller is established, is insufficient"[266] for rendering it as targeting the EU. Nevertheless, this does not mean that the non-EU controller will fall under exemption from the rule, – rather, additional evidences of directing will need to be provided.

On the surface, the analysed factor and its applicability do not cause difficulties. However, if to dig deeper, more questions arise. Recital 23 in the preamble to the GDPR defines the sai d index of offering as "the use of a language or a currency *generally used* in one or more Member States"[267] (emphasis added). At the same time, the Regulation does not explain when a language or a currency is considered 'generally used'. Presumably, it should be equated to 'official', thus, meaning official languages and currencies of the EU. If addressing the EDPB Guidelines on the matter, they interpret the said provisions as "a language or currency of one or more EU Member states"[268]. Notably, the Guidelines exemplify the situations in which only the official languages of the Union are concerned. Nevertheless, the formulation 'language of a Member State' suggests thinking that it means either the official language or any other language recognized at the national level of a Member State, e. g., the regional and minority languages. Though, this is only an assumption since it is neither affirmed by existing examples nor refuted by authorities.

Such conclusion derives also from the GDPR's orientation towards 'data subjects in the Union' who do not necessarily constitute the main population of a Member State. That is to say, referring to French people when addressing France or, by mentioning Germany implicating Germans only, is not true anymore. On the contrary, 'data subjects

[264] Department of Official Language, President's Order, 1960, Copy of Notification No. 2/8/60-O.L. (Ministry of Home Affairs), 27 April 1960. Available at: <www.rajbhasha.gov.in/en/presidents-order-1960>

[265] European Union, EU languages, 20 May 2020 – last published. Available at: <www.europa.eu/european-union/about-eu/eu-languages_en>

[266] Recital 23 GDPR

[267] *Ibid*

[268] EDPB Guidelines, p. 18

in the Union' can be a minority that does not even constitute the indigenous inhabitants of the country, but is its current population. So, on the basis of such logic, there are no obstacles for why not to understand the analysed provision as meaning 'languages spoken by people inhabiting a Member State'. Furthermore, as already mentioned hereinbefore, offering of goods and services may be addressed to a particular group of people in the Union.

In this respect, Karaduman exemplifies the situation when Turkish company, whose website is in Turkish only, targets Turkish-speaking individuals who live in Germany[269]. In Karaduman's view, despite the fact that Turkish is not the official language of the Union, the company still will be subject to the provisions of the GDPR[270]. This hypothetical case may actually be solved with either of the two following scenarios. According to the first one, the Turkish language *per se* cannot be considered appropriate language according to the Regulation since it is not one of the languages of the EU Member States in any case. So, there will be no targeting of data subjects in the Union established. Moreover, if to rely on the EDPB's Guidelines, Turkish is inappropriate *doubly* due to being a generally used language in the company's country which is Turkey. Pursuant to the second scenario, Turkish language still might be considered proper evidence, but only in combination with other weightier arguments of offering, if such are available. In this case, the non-EU language may serve as *a secondary, auxiliary evidence* which in combination with other factors would strengthen the established ones. In any event, Turkish language cannot be used as the only and independent evidence of offering. Finally, in the context of the instance at stake, it appears unreasonable that the EDPB excludes the use of a language generally used in the non-EU entity's country since, as just shown, situations when a website written in language A targets individuals in the Union who speak the same language A are more than feasible.

The use of a currency

As regards the use of a currency of one or more EU Member States, everything is more or less clear. Euro is the official currency of 19 EU Member States[271]. Thus, if a non-EU website indicates prices in euros or provides the possibility to choose currency from the

[269] Karaduman, Ozan, The General Data Protection Regulation: Achieving Compliance for EU and non-EU Companies. Business Law International, Vol. 18, No 3 (2017), 225-232, p. 226
[270] *Ibid*
[271] European Union, Which countries use the euro, 1 February 2020 – last published. Available at: <www.europa.eu/european-union/about-eu/euro/which-countries-use-euro_en>

list which includes euro in particular, this proves that the website is indubitably oriented towards customers from the Union.

Notably, euro is used also in few other European countries which are not members of the EU, such as Andorra, Kosovo, Montenegro, Monaco, San Marino and Vatican City[272]. Hence, in some cases, despite the use of euro, a non-EU entity may be targeting the *non-EU* individuals, – the circumstances need to be evaluated in the light of other evidences of directing. Nevertheless, it seems highly probable that the intentional targeting of the Union still might be confirmed because of the following factors: small size of the said non-EU countries, their neighbourhood to the Union, namely proximity to the eurozone, and, of course, the use of euro by them.

With respect to the other currencies of the European Union, they are not so widespread as euro, moreover, their usage is limited to one single country. For instance, Hungarian forint or Swedish krona are the official currencies only in the respective countries. Therefore, indication of such currencies by a non-EU entity would be a weighty argument for directing activities to a concrete EU Member State. Notably, the same concerns also if a non-EU website uses currencies of Iceland, Liechtenstein or Norway.

b) the use of a top-level domain name that refers to the EU or a Member State

The Guidelines provided by the EDPB are somewhat misleading due to their generalized formulation: "The use of a top-level domain name *other than that of the third country* in which the controller or processor is established, […]"[273] (emphasis added). This way, *any* third country with respect to a non-EU state is covered by the guideline, including EU Member States, however, not only them. To avoid ambiguity, this paragraph, as specified in the headline, will contemplate the use of a top-level domain name that refers to the EU or a Member State.

In general, a top-level domain *(hereinafter – TLD)* is the last part of a domain name, or, to be more precise, the letters in an Internet address which come after the final dot[274]. For instance, '.com', '.net', '.au', '.edu' etc. One of the purposes of a TLD can be indication of the geographical area where the website refers to. Therefore, a TLD may

[272] European Union, Use of the euro outside the euro area, 16 December 2019 – last published. Available at: <www.europa.eu/european-union/about-eu/euro/use-euro-outside-euro-area_en>
[273] EDPB Guidelines, p. 18
[274] Rouse, Margaret, top-level domain (TLD), April 2009 – last updated. Available at: <www.searchapparchitecture.techtarget.com/definition/top-level-domain-TLD>

potentially point out that certain offer of goods or services targets data subjects in the Union. However, of course, not any type of TLD is suitable for that.

Country-code top-level domain name

A TLD that identifies a particular country is called a country-code top-level domain *(hereinafter – ccTLD)*. It consists of two letters and corresponds to a country, territory, or other geographic location[275]. Each Member State of the EU has its own unique ccTLD name, e. g., '.fi' (Finland), '.se' (Sweden). Also, some territories of the EU, such as islands, have their own ccTLDs, e. g., '.ax' (Åland Islands), '.fo' (Faroe Islands). Interestingly, the TLD name '.eu' (EU) was set forth by the Internet Assigned Numbers Authority (IANA) on the ccTLDs list as well, though the EU is not a country[276]. In view of the aforesaid, both Member States' TLDs and EU's TLD belong to the category of ccTLDs. The List of ccTLDs[277] should be consulted when taking into consideration "the use of a TLD name" factor.

