TERRITORIAL SCOPE OF APPLICATION OF THE GENERAL DATA PROTECTION REGULATION

Sylwia Kotecka-Kral, Ph.D.
Center for Legal and Economics Issues of Electronic Communications
Faculty of Law, Administration and Economics
University of Wroclaw
Wroclaw, Poland
e-mail: sylwia.kotecka@uwr.edu.pl

Abstract

As a result of the rapid development of the information society, the intangible good that is information – and particularly personal data – has become an exceptionally valuable product. We are also in the midst of a phenomenon entirely unknown in the 1990s – methods of processing personal data using such means as cloud computing technology, so-called big data. The previous model of EU regulation that made the applicability of EU law dependent on economic activity being conducted by a data administrator within the territory of a Member State, or the use of data processing means located within that territory, is today insufficient and obsolete. It became necessary to abandon the principle of territoriality introduced by 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, replacing it with a more elastic means of regulating the application of EU law. The objective of the present work is to present the territorial scope of the 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).

Keywords: personal data, data subject, personal data processing, personal data controller, processing entity, territorial scope of application of GDPR

Introduction

As a result of the rapid development of the information society, the intangible good that is information – and particularly personal data – has become an exceptionally valuable product. Functioning in the information society is inextricably linked with the processing of personal data, which has evolved into something resembling almost a new currency. It is estimated that the market value of the total volume of data processed online within the borders of the European Union will reach EUR 739 bn by the year 2020. The ease with which information is transmitted and the universality of access to the open teleinformatics system that is the internet have led to the development of an entire segment of services provided online with tremendous significance for the economy. Previously unknown business models and means of providing services have emerged. Importantly, we are also faced with means of processing personal data completely unknown in the 1990s, such as with the use of cloud computing technology *id est* so-called big data. In the era of globalization, expansion of trans-border services, and the information society, in which online activities can be conducted from virtually any place on the planet, the territorial scope of application of legal regulations is taking on an increasing significance.

The previous model of EU regulation that made the applicability of EU law dependent on economic activity being conducted by a data administrator within the territory of a Member State, or the use of data processing means located within that territory, is today insufficient and obsolete. Presently, the omnipresence of the internet is leading to the data of EU residents being processed – frequently on a mass scale – outside the EU itself, by personal data controllers who are not governed by the stringent European standards applicable to personal data protection. American entities are particularly distinct in this respect, as in many fields of technology they tend to be more innovative than their European counterparts. They are offering with increasing frequency services with more robust functionalities than those offered by European competitors, thereby acquiring large numbers of customers within the borders of the EU.

As concerns standards of personal data protection, there is at present a great deal of diffusion; in an age of expansion of services provided globally, combined with the strong position on the internet of service providers from outside the EU, this is by no means a beneficial trend. In particular, data subjects from states offering high personal data protection standards are frequently unaware that they are using the services of personal data controllers who themselves are not governed by regulations that would ensure a

level of personal data protection aligned with EU standards. It became necessary to abandon the principle of territoriality introduced by 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, replacing it with a more elastic means of regulating the application of EU law.

In recent years, the Court of Justice of the European Union (CJEU) has engaged in the broad interpretation of the provisions of Directive 95/46 concerning the scope of its territorial applicability. Of particular importance to the subject of this paper are the Court's rulings in the cases C-131/12, *Google Spain*, C-230/14, *Weltimmo*, and C-191/15, *Verein für Konsumenteninformation versus Amazon EU Sárl*. All these cases, while from different perspectives, addressed the issue of the territorial scope of application of the regulations contained in Directive 95/46 and their implementation by the national regulations of EU Member States. The territorial scope of the 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) is aligned with the guidelines set out in the CJEU's judgments in those cases.

