Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 383 · 2019

Zarządzanie 19

Ewa Kulińska

Opole University of Technology
Faculty of Production Engineering and Logistics
Department of Logistics
e.kulinska@po.opole.pl

Karolina Kulińska

University of Wrocław
Faculty of Law, Administration and Economics
Institute of Administrative Sciences
karolina.kulinska@uwr.edu.pl

GENERAL DATA PROTECTION REGULATION AND VIRTUAL SUPPLY CHAINS

Summary: The article presents the most important changes resulting from the entry into force of the General Data Protection Regulation (GDPR) for the creation and management of virtual supply chains and introduces sources of risk associated with enhanced personal data protection. This issue is fundamental to the future development of virtual supply chains mostly due to the wide territorial scope of application of the new GDPR. Moreover, the Regulation extended the definition of personal data (including, among others, IP addresses and cookie files) and introducing a series of obligations for personal data operators. Therefore, analysis of potential consequences for entrepreneurs at every stage of the supply chain is necessary both from legal and logistics perspective.

Keywords: GDPR, personal data, virtual supply chains.

JEL Classification: K2, M00, L86.

Introduction. Personal data protection and virtual supply chain management

Logistics cannot function without an effective and properly secured flow of information. On the one hand, information flows accompany the physical processes of product flow (flow generates information), on the other hand, they can be a regulatory aspect of processes (information can shape processes and their course) [Kulińska, Rut, 2016]. The information and communication technologies (ICT) are the unquestionably dominant and arguably most effective information carrier in the modern world. Among other factors, ICT and quick information exchange enabled the evolvement of virtual supply chains. This specific type of supply chains is characterized by the following features [Kisperska-Moroń, 2010]:

- temporariness,
- client-oriented,
- geographical dispersion,
- intensive use of information technologies,
- network organizational structure,
- using the key competencies of its participants.

Each of these characteristics makes entities involved in virtual supply chains (both entrepreneurs and clients) particularly vulnerable to the potential undesired data exposure or loss, which translates to non-compliance with General Data Protection Regulation (GDPR). In the following sections of this article, each of these areas will be examined from the perspective of GDPR provisions and put in the context of ICT technologies supporting modern logistic processes. Although these are tailored to a single category of a network of individual enterprises organized around a given project [Saban, Mawhinney, Drake, 2017], presented considerations may as well be applied to a classical model of supply chain [Wieczerzycki, 2012; Wyrwich-Płotka, 2018].

However, some conceptual explanations are necessary, due to the identity of notions used by EU legislator in a said Regulation and those functioning in logistics and management science, as they are not always interchangeable. Some might be simply confusing.

Personal means any information relating to an identified or identifiable natural person ("data subject"). In other words, the data subject is an individual human being. *A contratio* information related to legal persons, including commercial companies or organizational units, as a rule, would not fall under the scope of "personal data". Nonetheless, personal data of natural persons operating within structures of said legal persons (for example employees) or natural persons conducting economic activity on their own behalf and personal basis of the GDPR should be treated equally with other personal data, even if they disclose this data voluntarily for the sake of economic performance. The simplest example would be using one's name as a company brand (such as: "John Smith – transport services").

A question could be raised if that includes personal data of deceased persons. The classical attribute of every natural person in its legal capacity which, as commonly agreed by legal scholars, cannot be attributed to deceased persons. This is confirmed in recital 27 of GDPR, which, however, grants Member State's a discretion to regulate this matter in a more restrictive manner through domestic legislation. In case of the data of unborn child (*nasciturus*), the proposed interpretation is that if a child is born alive, all information relating to him or her and

collected during fetal life should be considered as personal data of that child. The latter problem, however, is primarily, if not exclusively, applicable to the provision of health care [Litwiński (ed.), Barta, Kawecki, 2017].

An identifiable natural person, under GPDR, is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. "Identifiable person" as a relative concept must be distinguished from "identified person". The latter refers to a situation where the data processor is able to connect given data with a particular person and no additional effort is needed to achieve this purpose on his behalf. This, perhaps contrary to business intuition, is not about merely gathering information about a given person but includes factual ability to distinguish the individual. With that said, it can easily be observed that it is often not a name or even an address that would allow us to extract a person. There may be a dozen of persons with the same name when a larger area is considered, and this set of data might not allow us for identification if we have never seen the person. Appearance on the other hand, especially when the company is equipped with advanced technical tools (monitoring, automatic identification) might lead to satisfactory and legally regulated results. Identifiability is, therefore, relative in at least threefold way, it depends on: type of processed information, available means that could be used for identification (in practice especially ICT means) and type of data operator (different data is being processed by the owner of a small online shop who processes it only for the sake of delivery of goods and big insurance company that is in possession of injury records of a given person).