As Advocate General Trstenjak noted in her Opinion in *joined cases Pammer and Hotel Alpenhof*, the mentioning of the TLD name of a Member State clearly indicates that the entity directs its activities to the Member State whose TLD name it uses. This is especially relevant in cases when a legal person with its place of establishment in one country uses the TLD name of another country where it is not established.[278] Therefore, if, for example, an entity established in China sets up a website with the ccTLD name '.de', it is obvious that the entity addresses customers located in Germany.

Generic (geographic) top-level domain name

Besides ccTLDs, there may be other indicators of referring to the Member States – the generic TLDs that refer to the *cities* of the Member States, e. g., '.barcelona', '.berlin', '.helsinki', '.london', '.paris' and so forth. Though a city-level TLD *(hereinafter – clTLD)* does not embrace as many potential customers as a ccTLD does, nevertheless, first, it is easily recognizable since it usually copies the city's name in full, and, second, the cities using such TLDs are either capitals or other popular tourist destinations, which altogether actually makes the clTLDs *equally top* with ccTLDs. Therefore, it is

[275] ICANN, Resources for Country Code Managers. Glossary: Country-code top-level domain, 26 May 2020 – last visited. Available at: <www.icann.org/resources/pages/cctlds-21-2012-02-25-en>
[276] IANA Report on the Delegation of the .eu Top-Level Domain, March 2005. Available at: <www.iana.org/reports/2005/eu-report-05aug2005.pdf>
[277] The full list of ccTLDs can be found here: All of the world's top-level domains, 18 June 2019 – last updated. Available at: <www.norid.no/en/om-domenenavn/domreg/>
[278] Opinion of Advocate General Trstenjak, paras 84, 85

proper to give full weight to the clTLDs as well when considering whether offer of goods or services occurred.

There is one more group of geographic TLDs – the ones related to specific region of the EU and its culture. For instance, '.bzh' (Brittany, France) is intended for Breton language and culture, '.cat' (Catalonia, Spain) – for Catalan language and culture, '.irish' (Ireland) – for global Irish community[279] etc. Undoubtedly, the fact of using any of such TLDs speaks in favor of targeting people belonging to that specific local culture.

As just shown, generic (geographic) TLDs may also refer to certain Member States or territories. Therefore, the List of generic TLDs[280] should be consulted along with the List of ccTLDs, when taking into consideration "the use of a TLD name" factor.

Redirection

Irrespectively of the primary TLD name of the website, the latter still can be caught by the GDPR. This situation is possible, if the said website redirects customers located in the EU to the website with a TLD name that corresponds to their IP geolocation data[281]. For instance, a customer from Sweden visits the website 'example.com', however, he is redirected to 'example.com/se' which is a Swedish TLD name. In this case, the website has located the position of the customer and, since it has the separate TLD for Swedish users, the redirection occurred automatically. Alternatively, the redirection could happen manually, if the customer had a possibility of choosing or was offered to choose (e. g., by means of a pop-up window) his country from the menu of the website and so was redirected to 'example.com/se'.[282] In any case, having the separate TLD name for customers from the Member States speaks in favour of targeting data subjects in the EU by the non-EU based entities.

TLDs with commercial licenses

In fact, TLDs with commercial licenses are just that very way of how the non-EU companies obtain the EU-based TLDs. The said TLDs are opened to worldwide

[279] List of Internet top-level domains. Geographic top-level domains, 23 May 2020 – last edited. Available at: <www.en.wikipedia.org/wiki/List_of_Internet_top-level_domains#Geographic_top-level_domains>
[280] The full list of generic TLDs can be found here: Generic top-level domains (gTLD), 18 June 2019 – last updated. Available at: <www.norid.no/en/om-domenenavn/domreg/#gtld>
[281] Voigt – von dem Bussche 2017, p. 27
[282] *Ibid*, pp. 26-27

registrations for commercial use[283] and have no other connection with the country of origin of the TLD. For example, clTLD '.london' is officially opened not only to Londoners, but up to everyone[284].

Even though it seems obvious that a website using ccTLD of a certain country targets customers in that particular country, however, there is more here than meets the eye. According to Svantesson, sometimes, the choice of TLD is made in order "to achieve a play with words rather than as an attempt at attracting customers"[285] of the certain market. For instance, Spanish ccTLD '.es' may be used for forming plural words in the TLD names, e. g., 'parti.es', 'famili.es'[286]; Belgian ccTLD '.be' is used as a link shortener in the name of YouTube site 'youtu.be'[287], or simply for the literal term 'be' and so forth. In such cases, the non-EU based entity using Member States' TLDs cannot be considered to target the EU customers. Therefore, not only the TLD name itself has to be taken into account, but the whole Internet domain name as well, and, as Svantesson correctly noted, the true impact of the choice of TLD must be assessed[288].

c) the mention of geographical addresses or telephone numbers to be reached from an EU country

According to recital 23 in the preamble to the GDPR, "the mere accessibility of the […] website in the Union, of an email address or of *other contact details*" (emphasis added) is not sufficient to assert that the non-EU controller or processor intends to offer goods or services to data subjects in the Union[289]. Apparently, 'other contact details' implicate geographical addresses, telephone numbers and all other sorts of means of communication, mainly the Internet-based ones. Everything what concerns the Internet contact details, such as the email addresses, links to the social platforms or messengers, indeed cannot indicate the intention of offering since those contact details are universal and target everyone, not just the EU data subjects.

---

[283] Country-code top-level domains with commercial licenses, 17 May 2020 – last edited. Available at: <www.en.wikipedia.org/wiki/Country_code_top-level_domains_with_commercial_licenses>
[284] BBC News, .london web domain name goes on sale for first time, 29 April 2014. Available at: <www.bbc.com/news/uk-england-london-27193725>
[285] Svantesson, Dan Jerker B. Pammer and Hotel Alpenhof – ECJ decision creates further uncertainty about when e-businesses "direct activities" to a consumer's state under the Brussels I Regulation. Computer Law & Security Review, Vol. 27 (2011), 298-304, p. 301
[286] *Ibid*
[287] Make Way for youtu.be Links, 21 December 2009. Available at: <www.youtube.googleblog.com/2009/12/make-way-for-youtube-links.html>
[288] Svantesson 2011, p. 301
[289] Recital 23 GDPR

With respect to the addresses (in geographical meaning) and the telephone numbers, the situation is twofold. On the one hand, both are lacking an 'intention' feature, on the other hand, it depends on the format how they are provided. In general, addresses and telephone numbers can be either in a simplified format, or in an international one. While in a simplified version only the name of the city and the street address are sufficient since such address is obviously oriented towards the locals, the preconditions of the international format include the country's and the district's or region's names along with the postal code in addition, thus, allowing people from different corners of the globe to find it. Thereby simplified version of a geographical address surely cannot be deemed as targeting the EU data subjects. As regards an international address, it *per se* potentially aims at the whole world, however, whether it particularly targets the Union has to be evaluated together with other existing factors of directing activities since taken alone it would be, though appropriate, but insufficient evidence.

A much alike system takes place in case of telephone numbers. Each country has its own international calling code[290] with a help of which the international calls are possible. By analogy with addresses, if a telephone number is provided in a shorter format usable for local calls only, then, apparently, a non-EU controller or processor expects calls from the same country or city where it is established. However, the international format of the telephone number speaks in favour of offering goods or services to customers from abroad – very likely, including the EU data subjects as well, which must be assessed in combination with other factors.