One of the primary objectives to be achieved by the General Data Protection Regulation, in replacing Directive 95/46, is the adaptation of provisions of EU law to the realities of the information society and the present state of technology. For these changes to achieve their stated goal and to provide real protection of data subjects, it was vital to expand the territorial scope of EU law on the protection of personal data. Protection of natural persons in conjunction with the processing of personal data, which results directly from Art. 8(1) of the Charter of Fundamental Rights and Art. 16(1) Treaty on the Functioning of the European Union, has been elevated to the status of a fundamental right. The references provisions state that each individual has the right to the protection of personal data concerning him or her. This protection should be ensured regardless of the location of the controller or entity engaged in processing, as well as the location of technical means used for such processing. In the information society, jurisdiction based on the principle of territoriality means that data subjects are finding it increasingly difficult to pursue effective protection of their rights regarding personal data protection; these difficulties result from the inability of EU oversight bodies to effectively exert control over personal data controllers operating on the internet.

Pursuant to Art. 288 TFEU, the Regulation is of general reach, its provisions are binding in their entirety, and they are directly applicable in all Member States. By its very nature it constitutes an element of municipal legal systems without the necessity of any acts of transposition, and evokes direct effects in relation to individuals. Regulations encompass both vertical and horizontal effect without exception. The General Data Protection Regulation is of this very same nature, performing the role of a harmonizing act with regard to the law on protection of personal data within all Member States.

The employment of a Regulation as the form of harmonization means the derogation of the legal basis for the applicability in Poland of the Personal Data Protection Act in its present form (as legislation implementing Directive 95/46), which constitutes comprehensive regulation of the rules of conduct in the processing of personal data and the rights of people whose personal data is processed. From the perspective of the General Data Protection Regulation, the application of solutions not provided for in the Regulation and not expressly left for regulation by municipal law is prohibited. However, GDPR does not introduce full harmonization understood as the total (complete) shaping of regulations in a given area and the impermissibility of application of national legislation.

Territorial scope of Directive 95/46 in the context of the CJEU judgment in C-131/12, *Google Spain*

While the judgment handed down in 2014 in C-131/12, *Google Spain*, primarily addresses the "right to be forgotten," it also contains an interpretation of the provisions of Directive 95/46 concerning its territorial scope. The Court acknowledged Spanish jurisdiction over a controller of personal data with its seat located in the United States. To this end, the CJEU engaged in interpretation of the provisions of Directive 95/46 in respect of the conducting of economic activity. It held that Art. 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State. It thus held that the Spanish data protection authority exercised jurisdiction over Google Inc., a company incorporated in the United States, and which had only a subsidiary engaged in the promotion and sale of advertisements. A different interpretation of that provision of Directive 95/46 and different ruling by the Court would lead in that particular case to a situation difficult to accept in which a Spanish citizen, using an internet search engine offered in the Spanish languages to find the webpage of a Spanish newspaper with information about events taking place within the borders of Spain

and directly affecting that citizen, in which that individual's personal data was given, would be unable to pursue the enforcement of rights under Spanish jurisdiction.

Territorial scope of Directive 95/46 in the context of the CJEU ruling in C-230/14, *Weltimmo*

Differently than in the judgment in C-131/12, *Google Spain*, when ruling in C-230/14, *Weltimmo*, issues concerning the scope of jurisdiction related to determining the applicable law within the European Union, and more specifically – in relation to the facts of that particular case, was the authorized oversight body that of Slovakia, or of Hungary, and also under which national regulations that oversight should be exercised. Weltimmo, a company incorporated under Slovakian law, claimed that it was engaged in economic activity exclusively in Slovakia, *id est* in the Member State in which it has its registered seat. At the same time, the Hungarian oversight authority, basing on interpretation of Art. 4(1)(a) of Directive 95/46, claimed jurisdiction over that company, arguing that the activity of Weltimmo, the operator of an internet webpage with announcements, was focused on the territory of Hungary.

In this case as well the Court supported a broad interpretation of Art. 4(1)(a) Directive 95/46, in its judgment taking into account the role of the internet. The position taken by the CJEU was that the provisions of Directive 95/46 supply "a flexible definition of the concept of 'establishment', which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, in order to establish whether a company, the data controller, has an establishment, within the meaning of Directive 95/46, in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet." The Court adopted a very broad interpretation of the notion of an "establishment," holding that "the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question."

