SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIES NO. 145

PROTECTION OF PERSONAL DATA IN THE FREIGHT FORWARDING INDUSTRY

Tomasz SZEWC

Politechnika Śląska w Gliwicach, Wydział Organizacji i Zarządzania, Zabrze; tszewc@polsl.pl,
ORCID: 0000-0001-6326-4626

Purpose: The aim of this article is to analyze personal data protection requirements specifically in the context of the freight forwarding industry.
Design/methodology/approach: This article looks into the legal regulation of personal data protection and examines its application by freight forwarding companies, taking into account the specific needs found in this industry. This article should provide managers with the knowledge of how to properly protect personal data while increasing this way the company's competitive edge on the market. By analyzing legally binding laws and explaining them in a comprehensive way, focusing on the needs of the freight forwarding industry and the way it handles personal data.
Findings: The study revealed that the handling of personal data in the freight forwarding industry carries a high data risk theft. Moreover, a company in the freight forwarding industry can take on many roles in relation to personal data (i.e. controller, co-controller, or contract processor) and takes on the financial responsibility for that personal data.
Originality/value: The article presents the processes of handling personal data by a freight forwarding company and a plan to be followed while it implementing of the rules of the GDPR. It is valuable for managers of the freight forwarding companies.

Keywords: freight forwarding, personal data protection, management.

1. Introduction

A freight forwarding agreement is of great importance in economic turnover, connecting the seller or manufacturer of goods with the carrier (or directly with the consignee, if the forwarding also includes carriage). Dispatching and transporting of consignments is an activity so complex and distant from the sender's basic activity that they often decide not to undertake these tasks on their own, but to hand them over to specialised entities. This requires such activities as "professional advice, preparation of the consignment for transport (packaging, weighing, counting, marking, sorting, etc.), ordering a means of transport, delivering the

consignment to the place of shipment, issuing transport documents, concluding a contract of carriage, carrying out loading operations, insurance of the consignment, convoying, carrying out customs clearance, amending the contract of carriage, receiving the consignment and transport documents, checking the condition of the consignment, drawing up a damage report on behalf of the consignee, temporary storage, or storage of the consignment, etc." (Górski, 1976, pp. 576-577). For this reason, a significant development of the freight forwarding market can be observed over the recent years (Bartczak, and Barańska, 2016; Wojciechowski, 2012), supported by the Internet and on-line trade. A distinguishing feature of freight forwarding is also the volatility of freight forwarding company customers, often they provide services to some people on a one-off basis.

This all makes the processing of personal data an important aspect of a forwarder's activity. Given the profound change of legal regulations concerning personal data protection as of 25 May 2018 (The General Data Protection Regulation, 2016, hereinafter referred to as the GDPR) and competition enforcing improvements in the quality of services (Kruczek, Przybylska, and Żebrucki, 2015), this issue is still relevant from the point of view of the management of a freight forwarding company and valid in the context of financial penalties in case of violation of the GDPR. Moreover, a freight forwarder cannot refuse to apply the Regulation since he/she cannot claim (because of the professional nature of the activity) that it does not apply to him/her as he/she is a natural person carrying out activities of a purely personal or domestic nature [Article 2(2)(c) of the GDPR].

2. Methods

The purpose of this article is to analyze the specific problems associated with the management of a freight forwarding company in terms of processing and protection of personal data in the context of legal requirements. Therefore, a formal and dogmatic approach will be applied, consisting in the analysis of legal acts and literature.

3. Discussion

3.1. Freight forwarding agreement

A forwarding contract is one of the nominate contracts, that is, regulated by the law. In accordance with Article 794 of the Civil Code, by a freight forwarding contract the forwarder undertakes, for remuneration within the scope of his/her business activity, to send or receive the consignment or to perform other services connected with its carriage. It is worth

emphasising that as a rule a freight forwarder does not carry out the transport of a consignment, but only sends and receives it on behalf of the customer, however the Civil Code allows the freight forwarder in Article 800 to extend the contract further to carry out the transport on their own.

A contract formulated in this way deviates from the common understanding of freight forwarding — according to the Polish Dictionary, freight forwarding is "carriage and delivery of goods made by a transport company" (The PWN Polish Dictionary) or "transport agency consisting of sending goods and performing activities connected with sending or receiving a shipment" (Polish Dictionary, p. 285). The common definition combines two other nominate contracts — the contract of carriage and the contract of delivery, which does not entirely correspond to the truth (according to Article 605 of the Civil Code, by the contract of delivery the supplier undertakes to manufacture and deliver the items marked only as to their kind and to deliver them in parts or periodically, and the consignee is obliged to collect these items and pay). The supplier's obligations therefore include the manufacture of the goods, which differs significantly from the scope of the forwarder's obligations under the Civil Code. Nevertheless, apart from these doubts, it is possible to distinguish the freight forwarding contract in the broad and narrow sense, depending on whether it includes or not the carriage of goods.