Notably, recital 23, which is set forth above, does not specify what format of 'other contact details' are implied, i. e., simplified (short) or international ones, – rather, it stresses on the insufficiency of evidence if just one factor is present. Nevertheless, the EDPB interprets the said recital as if meaning insufficiency in case of a "telephone number without an international code"[291]. This explanation suggests an idea that, on the contrary, a telephone number *with* an international code would be considered sufficient evidence of offering. However, as shown above, it will not be so since other suitable factors must be at place as well. It seems that the EDPB has taken the given citation out

[290] *See*, for instance, International Calling Codes, 26 May 2020 – last visited. Available at: <www.internationalcitizens.com/international-calling-codes/>
[291] EDPB Guidelines, p. 18

of context from judgment in *Pammer and Hotel Alpenhof joined cases*[292], in which it actually makes sense, and misled into thinking of ambiguity in the Regulation.

Nevertheless, it should be observed that another EDPB's clarification is right to the point – it has suggested putting the factor under consideration more specifically into the EU plane, namely by construing it as "[t]he mention of dedicated addresses or phone numbers to be reached from an EU country"[293]. That is to say, if a non-EU controller or processor assigns, for example, a separate telephone number for calls from the territory of the Union, that will be an incontroverted evidence of targeting the EU data subjects. The same concerns the mention of address where specifically the EU customers are served.

In spite of the fact that the EDPB for some reason avoids acknowledging the international format of contact details as an appropriate evidence of offering, there are no obstacles to its acceptance. Moreover, international format of telephone numbers, in particular, was recognized admissible evidence of 'directing activities' in *Pammer and Hotel Alpenhof joined cases*[294] that have served as a basis for criteria of offering within the meaning of the GDPR. So, there are two cases when a non-EU controller's or processor's geographical address or telephone number may indicate an intention to offer goods or services to the data subjects in the Union: contact details either in an international format or specifically dedicated to data subjects from the EU. Even though it seems obvious that the second case would be a stronger evidence of offering, however, both examples may equally serve in proving offering.

d) other evidences of directing

There are many other factors of directing activities at the data subjects in the Union, and, as already noted, the list is not exhaustive. Some of them are contemplated hereinafter.

Naturally, when a non-EU controller directly states on the website that its business activities are oriented towards the EU market, or if it designates by name a Member State or the EU in general, notably "with reference to the good or service offered"[295], then undoubtedly its offering activities target the EU. By virtue of specifying the target

[292] Pammer and Hotel Alpenhof joined cases, para 77
[293] EDPB Guidelines, p. 18
[294] Pammer and Hotel Alpenhof joined cases, para 93
[295] EDPB Guidelines, p. 17

groups of consumers, the non-EU entity confirms that it targets objectively as well as demonstrates its intention via the subjective targeting. Also, if the EU Member States are listed among the countries where the non-EU controller delivers goods to, the possibility of delivery to the Union clearly indicates that the offers are directed to the EU Member States[296].

Not only the particular EU countries can be indicated as the target audience, but also the specifically mentioned customers and users in the Union[297], as already discussed in paragraph 3.5.2 (a) of the paper hereinbefore. There are various indices showing that the non-EU entity engages in transactions with the European customers. For instance, "presentation of accounts written by such customers"[298] demonstrates that those individuals have registered their accounts on the website and, thus, sent their personal data, or publication of testimonials written by the EU customers[299] shows that the non-EU entity has previously offered goods or services to the customers from the Union. The much alike role would play the customers' reviews of the products left on the website. Also, Advocate General Trstenjak considers that provision of the "facility […] to subscribe to a newsletter about the goods and services offered" serves an indicator that the non-EU entity "consciously [works] towards concluding distance contracts with consumers"[300]. In fact, subscription to a newsletter is a half way for a non-EU entity towards conclusion of a contract with a consumer, but what is more important, it is already acknowledged as an directing of its offers at the EU individuals.

The EDPB takes the same view as the CJEU[301] and considers that the international nature of the non-EU entity's activities, especially tourist activities, may be taken into consideration when evaluating factors of directing[302]. Trstenjak does not object to what regards tourist activities, however, suggests that the type of activities in general cannot be a determining factor, therefore, the activities should be evaluated without prejudice to their nature, for instance, craft activities do not necessarily target only customers living in the nearby areas[303] since products of craft activities can be delivered to the Union. So, in fact, any type of activities can be considered international if it allows reaching people in the EU.

[296] EDPB Guidelines, p. 18
[297] Recital 23 GDPR
[298] Pammer and Hotel Alpenhof joined cases, para 83
[299] Opinion of Advocate General Trstenjak, recital 59
[300] *Ibid*, para 78
[301] Pammer and Hotel Alpenhof joined cases, para 93
[302] EDPB Guidelines, p. 17
[303] Opinion of Advocate General Trstenjak, para 87

If a non-EU entity provides guidance, namely itineraries, on how an EU individual can get from a particular Member State to the place where the service offered by the said entity is provided[304], then such entity works actively and intentionally towards targeting the EU customers. The guidance may include various travelling instructions, for example, how to get from the airport to the city in the non-EU country of destination.

Last, but not least, are evidences of directing aiming at promotion of the non-EU controller's or processor's activities in order to reach the EU market. Such evidences envisage "marketing and advertisement campaigns"[305] of every sort and kind, including advertising by means of the Internet, television, radio, newspapers and so forth[306]. Also, the CJEU considers expenses on an internet referencing service relevant in the situations when a non-EU controller or processor pays for making its website accessible for the customers from the Union; such promotion clearly demonstrates the non-EU entity's intention of targeting the EU individuals[307].

3.6. Monitoring data subjects' behaviour in the Union

3.6.1. The concept of monitoring

The monitoring criterion is an innovative concept in the applicability of EU data protection law[308], and, despite the skepticism regarding its effective operability[309], it has already made the breakthrough by extending its sphere of influence onto the whole Internet. Furthermore, the scope of monitoring criterion is even broader than the offering of goods or services criterion since it is likely to cover all sorts of online as well as offline activities[310]. Indeed, the wording of Article 3(2)(b) GDPR allows inferring that the offline behaviour is not excepted from the provision. Nevertheless, as de Hert and Czerniawski rightly observe, the monitoring criterion was primarily projected to capture "third country operators of social networks, online providers of services such as e-mail accounts, operators of search engines and websites", many of

[304] EDPB Guidelines, p. 18
[305] *Ibid*, p. 17
[306] Opinion of Advocate General Trstenjak, para 89
[307] Pammer and Hotel Alpenhof joined cases, paras 81, 93
[308] Gömann 2017, p. 587
[309] *See*, e. g., Tene, Omer – Wolf, Christopher, Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation. The Future of Privacy Forum White Paper, 2013, pp. 2-4, 10; Gömann 2017, p. 588
[310] Svantesson 2019, p. 11

which monitor the users' behaviour on the Internet on continuing basis[311]. Finally, since Article 3(2)(b) GDPR captures wider range of grounds for the applicability of the Regulation, it will most likely catch those non-EU operators who target the EU, however, managed to bypass the grounds found in Article 3(2)(a) GDPR.