In the judgment analysed here, the Tribunal stated that for recognition of the jurisdiction of the Hungarian authority it was sufficient for the claimant to operate on the internet a website with listings for real estate located in Hungary, provided in the Hungarian language, possessing a representative that conducted in a continual manner the undertaking's business in Hungary by *inter alia* representing the undertaking in administrative and judicial proceedings, with a bank account opened in Hungary, and possessing a postal address in Hungary for conducting the undertaking's business. Such activity is sufficient to rule that Weltimmo conducts economic activity within the territory of Hungary. It would therefore seem that the notion of an "organisation" is obviously more flexible and broader than its definition under Polish law, which we shall discuss later on.

This judgment is of exceptionally far-reaching significance – it lends support to the application of a broad interpretation of the notion of "engaging in economic activity" and confirms the correctness of the interpretation under which the understanding of Art. 4(1)(a) Directive 95/46 should be based on the territory where the effective and actual performance of economic activity is done through continual measures, and not on the location of the registered seat of the organization processing personal data.

Territorial scope of Directive 95/46 in the context of the CJEU judgment in C-191/15, *Verein für Konsumenteninformation versus Amazon EU Sárl*

In a successive judgment, handed down on the basis of Directive 95/ but which remains applicable also after the implementation of GDPR, the CJEU held that an "organization" is located in the territory of a Member State to which the undertaking directs its activity if it occurs that the undertaking processes data in the context of economic activity within that Member State. The determination as to whether such circumstances exist is a matter for national courts.

Regulations contained in GDPR

The territorial scope of application of GDPR is provided for in Art. 3 of the Regulation and explained in paragraphs 22-25 of the preamble.

Article 3(1) GDPR

Pursuant to Art. 3(1), the 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.

The Regulation thus applies to processing activities related to the activity of the controller or the processor which possesses an establishment within the territory of the EU. It should be emphasized that "processing of personal data in the context of the activities of an establishment of a controller or a processor" does not mean that such processing must be performed by that particular establishment. For the provisions of the GDPR to be applicable, it is sufficient that there be a connection between the act of processing data and the activity of a given establishment of a controller or processor located within the territory of the EU.

Concerning the content of Art. 3(1) GDPR, it is essentially analogical to Art. 4(1)(a) Directive 95/46. In the Polish version, the English phrase "in the context of" from the Directive was translated as "w kontekście", while in GDPR, the English version remains unchanged, but the Polish translation now reads "w związku". Apart from the complicated matter of translation of the notion of an "establishment" (to be addressed later on), two significant differences in comparison to Directive 95/46 are:

1) the addition of reference to "processor", which was not given in the now-invalid Directive – and thus another element expanding the scope of application of EU legislation which referred in Directive 95/46 solely to controllers, and
2) the indication that this provision is applicable regardless of whether such processing is taking place within the EU – also emphasized by the extraterritorial aspect of Art. 3(1) GDPR, despite the fact that that article, through the criterion of location of the establishment of a controller or a processor within the EU, is *de facto* based on the principle of territoriality.

It is undoubtedly crucial to elaborate three notions employed in Art. 3(1) GDPR, specifically: "działalność" (operated by an organization), "jednostka organizacyjna", and "podmiot przetwarzający". Because the notions of "dane osobowe" and "przetwarzanie danych osobowych" are already well-established on the basis of previous legislation, the reader is referred to the rich literature related to it.

The notion of "activities (of an establishment)"

The provisions of GDPR do not directly define the notion of "activities of an establishment of a controller or a processor"; interpretation within this scope should, however, strive to encompass the broadest possible understanding of this notion. Doubtlessly this does not mean only the notion of economic activity, which is in a way confirmed by Recital 6 GDPR, which mentions the use by both private companies and public authorities of personal data in their activities in an unprecedented scale. This can thus be understood as both public activity interpreted very broadly to include the activity of public administration, as well as activity without a profit motive, undertaken by foundations and other similar organizations. Indeed, there is no reason to assume this should not mean the undertakings of natural persons, including those not operating establishments.

For the application of GDPR it is irrelevant where the processing of personal data takes place – the only important thing is whether the processing is done in the context of the activities of an establishment of a controller or a processor in the Union. Circumstances such as the physical location of servers or the use of services from subcontractors outside the EU are thus irrelevant to determining the scope of application of GDPR.