Examples on how this approach is applied by the Court of Justice of the European Union are discussed in the following parts of this article. Yet, it should be observed that this subjective approach is coherent with the way a relation between data and information understood in logistics and management. Category of data, so registered facts, is inextricably linked with data processing. Information is encoded in data. Different data may be a source of the same information but also the same data may deliver a set of different information [Kulińska, Rut, 2016]. In other words, information is data processed in a way that ensures its utility for the recipient [Penc, 1995].

The notion of processing also got defined by EU law-giver. It shall be understood as an operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, re-

trieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The wording of analyzed provision ("such as") implies that the proposed catalog is not exclusive and may serve rather as guidance in an ambiguous situation. On the other hand, with that said, a phrase "any operation" allows to safely assume that when a dispute arises, a particular operation is most likely to be associated with personal data processing.

Another general category that must be well understood by the data controller are the risk and personal data impact assessment. GDPR [2016] recommends taking into account risks when performing a number of obligations imposed by it, such as:

- data protection by design and by default [Art. 25],
- maintaining a record or processing activities [Art. 30],
- implementing appropriate technical and organizational measures to ensure the security of processing and its accordance with the Regulation [Art. 24 and 32],
- notification of personal data breach to the supervisory authority and to the data subject [Art. 33 and 34],
- data protection impact assessment [Art. 35].

Regulation refers primarily to the risk to the rights of and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage [GDPR, 2016, Recital 75]. Further, the legal act introduces an exemplary catalog of such damages, including i.a.:

- social (where the processing may give rise to discrimination, damage to the reputation),
- breach of the law, including contractual rights and obligations (identity theft or fraud, loss of confidentiality of personal data protected by professional secrecy),
- economic loss (financial loss).

The proposed interpretation is concretizing the concept of risk in the perspective of the operation of specific economic entities (the personal data controller) and exposing the causes of risk. More importantly, it is a data subject-oriented, which understandable taking into account purpose of the regulation (protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data).

However, without compromising the pursuit for human rights protection, what matters for the entities involved in a supply chains is the risk of non-compliance with all the rules and standards set in the regulation that might mate-

rialize in a form of sanction, loss of reputation and client's trust and barriers in business development, each of them translating to major economic loss. Sanctions in GDPR reach value up to 20 000 000 EUR or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Impact of trust and reputation damages is harder to measure. According to survey data, a month before GDPR entry into force, about 40% of Polish citizens never heard about it [www 1]. In the UK, only 8% of adults say they have a good understanding of how their personal data is made available to third parties and the public by companies and organizations [www 2]. However, it shall be kept in mind, that GDPR implementation is supposed, though informatory obligations, raise this awareness among EU citizens, so this aspect shall be monitored in the future and an extended period of time in order to obtain reliable results. Finally, as barriers are regarded, enhanced protection standard might be costly and complicated for small and medium-sized enterprises (SME's). Due to a threat of big sanctions, they might take a legal risk-averse attitude, and refrain from the implementation of innovative solutions, such as cloud computing [Adamczewski, 2014].

Besides, a non-compliance risk has recently driven a large new area on audit and legal services market. It is an interesting phenomenon, since in most European countries data protection laws were present for many years, also secured by sanctions – in Poland even punished by imprisonment. All the more, GDPR perhaps highlighted the lack of due diligence of enterprises in that regard and, indirectly, the need for an interdisciplinary study of data protection implication in logistic processes.

1. Temporariness, network structure, and geographical dispersion

The virtual supply chain brings together a group of companies and institutions, often uniting them only periodically for certain tasks through occasional common goals, values, and activities. It is, therefore, temporarily appointed for the duration of a specific task, after which it is decomposed, and even during the implementation of the task, members of the virtual supply chain can participate in other networks or activate new ones. Changing the goals may mean reconfiguring the network and the entire organization. This is in contrast to the more traditional strategic alliances, as virtual supply chains fall apart when the reason for cooperation disappears [Kisperska-Moroń, 2010].

Each time it is necessary to precisely determine the time for which data will be stored and the legal relationship that connects each of the entities in the virtual supply chain. Processing shall be lawful only if and to the extent that at least one of the prerequisites set out in article 6 of GDPR applies. One, which is most likely to apply between producers, distributors, transport companies, etc. is where processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract. If the contract is unprecise, uncertain or incompatible with data protection policy implemented by data controller it shall be adjusted accordingly.

Such a review includes all partners, also those operating outsides of the European Union, due to the wide territorial scope of GDPR. 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 [GDPR, 2016, Art. 3(1)]. Even if the controller or processor are not established in the Union, Regulation applies to the processing of personal data of data subjects who are in the Union, where the processing activities are related to:

- 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
- the monitoring of their behavior as far as their behavior takes place within the Union [GDPR, 2016, Art. 3(2)].