The monitoring criterion is stipulated in Article 3(2)(b) GDPR which states that a non-EU controller or processor can be subject to the Regulation provisions if its data processing is related to the monitoring of the data subjects' behaviour *"as far as their behaviour takes place within the Union"* (emphasis added)[312]. By putting it this way, the legislator expressly excludes the cases where there is insufficient link between the non-EU operator's processing activities and the Union. That is to say, the monitoring criterion cannot apply to the processing, for example, simply on the basis that it is related to an EU resident[313]. In this context, the EDPB clarifies that "the behaviour monitored must first relate to a data subject in the Union and, as a cumulative criterion, the monitored behaviour must take place within the territory of the Union"[314]. As it follows, the *monitored behaviour* is brought into the forefront since it appears as a common denominator of a data subject in the Union and the place where the behaviour occurs.

Recital 24 in the preamble to the GDPR states that for the finding that the processing "can be considered to monitor" the EU data subjects' behaviour, it is necessary to inquire into "whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques"[315]. Thus, the Regulation regards monitoring as an activity which envisages the data processing. Furthermore, as previously stated in paragraph 3.4.3 of the paper hereinbefore, monitoring as such consists of *targeting* as well as data processing[316], so, monitoring cannot be considered separately from these elements.

With respect to the EDPB, it focuses on the subjective part of the explanation and defines 'monitoring' as meaning that "the controller has a specific purpose in mind for the *collection* and subsequent *reuse* of the relevant data about an individual's behaviour

[311] de Hert, Paul – Czerniawski, Michal, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, Vol. 6, No. 3 (2016), 230-243, p. 238
[312] Article 3(2)(b) GDPR
[313] de Hert – Czerniawski 2016, p. 238
[314] EDPB Guidelines, p. 19
[315] Recital 24 GDPR
[316] *See* 3.4.3. Temporal scope of stay in the Union

within the EU"[317] (emphases added). Leaving aside at this point the types of activities that the said explanation implies, it is suggested to examine 'monitoring' from the data processing perspective[318]. Even though 'monitoring' is not found in the list of processing operations set out in Article 4(2) GDPR, nevertheless, it seems obvious that it should be there. As stated above in the definition, monitoring consists of the collection and reuse of personal data, both of which refer to the data processing operations[319]. So, basically, 'monitoring' is a *compound operation* that includes two steps: first, collection of data and, second, its subsequent use (or reuse). This ascertainment allows considering monitoring not only as a targeting activity, but also as a full-fledged processing, bearing in mind that it consists of two indispensable steps.

In some forms of monitoring, there may be additional, that it to say interim, steps presented. For instance, in the illustration of profiling activities, provided in Recommendation of Council of Europe, it was clarified that profiling includes *three* stages: first, data collection and storage that altogether constitute data warehousing, second, automated analysis in order to identify correlation between various behaviours – a so-called 'data mining', and, third, applying the correlation results to a particular data subject in order "to deduce some of his or her past, present or future characteristics"[320]. Thus, using the terminology of the Regulation, namely the list of processing operations set out in Article 4(2) GDPR, profiling as a form of monitoring involves collection, storage and various forms of data use, such as organization, combination or any other similar forms.

Azzi additionally clarifies the question by noting that the concept of monitoring is conditional on the definition of 'personal data' provided in the Regulation, which implicates in particular "personal preferences, interests, location or movements"[321] etc. In other words, only what refers to 'personal data' and constitutes the data subjects' behaviour can be monitored. Due to the major focus of the GDPR on the Internet users' activities with the respective monitoring of their behaviour (the so-called 'surfing

[317] EDPB Guidelines, p. 20
[318] *See* also 3.4.2. Spatial scope of stay in the Union and 3.4.3. Temporal scope of stay in the Union
[319] Article 4(2) GDPR
[320] Council of Europe, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum, adopted 23 November 2010, recitals 38, 96-98
[321] Azzi, Adèle, The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation, Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 9, Issue 2 (2018), 126-137, recital 28

behaviour'[322]), it is obvious that new types of personal data come to the foreground. In this respect, the Regulation singles out the category of online identifiers, among which internet protocol (IP) addresses, cookie identifiers and radio frequency identification (RFID) tags, since all of them can be utilized for profiling[323] of the EU individuals.

Summarising all the aforesaid explanations of the scope of monitoring, it appears that the concept is quite broad, and various provisions and clarifications complement each other. As a result, monitoring appears to refer to all possible types of activities, – both online and offline, – which lead to tracking of individuals in the Union and envisage "potential subsequent use of personal data processing techniques"[324].

3.6.2. Monitoring requires an intentional purpose

Passing ahead the then-forthcoming clarification from the EDPB, Svantesson rightly observed that unlike Recital 23 (corresponding to Article 3(2)(a) GDPR), which helpfully ascertains that the criterion of offering goods or services *requires intention* on the part of a non-EU controller or processor, neither Recital 24 nor any other part of the Regulation "include any expressed such requirement in relation to Article 3(2)(b)" GDPR[325]. Indeed, related to Article 3(2)(b) Recital 24 is silent about any subjective components of monitoring on the part of non-EU operators. Therefore, logically, it is possible to assume that since the content of recitals differs, so is their meaning: under Article 3(2)(b) GDPR, an "unintentional monitoring *may* be caught" too[326] (emphasis added). As regards *intentional* monitoring, it, undoubtedly, is subject to the Regulation irrespective of whether this is directly specified so or not. Elaborating on the issue, Svantesson further suggests that unintentional monitoring may take place when a non-EU entity is not going to apply any data processing techniques to the collected data related to individuals in the Union[327], that is to say, the first step which is collection occurred, however, since no subsequent use featuring monitoring activities is intended, the monitoring criterion cannot be applied. Without other clarifications available, this,

[322] Moerel, Lokke, The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? International Data Privacy Law (2011), Vol. 1, No. 1, 28-46, p. 28
[323] Recital 30 GDPR
[324] Recital 24 GDPR
[325] Svantesson 2019, p. 11
[326] *Ibid*
[327] *Ibid*

indeed, could make sense. However, as shown below, data processing activities under the given circumstances of the case cannot be deemed as monitoring.

Admitting the legislator's omission, the EDPB has cleared up the confusion. It agreed that none of the provisions "*expressly* introduce[s] a necessary degree of "intention to target""[328], thereby probably implicating that it is necessary to read between lines or even think unconventionally (emphasis added). Following the EDPB's logic, an intention to target was actually *implicated*, but introduced vaguely. In any case, the issue was resolved by providing the definition of 'monitoring' which was discussed hereinabove, but this time its another part will be contemplated closely: "the use of the word "monitoring" implies that the controller has a *specific purpose in mind* for the collection and subsequent reuse of the relevant data […]"[329] (emphasis added). Taking into account all the above-stated, it appears that for the applicability of the monitoring criterion it is required that a non-EU entity envisages not just a purpose, but *an intentional purpose*, which is different from the former.

Interpretation in such light clarifies why Svantesson's conjecture is partly inaccurate – monitoring must actually be *intentional by default*, and the lack of will to further use the data processing techniques to the collected data demonstrates the absence of intention to monitor, which has to be present on the whole way of monitoring activities. Therefore, for instance, passive, i. e., without intention, continuing collection of data regarding the natural persons' behaviour within the Union will not present monitoring[330].