The notion of an "establishment of a controller or a processer"

A key element in the modified territorial scope of EU regulations on protection of personal data is the notion of an "establishment" employed in Art. 3 GDPR. This notion, equally important in Directive 95/46, was translated there as "prowadzenie działalności gospodarczej", whereas in the new Regulation it reads as "działalność prowadzona przez jednostkę organizacyjną". The phrase "establishment" was for years repeated in judgments of the CJEU, as well as in opinions of the Article 29 Working Group. In the course of work on the Polish translation of the General Data Protection Regulation, many different versions were considered for translation of the English notion of "establishment", including "siedziba", "jednostka", "oddział", "miejsce prowadzenia działalności", "miejsce prowadzenia przedsiębiorstwa", and "zakład". Ultimately, however, the phrase "jednostka organizacyjna" was adopted. This change, itself revolutionary, thus only took place in reference to the Polish version of the text of GDPR. What results from this is that the phrase employed by translators in the Polish version of Directive 95/46 "prowadzenie działalności gospodarczej" had a narrower scope than the notion of "establishment" as understood by the Court of Justice, and did not accurately reflect the intentions of the European legislator.

One of the arguments in favour of such a translation into Polish was the imprecision of the previous solution – indeed, GDPR is applicable also in respect of personal data and processors who are not engaged in operating an establishment. For example, the activity of public administration, churches and faith unions, as well as of many nongovernmental organizations cannot be considered economic activity, but it is encompassed by the scope of application of the Regulation. At the logical level, this entirely excludes the possibility of invoking in Art. 3 GDPR the notion of "prowadzenie działalności gospodarczej" (which we may translate into English as "conducting economic activity".

In light of the foregoing, despite the commencement of the application of GDPR, the indications of CJEU referring directly to interpretation of the notion of "establishment" contained in judgments handed down during the period in which Directive 95/46 was in effect, particularly in the cases C-131/12 *Google Spain*, C-230/14 *Weltimmo*, and C-191/15 *Verein für Konsumenten-information*, retain their relevance also in relation to interpretation of the notion of "jednostka organizacyjna" (as the Polish translation of "establishment") following the entry into force of the GDPR.

The General Data Protection Regulation does not contain a legal definition of the notion of an establishment, which would seem a deliberate act on the part of the European legislator, one designed to give the Regulation greater flexibility in defining the territorial scope of application of its provisions. In the absence of a definition, the Court of Justice or the European Data Protection Board will be able to exert greater influence on the interpretation of that notion and adapt its understanding to new models and the state of the art in personal data processing. Through the broad scope of application of European legislation, it will also facilitate more effective protection of the rights of data subjects in the information society, particularly the broad applicability of EU supervisory authorities.

Because "jednostka organizacyjna" is a concept deeply rooted in the Polish legal system, in both civil law and administrative law regulations, the notion is deserving of particular attention. At the same time, there shouldn't be even the slightest doubt that the notion of "establishment" in Art. 3 GDPR should be treated as an autonomous notion of EU law in respect of protection of personal data, and should thus be interpreted without reference to national regulations. The notion of an "establishment" is broader than the notion of seat, place of residence, branch, or office of an enterprise. In this context, Recital 22 in the preamble of GDPR indicates that the notion of an establishment assumes the effective and real conducting of activity through stable structures. The legal form of those structures, regardless of whether a branch or a subsidiary with juridical personhood, is not the deciding factor in this respect. It is of no relevance in what legal form the activity of an establishment is conducted. There is thus no reason to exclude branches or subsidiaries solely on grounds of the form of the establishment from the application of GDPR. The Regulation puts emphasis on the factual circumstances and does not require the existence of a name, seat, or body.

Although on grounds of Art. 3 GDPR there is no formal distinction between personal data controllers from the public and private sector, the particular solutions provided for in the Regulation in areas like the scope of legal bases for the processing of data exhibit certain differences depending on whether a given entity is part of the public or the private sector. The scope of application of GDPR encompasses entities in both the public and the private sectors. In respect of public entities, the scope of application of GDPR encompasses organs of public administration, *id est* organs of central governmental administration, local self-government, and all entities or organizations granted by statute competences within the scope of administration.