Finally, it applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 3 sec. 2 of the GDPR [2016] emancipates the application of EU rules from the principle of territoriality, reducing the importance of the premise of paragraph 1 of that provision. Instead, it introduces a solution, which can be defined as "targeting", departing from territoriality to a protective principle. New EU data protection rules will apply to anyone who offers goods or services to data subjects in the Union or monitors the conduct of such entities, as long as the action occurs within the Union – thus "targeting" the data subjects. Provisions will apply regardless of whether the data subject is taking any activity. It is up to the controller or processor to assess whether certain actions, in particular, their nature, may result in the extension of obligations under the general regulation. The provisions of the regulation will cover providers of services on the Internet and, by way of behavioral monitoring, those that use profiling methods, e.g. for marketing purposes, or processing personal data within the so-called big data. It will happen no matter where someone who processes personal is located.

According to the opinion of M. Czerniawski [2016], the long-term consequence of such a territorial scope will be the need for many data controllers or processors from third countries to assume that specific data processing operations are governed by the general regulation as there is a risk that, some data subjects are from the European Union. So far-reaching extension of the territorial application of EU legislation raises opposition to some legal scholars and the concern of data controllers from non-Member States. In particular, small and medium-sized enterprises from third countries may not be aware of the existence of EU data protection laws and the fact that they are subject to them.

2. Client-oriented approach

As already mentioned, the idea of legislating personal data protection is not in itself innovative. Also, a concrete and directly binding regulation of human rights protection is not a classical area of EU harmonization. Nonetheless, the economic and social integration resulting from the functioning of the internal market together with the development of ICT and globalization have led to a substantial and inevitable increase in cross-border flows of personal data.

What GDPR does not directly mention is the rapid growth of the value of personal data in recent years. Data subjects, additionally to right to privacy, have a real economic interest in being granted effective legal tools to manage their personal data, such as the right to be forgotten. A report by the Boston Consulting Group in 2012 stated that the value created through digital identities would amount to approximately 8% of GDP for the EU-27 countries [www 3]. Not to mention commercial giants, such as Facebook, where profits are measured in billions of dollars [www 3].

The concept of quasi-possession of personal data by the data subject is supposed to turn back objectification of such data, where information important for a person's identity in the society are treated as any other sellable good. Parallelly, decentralized and safe systems that collect data, which would allow for its monetization. Whether this is desired evolution remains uncertain, as those solutions are based on the assumption that data subject genuinely understands and cares for its own rights.

3. Intensive use of information technologies

The starting point for consideration of what entrepreneurs must include in overall decision-making when protecting data subjects is again – definition of personal data. Similarly, to territorial jurisdiction, GDPR broadens the catalog of information that upon fulfillment of relativity criteria could be treated as personal data. One of them being an identification number and location data. A great example is the issue of IP addresses, which have raised many doubts in the past and was subject of deliberation by the Court of Justice of the European Union.

In the first case *Scarlet Extended*, the Court decided that dynamic IP addresses are personal data from the perspective of Internet Service Providers (ISP) because those addresses allow for the identification of a natural person. According to the Court, „(…) the injunction would involve a systematic analysis of all content and the collection and identification of user's IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data, for they allow those users to be precisely identified" [Judgment of 24 November 2011…, par. 26]. The reasoning in *Scarlet Extended* was further developed in *Breyer* case.

In *Breyer* case, the Federal Republic of Germany used to log dynamic IP addresses during each entry on federal websites. At the end of the session, various information was stored, including dynamic IP addresses. Mr. Breyer, a German citizen, wanted to challenge the federal actions. He brought a suit against the Federal Republic of Germany and claimed for a prohibitory injunction, alleging that dynamic IP addresses were personal data. To process such data, according to German law, consent was required, which had not been obtained. Therefore, the State could not store such IP addresses. The key aspect in this statement of facts was that single information that service provider (Germany) possessed – a dynamic IP – due to its unstable nature, would have to be combined with data gathered by ISP in order to make Mr. Breyer identifiable. In other words, the causal link leading to identification was extended. The Court noted that the definition of personal data implies the possibility of both direct and indirect identification [Judgment of 19 October 2016…]. The term "indirectly" means that it is not necessary for the information to be received without obtaining additional data to be identifiable. The rational approach should be taken when assessing what means a data controller can use. It was also considered that possession of the information necessary for identification by an entity other than the service provider does not preclude the possibility of being considered as personal data. However, there must exist legal means to obtain the necessary information from the ISP.