Complications with intentional purpose of monitoring do not come to an end at this point. Recital 24 in the preamble to the GDPR explains that in order to ascertain that a non-EU entity monitors the individuals' behaviour within the Union, two things need to be established: first, data subjects tracking on the Internet, and, second, "potential subsequent use of personal data processing techniques" that envisage profiling of the data subjects[331]. While feasibility of the first condition is technically possible, the second one is more problematic. If the use of data has already occurred, then there will be evidences of profiling – the profiles on data subjects. However, how to check *potentiality* of subsequent data use remains unclear. Gömann argues that such construction concerns the subjective intentions of a non-EU entity; as a result, whether

[328] EDPB Guidelines, p. 20
[329] *Ibid*
[330] Bird & Bird, Guide to the General Data Protection Regulation, p. 8
[331] Recital 24 GDPR

the fact of monitoring will be established or not, depends on the non-EU operator's desire to advance processing to the stage of data use[332]. Without further clarification from the authorities, the mere availability of data processing techniques at the disposal of a non-EU data controller may lead to the conclusion that it could potentionally use them for monitoring activities. Alternatively, it seems rational to take the same approach which is used in application of offering criterion, that is to say, ascertaining whether a non-EU entity actively demonstrates its intention to target – here: to monitor – individuals in the Union.

Though namely 'purpose' is a distinctive element of the monitoring, it is important to remember that monitoring is a form of targeting, therefore, nothing targeting is alien to monitoring. To put it differently, the latter has adopted all attributes of targeting, in particular 'targeting as a goal'[333]. So, intention to target is an equally important precondition under both offering criterion and monitoring criterion.

Purposes for which the non-EU controllers monitor the data subjects' behaviour in the Union vary. Often they are marketing or advertising and they are directly dependent on the monitoring activities. Neither GDPR, nor EDPB Guidelines define the purposes of monitoring as such, however, some clarification they do provide. For instance, profiling aims at *making decisions* regarding a particular data subject or *analyzing* or *predicting* "personal preferences, behaviours and attitudes"[334]; or another example: a non-EU "controller has a specific *purpose* […] *for the collection* and subsequent *reuse*" of personal data[335] (emphases added). The italicized factors are actions that accompany and at the same time serve as interim steps towards the ultimate goal which is conditional on the factual purpose of monitoring. In other words, activities, such as decision-making, analysis, prediction, collection, reuse etc. help non-EU operators to realize their real intentions.

Gömann deems that, due to all difficulties with ascertaining the targeting features of monitoring, it will turn out to be merely "a declaration of political intent" in practice[336]. Nevertheless, the ICO proved it to be different. It initiated the first enforcement action under the GDPR against a data controller based outside the Union which took place on 24 October 2018. Notably, this was clearly the case when the company had no physical

[332] Gömann 2017, p. 587
[333] *See* 3.2. The concept of targeting
[334] Recital 24 GDPR
[335] EDPB Guidelines, p. 20
[336] Gömann 2017, p. 588

presence, i. e., establishment, in the EU at all. The UK Information Commissioner's Office (ICO) accused the Canada-based company *AggregateIQ Data Services Ltd (AIQ)* of unlawful using of personal data of the UK data subjects for the purposes of targeting them "with political advertising messages on social media"[337], so far as this way *AIQ* monitored the behaviour of individuals in the EU. The case included two Enforcement Notices from the ICO. The first Notice contained the reference to Article 3(2)(b) GDPR as the grounds of the Regulation's applicability to the processing carried out by *AIQ*[338]. However, in the revised version of the Enforcement Notice, which was aimed at clarifying "the steps to be taken by AIQ", the said reference to Article 3(2)(b) GDPR was removed[339] for unspecified reason. Nevertheless, this amendment does not seem to have changed the grounds the Enforcement Notice was issued against *AIQ* on.

It may be argued that enforcement notice is just an act of warning. However, the notice informs about the essence of infringement and notifies that, in case of failing to comply with it, Comissioner may serve a penalty notice next. So, as it follows, monitoring criterion is actually operational.

3.6.3. Monitoring activities

Recital 24 in the preamble to the GDPR provides somewhat misleading guidance since, in the context of contemplating what activities the monitoring consists of, the legislator confined itself to mentioning only tracking on the Internet[340]. However, as Ustaran rightly observed, there are no grounds to consider that the monitoring cannot concern other examples as well, at least due to the fact that the "EU data protection law is meant to be technologically neutral"[341]. Indeed, as the EDPB later defined more precisely, "tracking through other types of network or technology" used in "wearable and other smart devices"[342] may also amount to monitoring. The specification that monitoring is applicable not only to online behavioural monitoring, but to offline in particular, once again confirms how all-embracing the monitor criterion proves to be. Also, as Granmar

[337] The Information Commisioner's Office, Enforcement Notice to AggregateIQ Data Services Ltd ("AIQ"), The Data Protection Act 2018, Part 6, Section 149, dated 24 October 2018. Available at: <www.ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf>, para 6

[338] The Information Commisioner's Office, Enforcement Notice to AggregateIQ Data Services Ltd ("AIQ"), The Data Protection Act 2018, Part 6, Section 149, dated 6 July 2018. Available at: <www.ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf>, para 2

[339] The First Enforcement Notice to AIQ, dated 24 October 2018, para 2

[340] Recital 24 GDPR

[341] Ustaran 2013, p. 155

[342] EDPB Guidelines, p. 19

noted, this brings the monitoring applicability to the non-EU controllers and processors outside the framework of e-commerce[343].

Based on the purposes and aims that are pursued, and taking into account the methods that a non-EU entity applies in order to monitor data subjects' behaviour in the Union, its data processing activities can be referred either to mapping, tracking or profiling activities. Notably, due to the rapid changes in the information society that take place continuously, it is not reasonable to consider existing monitoring activities as the ultimate ones. Therefore, it is suggested to regard the list of monitoring activities provided in the EDPB's Guidelines[344] (which will be discussed hereinbelow) as an approximate list orienting us in the technological world.

a) geo-localisation activities

Geo-localisation is an extremely widespread monitoring activity due to the availability of Wi-Fi technology in practically all modern smartphones, tablets and other portable electronic devices. By using geo-localisation technology, a non-EU operator aims at determining the exact location of a data subject in order to, e. g., offer him or her the close by services. Geo-localisation is a good example of how monitoring works: first, a non-EU entity collects personal data of an individual in the Union through Wi-Fi tracking, afterwards, data is processed – most likely for the marketing purposes[345] of the said entity, and, finally, if the purpose of monitoring is marketing, the respective advertisements or offers will be sent to the data subject.

b) CCTV (video surveillance)

Monitoring by means of CCTV (or closed-circuit television) envisages that when individuals happen to be in the field of view of video surveillance facilities, they are filmed. Notably, not any kind of such video recording is considered as monitoring, – the necessary requirement is that the natural persons have to be "identified or otherwise singled out"[346] in the result, otherwise monitoring is useless if it is not known what exactly person is being surveyed.

[343] Granmar 2019, p. 40
[344] EDPB Guidelines, p. 20
[345] *Ibid*
[346] Korff 2019, p. 49

c) online tracking through the use of cookies or fingerprinting

Cookies and fingerprinting as the technologies for online tracking have much in common, therefore, it seems reasonable to discuss them jointly. Both cookies and fingerprinting refer to the device identification which, in turn, leads to a natural person who uses the said device, that is to say, a so-called 'device identifier'. As a result, the user's behaviour is being monitored every time when a person visits the website which has stored the indentifier onto device.