Regulation of territorial scope within national legislation is important in the context of a situation in which the GDPR allows the law of Member States to modify the general principles provided for in that legal act. Here we should point out an issue of potentially large practical significance – in particular, the Regulation, in the event of discrepancies within national legislation, does not harmonise the territorial scope of their application, nor does it provide any conflict of laws rules. This means that, contrary to the original intentions of the European legislator, the same controller or processor of personal data operating in a trans-border manner can be governed by provisions of the legislation of particular Member States that are in conflict with one another. This can occur in a limited number of cases, particularly when national regulations seek to add detail to the issue of the expression of consent by a (Art. 8(1) GDPR), the processing of genetic, biometric, or other data concerning health (Art. 9(4) GDPR), and in respect of exclusion of the possibility of expressing consent to the processing of particular categories of personal data (Art. 9(2)(a) GDPR). For example, the Polish regulations adopted on the basis of Art. 8(1) GDPR set a threshold of 13 years, Austrian regulations – 14 years, and German regulations – 16 years. When it comes to services of the information society, the processor processing the personal data of children from those three Member States will thus be governed by three national rules in conflict with one another, as the Regulation does not provide for separate rules to avoid conflict of laws issues. This is why it will also be of importance to determine the territorial scope of application of particular national legislation.

It should be considered that the primary criterion for determining the territorial scope of the

provisions of the General Data Protection Regulation is possessing an establishment within the territory of the EU, and only in the event that condition is not fulfilled, proceeding to the conditions provided for in Art. 3(2 and 3) GDPR.

The notion of the processor

The General Data Protection Regulation contains a legal definition of data processor. Pursuant to Art. 4(8) GDPR, the notion of "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." The definition of a processor thus encompasses an equally broad scope of entities as the definition of a controller. This notion plays an important role in the context of ensuring the confidentiality and security of data processing when considering that it serves to indicate the entity engaged in processing operations on behalf of the controller, and in consequence establishes a certain framework for its activity. The controller and the processor are participants in the primary mechanism of processing undertaken with a specified goal and scope. However, the mere presence of a processor within the processing process is dependent on a decision of the controller, who is free to select a mode of processing requiring the exclusive participation of people directly subordinate to the controller and authorized to engage in processing under that controller's direct supervision, but which can also potentially decide to engage other entities acting on its behalf in the process of data processing. It should, however, be kept in mind, and with regard to the wording of Art. 28, that in certain circumstances the fact of entrustment of data processing does not result from the autonomous decision of the controller, but rather from legal instruments regulating a given processing. Such cases can arise primarily in the public sphere.

In the light of Art. 28(3)(a), the processor can essentially work based exclusively on the documented instructions of the controller. This means that it is the controller that determines the purposes and modes of processing, including the decision to entrust data to a processor for the processing of that data in the controller's name. The activity of a processor must thus remain within the framework defined by the controller and is essentially devoid of any discretion and freedom. The binding of a processor by the controller by way of purposes and modes of data processing sets out the boundaries of the processor's activities.

Article 3(2) GDPR

Far more revolutionary is Art. 3(2) GDPR, which states that "(t)his 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
b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Indeed, this provision entirely decouples the application of EU rules from the principle of territoriality, in practice essentially marginalising the meaning of the condition set out in para. 1 of that provision, itself repeated from Directive 95/46. Instead of this, a solution was introduced which can be defined as "targeting", abandoning territoriality in favour of the principle of protection. New EU data protection principles will be applicable to everyone offering goods and/or services to data subjects in the EU or monitoring the conduct of such entities, to the extent it is done within the EU – and thus "targeting" data subjects with their activities. They are applicable regardless of whether the data subject engages in any activity at all. It is for the controller or processor of data to assess whether the nature of their activity can lead to assuming obligations arising from the provisions of the General Data Protection Regulation. The provisions of GDPR encompass entities providing services via the internet, and also – because of the reference to monitoring of behaviour – those which employ methods based on profiling, such as for marketing purposes, or processing personal data within the context of so-called big data. This is the case regardless of the location of the individual processing personal data.