What follows from this reasoning, is that at least in theory, a constant screening and evaluation of data generated by an enterprise shall be implemented. It seems that this would be to the greatest detriment of big international enterprises using internet technologies, but despite of fact, that they indeed operate large sets of data they also already employ a number of well-educated specialists for data management so to significant degree this problem could be solved by staff training [see: Smoląg, 2011; Wyrwich-Płotka, 2018]. To the contrary, SME's would rather outsource data management and use cloud computing services. Providers of the latter also must comply with GDPR standard, although it may affect pricing for such services and lessens supervision of controller over data entrusted to him.

Conclusions

Presented consideration introduced only some basic, but key aspects of personal data management under GDPR. It allowed for emphasizing that in order to develop modern virtual supply chains interdisciplinary research is necessary. Regulatory law is penetrating more and more subtle areas on the border of private life and economic performance. Understanding the legal rules in isolation from the output of economic sciences and even some aspects of modern communication technology is impossible, or at least may lead to faulty applications. As theoretical research showed, further exploration of personal data within information flow is recommended. Also, a need for the development of risk assessment tools in terms of compliance can be recognized. In the context of GDPR, many of such tools and instructions are available for entrepreneurs for free, but no complex solution was yet proposed that would include damages on behalf of the data controller, and which would be universal and potentially applicable in other fields of law.

References

Adamczewski P. (2014), *Infrastruktura ICT dla sektora MSP w modelu cloud computing* „Zeszyty Naukowe Uczelni Vistula", nr 35, pp. 115-128.

Czerniawski M. (2016), *Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej* [in:] E. Bielak-Jomaa, D. Lubasz (eds.), *Polska i europejska reforma ochrony danych osobowych*, Wolters Kluwer, Warszawa, pp. 86-101.

GDPR (2016), 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. Dz. Urz. UE L. 119/1.

Judgment of 19 October 2016, *Breyer*, C-582-14, ECLI:EU:C:2016:779.

Judgment of 24 November 2011, *Scarlet Extended*, C – 70/10, ECLI:EU:C:2011:771.

Kisperska-Moroń D. (2010), *Kompetencje logistyczne firm polskich jako czynnik rozwoju wirtualnych łańcuchów dostaw*, „LogForum", vol. 6, nr 1, pp. 3-12.

Kulińska E., Rut J. (2016), *Procesy decyzyjne w logistyce i pokrewnych obszarach badawczych*, Oficyna Wydawnicza Politechniki Opolskiej, Opole.

Litwiński P. (ed.), Barta B., Kawecki M. (2017), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, C.H. Beck, Warszawa.

Penc J. (1995), *Decyzje w zarządzaniu*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków.

Saban K., Mawhinney J.R., Drake M.J. (2017), *An Integrated Approach to Managing Extended Supply Chain Networks*, "Business Horizons", Vol. 60, Iss. 5, pp. 689-697.

Smoląg K. (2011), *IT Solutions in the Context of Operation of Virtual Supply Chain*, "Gospodarka Materiałowa i Logistyka", nr 12, pp. 84-88.

Wieczerzycki W. (2012), *Możliwości rozwoju e-logistyki* [in:] W. Wieczerzycki (ed.), *E-logistyk*a, PWE, Warszawa, pp. 219-236.

Wyrwich-Płotka S. (2018), *Wirtualna praca w łańcuchu dostaw*, Difin, Warszawa.

[www 1] https://arc.com.pl/Polacy-bez-szerszej-wiedzy-o-RODO-blog-pol-1535059522.html (accessed: 30.05.2018).

[www 2] https://londoneconomics.co.uk/wp-content/uploads/ (accessed: 21.04.2018).

[www 3] https://www.bcg.com/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity.aspx (accessed: 21.04.2018).

OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH A WIRTUALNE ŁAŃCUCHY DOSTAW

Streszczenie: W artykule zaprezentowano najważniejsze zmiany wynikające z wejścia w życie ogólnego rozporządzenia o ochronie danych osobowych (RODO) w zakresie tworzenia wirtualnych łańcuchów dostaw i zarządzania nimi oraz przedstawiono źródła ryzyka związane ze zwiększoną ochroną danych osobowych. Kwestia ta ma zasadnicze znaczenie dla przyszłego rozwoju wirtualnych łańcuchów dostaw, głównie ze względu na szeroki zakres terytorialny zastosowania nowych przepisów. Ponadto rozporządzenie rozszerzyło definicję danych osobowych (kwalifikując do tej kategorii m.in. adresy IP i pliki cookie) oraz wprowadziło szereg obowiązków dla operatorów danych osobowych. Analiza potencjalnych konsekwencji wprowadzonych zmian dla przedsiębiorców na każdym etapie łańcucha dostaw jest zatem konieczna zarówno z perspektywy logistyki, jak i zgodności z prawem (*legal compliance*).

Słowa kluczowe: RODO, dane osobowe, wirtualne łańcuchy dostaw.