It is worth noting that not all categories of cookies are covered by the monitoring criterion: the strictly necessary cookies, which are indispensable for normal functioning of a website, are *a priori* excluded. They are often session cookies and their life is conditional on the time of visit of a website, therefore, they do not collect any data that could be used by a non-EU controller in future. However, as regards preference, statistics, marketing, third-party or any other categories of cookies which imply purposeful targeting of the data subjects in the Union, they clearly indicate intention and purpose on the part of a non-EU operators to monitor individuals, so monitoring criterion will apply.

Even if a non-EU controller does not utilize cookies (which is unlikely, though), it can still monitor the data subjects' behaviour through the identification of user's browser, which is also known as 'browser fingerprinting'[347]. The thing is that browsers send huge amount of data to the service providers "to enable an optimized display of [the] website, such as type and version of the browser, the operating system, installed plug-ins […], language, header and cookie settings, the used monitor resolution and time zone"[348]. Though the listed types of data speak in the first place of technical features of the browser and have little to do with the data subject as such, nevertheless, the browser fingerprint generated on their basis may, *in combination* "with additional information such as IP addresses", allow identification of the website user[349].

[347] Skouma, Georgia – Leonard, Laura, *On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection* in: Gutwirth, Serge – Leenes, Ronald – de Hert, Paul (eds.), *Reforming European Data Protection Law*. Springer Science+Business Media Dordrecht, 2015, 35-60, p. 41

[348] Alich, Stefan – Voigt, Paul, Mitteilsame Browser – Datenschutzrechtliche Bewertung des Trackings mittels Browser-Fingerprints, Computer und Recht, Vol. 28, Issue 5 (2012), 344-348, pp. 344, 345 in: Voigt – von dem Bussche 2017, p. 27

[349] Alich – Voigt 2012, pp. 344, 346-347 in: Voigt – von dem Bussche 2017, p. 27

d) behavioural advertising

Given activity envisages that a non-EU entity conducts monitoring of the individuals in the Union for the purpose of behavioural advertising. In essence, it means that a non-EU operator analyses data subjects' behaviour and on the basis of their preferences directs respective advertisements to them. This activity may embrace various forms of monitoring, including, but not limited to, online tracking, geo-localisation, profiling, since the range of sources where behavioural data can be get from is, roughly speaking, unlimited.

Ustaran finds it controversial that the monitoring criterion may apply to the behavioural advertising even in the cases where the data subjects' personal data are not compromised, exemplifying the situation in which an Internet user simply receives an ad which corresponds to his or her browsing patterns and interests; scholar argues that it is common practice that aims at providing "an ad about one particular product or service instead of another"[350]. In theory, it could be so, if a non-EU entity had altruistic goals instead of marketing ones. However, it seems more probable that nowadays most of the companies, if not themselves, then through the third parties, use, reuse and sell personal data. In this respect, Skouma and Leonard consider that what operators indeed do with data is 'invisible' to data subject and beyond his or her control since the processing includes many unknown puzzles, – especially this concerns the non-EU processors and various recipients of data[351].

e) market surveys and other behavioural studies based on individual profiles

The key purpose of the monitoring activity under consideration lies in its name – marketing. The studies or surveys related to the behaviour of individuals in the Union can be executed using both online or offline activities. They may include interviews of the data subjects, various forms of questionnaires or surveys, analyses of shopping behaviour through the customer database and so forth.

Importantly, the subsequent analysis of data subjects' behaviour must be based on their existing *individual profiles*, or, in case of processing the personal data of new clients, such processing has to lead to the creation of a profile; as Korff states, the fact that a

[350] Ustaran 2013, p. 155
[351] Skouma – Leonard 2015, p. 47

profile is created is the best evidence that the data subject is being monitored[352]. Moreover, profiling has to evaluate *individual* characteristics of a person[353] which uniquely describe the said person and allow distinguishing him or her from other data subjects. So, as just shown, for the applicability of monitoring criterion on the grounds of market surveys and other behavioural studies, the behaviour of each particular individual has to be analysed separately so that the said person can be identified.

By contrast, if to apply the same activities, for example, to the EU market and analyse it as a whole, the monitoring criterion will not be invoked. The WP29 has provided helpful guidance in this respect. It clearly stipulates that, if a non-EU operator conducts "simple classification of individuals based on known characteristics such as their age, sex, and height", such activities do not necessarily constitute profiling [354]. That is to say, if a non-EU entity pursues a goal to classify data subjects purely "for statistical purposes" and does not intend to make any predictions about them, this will result in "an aggregated overview"[355], by contrast to *specific* individual profiles.

There are other circumstances of behavioural monitoring under which a non-EU entity will not fall under Article 3(2)(b) GDPR. Skouma and Leonard particularly single out *anonymous* tracking of the website users, which in practice allows avoiding use of personal identifiers[356]. Also, collected personal data of the data subjects in the Union may be de-identified or, as discussed above, aggregated[357]. In all specified instances, the idea is that the collected data has to lose its ability to connect particular individual and the information about him or her, or to be unable by default to do that.

f) other monitoring activities

The EDPB singles out also "personalised diet and health analytics services online" and "monitoring or regular reporting on an individual's health status"[358] as the monitoring activities, – obviously, for the reason of concerning sensitive data. Besides including special category of data, these types of monitoring activities do not have other peculiarities distinguishing them from the above contemplated activities. Thus, most of

[352] Korff 2019, p. 49
[353] WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN, WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, p. 7
[354] *Ibid*
[355] *Ibid*
[356] Skouma – Leonard 2015, p. 48
[357] *Ibid*
[358] EDPB Guidelines, p. 20

the probability, they were singled out in order to emphasize on the applicability of monitoring principle to them, in case some non-EU entities are going to prejudice this.

While defining concretely one monitoring activities, the EDPB has skipped some other which are not less important. For instance, it did not mention monitoring of the behaviour in relation to "anti-money laundering checks, email monitoring in the employment context and fraud prevention"[359], while the latter, indeed, deserves separate consideration.

Fraud prevention

It is a global practice that banks monitor the use of the bank cards issued to their clients, particularly for the purpose of fraud prevention, especially closely "when they travel abroad"[360]. Of course, this is true for the non-EU banks as well. In this context, Korff exemplifies the hypothetical situation when a holder of a bank card (resident of the third country), which was issued by the non-EU bank, travels to one of the Member States of the Union, and the use of the said card in the territory of the EU is monitored by the non-EU bank (the issuer)[361]. As it follows, unexpectedly, but many facts of the case speak in favour of the application of Article 3(2)(b) GDPR. Firstly, the non-EU bank acts as a non-EU controller of the data processing. Secondly, the holder of the bank card is not a resident of the Union, however, this does not matter since at the moment of monitoring he was in the territory of the Union. Thirdly, the non-EU bank had clear purpose for monitoring – to prevent fraud – and intention to do so. And so forth. However, Korff rightly argues that despite all pros, the situation causes disproportionate difficulties in practice since it binds the non-EU bank to comply with the GDPR provisions, thus, the question is undecided[362].