This means that even entities located outside the EU will be required to apply European personal data protection legislation. This is a very significant change with respect to the previous regulations in force, under which entities with their seat in a third-party state and engaged in the processing of personal data from outside the European Economic Area or employing technical measures located within the territory of Poland exclusively for the purpose of transmitting data to a third-party state were not subject to the Polish Personal Data Protection Act of 29 August 1997. The previous legal environment made it possible to escape from the regime of strict and formalized personal data protection standards provided for in Polish regulations. International capital groups could also organize their personal data processing processes in such a manner that the entity deciding on purposes and means of data processing is in fact e.g. a holding

company with its seat in the United States, while the activity of the local Polish subsidiary was limited to forwarding data to its parent company. In this manner it was possible to escape the rigorous Polish personal data protection laws. GDPR does not allow for such a possibility. For example, under the Regulation, a company with its seat in the USA and operating a worldwide internet shop available also in Poland will have to operate the Polish portion of its business in compliance with GDPR, even if it processes data via technical means located within the borders of the USA.

A long-term consequence of this formulation of territorial scope will be the necessity of many data controllers and processors from third-party states (i.e. from outside the European Economic Area) adopting the assumption that specific personal data processing operations are governed by the provisions of GDPR, as there is a risk that some of the users of a given service are EU data subjects. It thus comes as no surprise that such a far-ranging expansion of the territorial scope of application of EU law is causing concern among controllers of personal data in third-party states. In particular, small and medium enterprises from such states may not be aware of the existence of EU rules on personal data protection, nor of the fact that they are obliged to follow them.

Article 3(2) GDPR, which introduces the previously mentioned jurisdiction based on "targeting", is intended to protect data subjects in the EU irrespective of the location of the controller or processor of the personal data (*id est* the entity which has been entrusted with the processing of personal data) and the location of the technical means employed in that processing. This approach is clearly different from that employed by e.g. 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'), which uses the principle of the state of origin, as the location of the data processor or controller is irrelevant to "targeting".

The provisions of Art. 3(2) GDPR should be interpreted in connection with the content of Recitals 23 and 24 of the preamble. Recital 24 clearly indicates that in the case of "monitoring behaviour" referred to in Art. 3(2)(b), the European legislator was concerned with observation and profiling, *id est* activities which are universal on the internet. This observation is done using such means as cookies, which are files saved on the computes of users visiting particular webpages. Profiling is a practice of social media portals, internet shops, and also search engines, the vast majority of which (including the largest) have their seat outside the EU. It is slightly more difficult to understand the intentions of the European legislator as concerns Art. 3(2)(a) and the offering of goods and services. Recital 23 of the preamble to GDPR indicates such factors as " the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union." This is, however, only a partial list. In the future it will be possible to interpret this provision even more broadly. Presently, the reference in Art. 3(2)(a) to the irrelevance of payment stems from the fact that many services in the internet, such as e-mail, social media accounts, some games, and activities based on Web 2.0 are offered on a free basis. The Union legislator thus desired to clearly indicate that these services as well would be encompassed by the scope of the new regulation.

It should be emphasized that Art. 3(2) GDPR establishes an exceptionally broad territorial scope for the application of the Regulation. Particularly with regard to online activities, many of them, regardless of who is engaged in them, could potentially be encompassed by the territorial scope of application of EU provisions. At the same time, this approach seems largely justified in times where a single individual with a portable computer can process millions of records of personal data. It should, however, be given special attention, and with all certainty should be analysed during the nearest evaluation referred to in Art. 97.

The determination of whether we may speak in a given case of targeting can in practice give rise to doubts. On the one hand, invoking case-law and scholarly writings to assist in grasping the question of liability on the internet, it should be said that, when referring to targeting, the mere potential accessibility in a given state of information uploaded to a publicly accessible portal is an insufficient criterion. This is confirmed in Recital 24 in the preamble to GDPR, pursuant to which the determination of whether a controller or processor is offering goods or services to people located in the Union and whom that data concerns, the mere accessibility within the Union of the webpage of the controller, processor, intermediary, email address, or other contact data, nor the use of a language generally spoken in the third-party state in which the controller has an undertaking, is insufficient. On the other hand, if the addressing of an offer to citizens of an EU state is clear owing to the selection of language in which an order may be placed or a list of states in which the client may reside, the processing of data is governed by GDPR.

Article 3(3) GDPR

In accordance with its wording, the Regulation is applicable to the processing of personal data by a controller without an undertaking in the Union, but which has an undertaking in a place where it results from application of the provisions of public international law the law of a Member State is applicable.

Public international law may be defined as a group of norms regulating the legal relations among states, among states and other entities active in the international arena, and among those entities with the capacity to act in international relations. These other entities are primarily international organizations. Public international law is among those public laws whose domain is the admission of the priority of the state in relations with persons. The primary source of public international law is the international agreement, but also international custom, the case-law of international courts, scholarship, the legislation of states, unilateral acts (notification, protect, recognition, renunciation), the resolutions of international organizations, and general principles of international law.

We should also recall situations in which GDPR is applied pursuant to conflict of laws provisions in private international law, which is not, however, encompassed by the scope of Art. 3(3).

Conclusions

The General Data Protection Regulation introduces a range of changes to EU law. One of them, important not only for the European but also the global personal data protection system, is the European legislator's departure from the scope of application of EU rules based exclusively on the criterion of territory. The new model, while still retaining references to territory, is based on a mechanism that can be referred to as "targeting" and is intended to ensure effective protection of personal data in the information society. These changes should doubtlessly be judged positively. However, the key issue that comes to the fore in conjunction with the territorial scope of GDPR application is the real possibility for European bodies to enforce decisions issued against entities from outside the EU.

References

BARTA, P., LITWIŃSKI, P., KAWECKI, M. 2018. *Komentarz do art. 3* (*Commentary to Article 3 GDPR*)(in:) Litwiński, P. (ed.), Barta, P., Kawecki, M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz* (*EU regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data. Commentary*), Warsaw, p. 151-160.

CLOUD COMPUTING. STUDY, 2012. Online access: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf, p. 8.

CZERNIAWSKI, M. 2015. *Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych* (*The current and planned territorial scope of the EU provisions on the protection of personal data*), Europejski Przegląd Sądowy, 5: 4-9.

CZERNIAWSKI, M. 2016a. *Rozdział 4. Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej* (*Chapter 4. Territorial scope of application of Polish and EU provisions on the protection of personal data in the context of the latest case law of the Court of Justice of the European Union*) (in:) Bielak-Jomaa, E. (ed.), Lubasz, D. (ed.), *Polska i europejska reforma ochrony danych osobowych* (*Polish and European reform of personal data protection*), Warsaw.

CZERNIAWSKI, M. 2016b. *Zakres terytorialny a pojęcie "jednostki organizacyjnej" w przepisach ogólnego rozporządzenia o ochronie danych – zarys problemu* (*Territorial scope and the notion of an "establishment" in the provisions of the General Data Protection Regulation - outline of the problem*) (supplemental to Monitor Prawniczy, 20), Monitor Prawniczy, 20: 22-28.

CZERNIAWSKI, M. 2018. *Komentarz do art. 3* (*Commentary to Article 3*) (in:) Bielak-Jomaa, E. (ed.), Lubasz, D. (ed.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz* (*General Data Protection Regulation. Commentary*), Warsaw.

EUROPEAN DATA MARKET SMART 2013/0063, Final Report of 1.01.2017, 2017. Online access: http://datalandscape.eu/study-reports/european-data-market-study-final-report.