The problem lies in the subjective component of the monitoring. The non-EU bank, indeed, had the purpose to prevent fraud by means of monitoring how its customers use the bank cards. On the one hand, it, most likely, did not mean to monitor them while they travel in the Union. However, on the other hand, since the nature of the monitoring activity at stake included the monitoring of the cards usage *abroad*, perhaps in the EU, the non-EU bank should have foreseen such probability. So, the question which is left opened is: 'Did the non-EU bank *purposefully intend* to monitor the use of bank cards

[359] Bird & Bird, Guide to the General Data Protection Regulation, p. 8
[360] Korff 2019, p. 20
[361] *Ibid*, p. 21
[362] *Ibid*, p. 49

realizing that its processing activities will concern monitoring in the Union?' If the answer is 'yes', then the bank is subject to Article 3(2)(b) GDPR; if 'no' – it might avoid the applicability of the monitoring criterion to its activities.

3.7. Gap in Article 3 GDPR

Arguably, there is a scenario that is not covered by either part of Article 3 GDPR (and not even by part 3(3) which is not contemplated in the paper). The hypothetical issue raised by Jay concerns the situation when the conditions stipulated in parts 1 and 2 of Article 3 GDPR are mixed so that neither can be applied[363]. This may potentially be the case if, for example, a US-based company that offers goods or services to data subjects in the Union or monitors their behaviour (does not really matter) *has an establishment in the EU* for lobbying purposes, and, importantly, that is the only presence that the US company has in the Union[364]. Indeed, the GDPR does not envisage such a combination of facts.

The establishment principle cannot be applied here since, even though the non-EU company has the establishment in the EU, the processing is not carried out in the context of the activities of the said establishment – data processing based on targeting and monitoring activities lies too far from lobbying activities. Highly unlikely, depending on the other facts of the case, an inextricable link required under Article 3(1) GDPR may be proved. However, under available facts, that is impossible.

As for the targeting principle, the required activities, such as offering or monitoring, are at place. However, the fact that the US company is presented through the establishment in the Union sits uncomfortably with the key provision of Article 3(2) GDPR which stipulates that the non-EU controller or processor has to be *not established* in the EU. Thus, the targeting principle is dismissed, too.

It would be unreasonable in such situation to completely avoid the GDPR application to the data processing, especially if it concerns the data subjects in the Union[365]. Therefore, Jay considers that the European data protection authorities would interpret the GDPR provisions "teleologically rather than literally" and read Article 3(2) GDPR as follows: "This Regulation applies to the processing of personal data *by a controller or processor in the context of an establishment of the controller or processor outside the Union*,

[363] Jay 2017, section 21-015
[364] Korff 2019, pp. 21-22
[365] Recitals 23, 24 GDPR

where the processing activities are related to [the offering of goods or services to, or the monitoring of the behaviour of, data subjects in the Union]"[366] (the differing from the original text part in italics). This way, Jay has omitted that part of the provision which prescribes that a controller or processor is not established in the Union. So, in such interpretation, it *can be established*, and that fact would not affect the applicability of Article 3(2) GDPR. Such a solution is rather controversial since it concedes the probability of overlapping with the establishment principle and, thus, whittles away the distinction between Article 3(1) and 3(2) GDPR.

Nevertheless, the said solution deserves justification. As stated above, on the basis of processing personal data of the data subjects in the Union, data protection law must guarantee them protection. So, the lack of a suitable provision applicable in the specific case is not an argument of depriving data subjects in the Union of their right to protection. If choosing between the establishment and targeting principles, the latter gains an advantage. And that is obvious: the EU establishment is the only physical presence in the Union, it merely conducts lobbying activities and, presumably, does not contribute to data processing. On the contrary, the US establishment (possibly there are other establishments in the US as well) is a parent company, it definitely targets data subjects in the Union, processes their data and, moreover, does so in the context of the same establishment. So, if to weigh the arguments, the US company has much more to do with the data processing than its European subsidiary. Thereby, in the event discussed above, the Regulation would still apply to the data processing and, despite having features attributable to different parts of the provision, Article 3(2) GDPR is most likely to be applied in the teleological interpretation.

[366] Jay 2017, section 21-015

IV. CONCLUSIONS

There are two general criteria of the GDPR applicability to the data processing activities performed by a non-EU controller or processor – the establishment principle (Article 3(1) GDPR) and the targeting principle (Article 3(2) GDPR). Both criteria are based on the explicit links with the EU – either through having establishment in the Union or targeting individuals in the territory of the EU. Applicability concerns one specific processing operation or set of operations of the same non-EU operator, thereby applicability of the Regulation in one case does not entail the applicability to the rest of processing activities of the same entity – each case requires separate consideration.

In order to ascertain that a non-EU entity is subject to the GDPR, conditions stipulated under either the establishment principle (including establishment test) or the targeting principle (coincides with targeting test) must be met. Application of both tests at once to the same non-EU controller or processor is impossible since application of one test excludes applicability of the other. Whatever the circumstances of the case, establishment test has to be checked first, and only in the event of its inapplicability, the conditions of targeting can be tested.

The establishment test allows ascertaining availability of an establishment in the EU by means of determining whether a non-EU controller or processor executes an activity through stable arrangements in the Union and whether the activity is real and effective, after that the activity has to be evaluated in the light of its nature and the services provided. In order to invoke Article 3(1) GDPR, processing has to be carried out in the context of the activities of the said establishment in the Union.

The legal form of arrangements, – whether a branch, an office or a subsidiary, – is not decisive in respect to the application of the establishment criteria. Even lack of a registered office in the Union does not preclude a non-EU entity from having an establishment there within the meaning of EU data protection law. On the contrary, it is possible that a non-EU company can have a formally registered branch in the Union, however, that branch will not be considered an establishment for the purposes of EU data protection law. A travelling agent of the non-EU entity cannot constitute stable arrangement due to being unstable *a priori*, at least on the basis of not having a fixed location.

As regards a non-EU company providing services via the Internet, it is considered to be established in the place where it pursues economic activities. A website as such cannot be singled out as a separate stable arrangement, however, an establishment becomes established through the website. A non-EU entity cannot be admitted to have an establishment in the Union based solely on the fact that its website can be accessed from one of the Member States.

Stability of arrangements is always relative: what is sufficiently stable in one case, might be not stable enough to be rendered establishment in another. Thus, the degree of stability always has to be evaluated on a case-by-case basis.

In order to be considered real and effective, the activities exercised in an establishment in the Union must contribute to the data processing activities of the non-EU parent company and occur in the place of stable arrangements. Practically any kind of activities may be considered as related to the activities of the parent company, especially when a local establishment serves as a link between the data subjects and the non-EU entity.

Processing in the context of the activities of an establishment in the Union implies that the establishment has to play a relevant role in a particular processing operation. If not the 'in the context of' formula, it would be impossible to connect establishments in the Union with their parent companies and data processing standing behind them. The processing does not necessarily have to be done by an establishment itself, though it may be carried out so. Even if an EU establishment does not carry out any data processing operations itself, its other activities can still trigger the applicability of Article 3(1) GDPR to the data processing on the basis of being otherwise inextricably linked to the data processing operations of the non-EU parent company. The case law allows inferring that activities of the EU establishments that concern the EU sales offices, such as promotion or selling of advertising, marketing directing at the EU residents, commercial prospection, are likely to fall under 'inextricable link'. Nevertheless, 'in the context of' formula remains problematic due to being potentially boundless and covering practically any connections between the non-EU operator performing processing and its establishment in the Union.