KAMIŃSKI, I.C., WARSO, Z. 2014. *Czy można zniknąć z Google'a? Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González (C-131/12)* (*Can you disappear from Google? Judgment of the Court of Justice of the European Union regarding Google Spain SL and Google Inc. against the Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12)*) (in:) Bychawska-Siniarska, D. (ed.), Głowacka, D. (ed.), *Wirtualne media - realne problemy: materiały z konferencji zorganizowanej w dniu 15 kwietnia 2014 r. przez Obserwatorium Wolności Mediów w Polsce*

Helsińskiej Fundacji Praw Człowieka, Zakład Praw Człowieka Wydziału Politologii Uniwersytetu im. Marii Curie-Skłodowskiej w Lublinie i Zakład Praw Człowieka Wydziału Prawa i Administracji Uniwersytetu Warszawskiego (*Virtual media - real problems: materials from the conference organized on 15 April 2014 by the Observatory of Freedom of Media in Poland The Helsinki Foundation for Human Rights, Department of Human Rights, Faculty of Political Science, University of Maria Curie-Skłodowska in Lublin and the Human Rights Department of the Faculty of Law and Administration of the University of Warsaw*), Warsaw, p. 51–66.

KLOC, K., GAWROŃSKI, M. 2018. *Przedmiotowy i terytorialny zakres stosowania RODO* (*Material and territorial scope af application of GDPR*) (in:) Gawroński, M. (ed.), *RODO. Przewodnik ze wzorami* (*GDPR. Guide with patterns*), Warsaw, p. 45-46.

KOMENTARZ do art. 4 pkt 8 (*Commentary to Article 4(8) GDPR)*, 2018 (in:) Bielak-Jomaa, E. (ed.), Lubasz, D. (ed.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, (*GDPR. General Data Protection Regulation. Commentary*), Warsaw

KOMENTARZ do art. 8 (*Commentary to Article 8*), 2013 (in:) Wróbel, A. (ed.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz* (*The Charter of Fundamental Rights of the European Union. Commentary*), Warsaw

LUBASZ, D., 2018, *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi* (*GDPR. Changes in the protection of personal data. Comparison of legal provisions. Practical notes*), Warsaw, p. 19

SIBIGA, G. 2016. *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia* (*Permissible scope of Polish provisions on the protection of personal data after the date of application of the General Data Protection Regulation - selected issues*), supplemental to Monitor Prawniczy, 20.

SZAFRAŃSKI, B. 2014. *Realizacja zadań publicznych a Big data* (*Implementation of public tasks and Big data*) (in:) G. Szpor (ed.), *Publiczne bazy danych i Big data* (*Public databases and Big data*), Warsaw.

SZYMIELEWICZ, K. 2017. *Śledzenie i profilowanie w sieci: w czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość? Raport Fundacji Panoptykon* (*Tracking and profiling on the web: what's the problem? What will change in the law? What can the future look like ? Report of the Panoptykon Foundation*), Warsaw. Online access: https://panoptykon.org/sites/default/files/publikacje/sledzenie_i_profilowanie_w_sieci_scenariusze_po_reformie_ue_wrzesien_2017.pdf.

ŚWIERCZYŃSKI, M. 2017. *Rozdział IV. Jurysdykcja krajowa w świetle ogólnego rozporządzenia o ochronie danych* (*Chapter IV. National jurisdiction in the light of the general Data Protection Regulation*) (in:) Kawecki, M. (ed.), Osiej, T. (ed.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia* (*General Data Protection Regulation. Selected issues*), Warsaw.

THE EUROPEAN DATA MARKET MONITORING TOOL REPORT 20.04.2018, 2018. Online access: http://datalandscape.eu/sites/default/files/report/EDM_D2.2_First_Report_on_Policy_Conclusions_20.04.2018.pdf.

WIEWIÓROWSKI, W. 2012. *Nowe ramy ochrony danych osobowych w Unii Europejskiej* (*New framework for the protection of personal data in the European Union*) (in:) Sibiga, G. (ed.), *Aktualne problemy ochrony danych osobowych* (*Current problems of personal data protection*), supplemental to Monitor Prawniczy, 7.

WIRSKA, P. 2017. *Rozdział V. Rozszerzenie zakresu stosowania unijnych przepisów na administratorów danych i podmioty przetwarzające z państw trzecich* (*Chapter V. Extending the scope of application of the EU provisions to data controllers and processors from third countries*) (in:) Kawecki, M. (ed.), Osiej, T. (ed.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia* (*General Data Protection Regulation. Selected issues*), Warsaw.