The establishment principle applies differently to the non-EU controllers and processors within one processing operation. The ascertained applicability of the Regulation to one of them does not automatically invoke the applicability to the other. The GDPR controller obligations apply to joint controllers separately and in view of contribution of

each of them to the specific processing operation or its part. In case an EU controller which is subject to the GDPR uses a non-EU processor, the latter will become subject to the Regulation on the basis of indirect application through Article 28 GDPR by means of the contract or other legal act. By contrast, if a non-EU controller which is not subject to the GDPR uses an EU processor, the fact of applicability of the establishment principle to the EU processor will not actuate the applicability to the non-EU controller – the legal relationship at stake will concern provision of a processing service on behalf of the non-EU entity where the latter appears as a client and the EU processor as a contractor.

Under exceptional circumstances, a non-EU controller may be applicable to the GDPR controller obligations due to having an establishment in the Union through the EU processor. The given case may occur only if the EU processor's activities are considered inextricably linked (for instance, essential to revenue-raising) to the processing carried out by the non-EU controller.

Even if a non-EU entity is not established in the Union, the GDPR can still apply to it through targeting criteria. The targeting principle is oriented purely towards the controllers and processors that are not established in the Union and also focuses on those non-EU entities which do not process personal data in the context of the activities of their EU establishments (if such are available). The applicability of the targeting principle may be possible on precondition that the establishment principle is not applicable.

The concept of targeting characterizes not only the scope of the nature of the activities, i. e., targeting as an activity, but also defines the subjective component of the non-EU entities which is to reach the data subjects in the Union – targeting as a goal. So, to invoke application of the targeting principle, the activities must have features attributable to targeting.

In order to determine whether a non-EU controller or processor directs its activities at the data subjects in the Union, it is necessary to apply the targeting test which includes checking whether the processing of personal data concerns the data subjects who are in the Union and determining whether the processing is related to either the offering of goods or services or to the monitoring of data subjects' behaviour within the Union.

The scope of a data subject in the Union is not limited to any legal status defining a physical person. In the context of Article 3(2) GDPR, the only significant circumstance is that the data subject in question is located within the EU.

To be located in the Union in terms of spatial scope means that a data subject is physically present in the territory of the EU. The duration of the physical presence is not decisive. The most important thing is that the processing of personal data takes place at some point of time during stay in the EU. Even in cases of online behaviour, the data subjects must be physically present in the Union, notably when accessing the Internet. The data subjects' being in the Union has to be evaluated at the moment when the processing related to the relevant targeting activity – monitoring the behaviour or offering of goods or services – takes place. A non-EU controller or processor becomes pursued under Article 3(2) GDPR at the moment of collection (in a broad sense) of personal data. Therefore, requirement that data subjects have to be located within the EU concerns only the time of collection of their personal data; subsequent leave of the Union does not affect applicability of Article 3(2) GDPR to the non-EU operator.

Monitoring as such consists of the targeting and the immediate data processing which happens at the same time as the targeting activity. In essence, targeting becomes monitoring only when it is accompanied by data processing. Thus, if personal data of a data subject in the Union was not processed, this means that the data subject was not monitored. For the applicability of Article 3(2) GDPR on the basis of monitoring, there need to be two conditions met: first, a non-EU controller or processor monitors the behaviour of a data subject in the Union, i. e., targets a data subject and processes the data subject's personal data, second, the data subject is physically present in the Union.

Unlike in monitoring, the moment of offering goods or services is not a data processing yet. Offering as such does not necessarily include processing, especially if it concerns offline activities. Therefore, if offering does not draw after it the data processing, it will not invoke the application of Article 3(2) GDPR. As regards offering of goods or services online, in fact any offering will additionally invoke processing of personal data since the mere visit of the website will lead to the processing. For the applicability of Article 3(2) GDPR on the basis of offering, the following conditions must be fulfilled: first, a non-EU controller or processor offers goods or services to a data subject in the EU, second, the data subject is physically present in the Union, third, the data processing takes place when the data subject is in the EU. To invoke the targeting

principle, it is important that the data subject is located in the Union not when the offer is made, but when the processing related to the offer is carried out.

There are certain general criteria indicating that a non-EU controller or processor intentionally targets data subjects in the Union by offering goods or services to them. The specifically mentioned EU individuals or the specific advertising in the EU territory speak in favour of targeting data subjects in the Union. By contrast, the less specific offering is, the less probably it will be ascertained as targeting individuals in the EU. Also, offering needs to be accompanied with the processing which relates to it. For this reason, processing of personal data related to employment matters cannot invoke application of Article 3(2)(a) GDPR since it does not foresee *per se* any offers of goods or services to the employees. Furthermore, offering has to target individuals in the Union *ab origin*, therefore, when individuals from the third countries enter the EU and continue using the non-EU service in the Union, this does not change the fact that the service still targets individuals in the third states only.

Finally, offering requires intention. Objective targeting implies that offering activities include an objective intention of a non-EU operator to direct its activities to data subjects in the Union, and this intention is manifested through objective evidences. The availability of just one evidence may be insufficient to ascertain a non-EU controller's intention of offering, nevertheless, this will depend on the facts of a concrete case. So, as a general recommendation, it is suggested that the more factors of offering are ascertained, the better. The indices of offering (are discussed closely in the paper) are not exhaustive. Their common feature is that each evidence has many 'buts', and the applicability depends on the content of the website (in case of online offering), thus, must be evaluated in the light of other evidences of directing.

So far as Article 3(2)(b) GDPR captures wider range of grounds for the applicability of the Regulation since it is likely to cover all sorts of online as well as offline activities, it will most likely catch those non-EU operators who target the EU, however, managed to bypass the grounds found in Article 3(2)(a) GDPR.

In order to ascertain that a non-EU entity monitors the individuals' behaviour within the Union, two things need to be established: first, data subjects tracking on the Internet, and, second, potential subsequent use of data processing techniques that envisage profiling of the data subjects. While tracking can be objectively ascertained, the subjective intention is not that easy to determine. It seems rational to take the same

approach which is used in application of offering criterion, that is to say, ascertaining whether a non-EU entity actively demonstrates its intention to target – here: to monitor – individuals in the Union.

Monitoring requires an intentional purpose which implies that monitoring must be intentional by default. The lack of will to further use the data processing techniques to the collected data demonstrates the absence of intention to monitor, which has to be present on the whole way of monitoring activities. Therefore, for instance, passive, i. e., without intention, continuing collection of data regarding the natural persons' behaviour within the Union will not present monitoring.

Purposes for which the non-EU controllers monitor the data subjects' behaviour in the Union vary. Often they are marketing or advertising. Activities, such as decision-making, analysis, prediction, collection, reuse etc., are actions that accompany and at the same time serve as interim steps towards the ultimate goal which is conditional on the factual purpose of monitoring.

Monitoring activities may consist of tracking on the Internet or through other types of network or technology used in wearable and other smart devices. Data processing activities can be referred either to mapping, tracking or profiling activities. The main feature shared by all monitoring activities is that the monitored data subject can be identified in the result, i. e., monitoring activity is supposed to enable connecting particular individual and the information about him or her. The fact of creation of a profile on the data subject is the best evidence that the data subject is being monitored.