In the specialist literature, however, freight forwarding is defined as an activity facilitating the use of transport services, namely the organisation of transport processes and other related activities. As a result, the duty of a forwarder covers the whole process of delivery of a shipment, from the consignor to the consignee (Kędzior-Laskowska, 2014; Salomon, 2013; Słowiński, 2008).

Such a formulation of a forwarding contract has significant consequences. Firstly, it is a contract for the benefit of a third party, that is, a contract in which there is a wider circle of creditors. Its execution may be demanded not only by the person ordering the forwarding, but also by the consignee. Secondly, forwarding services are provided only within the framework of the activity of the company providing the forwarding services. For this reason it is also a qualifying agreement (Gudowski, 2013). Being a professional activity, forwarding is characterised by higher standards of requirements as to the quality of services provided, as well as increased responsibility [Article 355, §2 of the Civil Code]. Thirdly, the legal situation of a forwarder is complex, as he/she enters into many legal relations (e.g. with principals, with consignees, with his/her own employees, with public administration bodies, with injured parties or perpetrators of damages etc.).

3.2. Personal data processing in a freight forwarding company

The running of each business involves the management of various types of processes which result in the creation of a product (service) that is an essential part of its operations and meets its customers' needs (Müller, and Rupper, 2000; Maleszka, 2000). This process consists of a number of related tasks (Hammer, 1999). According to the popular division of business

processes by M. Porter, they can be divided into primary and secondary processes. Secondary processes are to support the main activity of the company and include management of the entire entity, human resources management, procurement and development activities (Porter, 1985). There is no doubt that the processes connected with personal data processing are secondary processes in a freight forwarding company. They support and complement the main activity and refer to the management of the entire entity. It arises from their scope, as they concern both the subject of activity (i.e. provision of services) and aspects of internal organisation (i.e. ensuring its operations).

The processes of personal data processing permeate all stages of service provision by a freight forwarding company, starting from marketing and promotion. Running a website, a fanpage, sending a newsletter and other forms of reaching out to customers require processing of their personal data. When concluding a contract with the customer, the entrepreneur processes their data either as a contractor or as a beneficiary of the contract (i.e. a third party), and finally obtains a confirmation of delivery (and processes the data further, e.g. by sending a confirmation of delivery to the consignor). From an internal point of view, a freight forwarding company looks for and concludes contracts with its own employees and contractors. The employment of drivers, pilots, etc. requires the processing of their working time data (e.g. readings from tachographs), as well as the collection of their data from carriers and making them available to operators (e.g. to verify that the person is entitled to receive the goods). There are also frequent vehicle location data based on GPS sensors (telemetry) and recordings from cameras documenting the image outside and sometimes inside vehicles. Vehicle traffic also involves the risk of collisions and violations of regulations governing this traffic, i.e. data on the perpetrators or victims of collisions and fines imposed on drivers. Certainly, it will be more than average often required in such a company to process personal data in matters related to claims, not only due to traffic accidents, but also due to non-performance or improper performance of a contract, as well as due to some torts (e.g. thefts). It is clearly visible that the forwarding activity is related to the use of personal data in many areas, data of high individual variability and high intensity of flow between entities involved in the process of goods forwarding, and their transfer is more and more often carried out using new technologies. It is also standard to share data with other entities. In this industry, it is even stated that in the forwarding activity, data processing takes place to a degree unprecedented in other industries (Fijałkowska).

3.3. The notion of personal data, the types and reasons for the processing in the context of the operation of a freight forwarding company

Personal data means information on an identified or identifiable natural person [Article 4(1) of the GDPR]. Information is an intangible communication which reduces uncertainty (increases certainty) and therefore allows for the characterisation of a specific situation and, in case of personal data, of a specific person (Hoc, and Szewc, 2014; Szpor, 2008).

This communication may take any form, e.g. paper records, tachograph disk recordings, IT system recordings, etc. (Opinion of the Article 29 Working Party). The information concerns a natural person if it is information about that person (Lubasz, and Bielak-Jomaa, 2018). A natural person, in turn, is a person from birth until death (Fajgielski, 2018; Hoc, and Szewc, 2014; Krzysztofek, 2016). However, information about natural persons who are economic entities are not protected (although they are still personal data) [Article 45(1) in connection with Article 2(2)(1) of the Act on the Central Registration and Information on Economic Activity] and do not have to be protected according to the GDPR (Fajgielski, 2018).

Similarly, the content of personal data can be discretionary as long as it concerns an identified person, i.e. one whose identity is established directly and immediately in a way that distinguishes him/her from other people (Lubasz, 2018). Normally, personal data will consist of identifying information (e.g. name and surname) and further information concerning that person, e.g. data of the consignor, residential address of the consignee, address of delivery, if different from the residential address, telephone number, PESEL (Personal ID Number) of the employee, registration number of the vehicle the person is driving, data registered in the GPS tracking system, biometric data, etc. (Fajgielski, 2018).

A person can be identified both directly and indirectly. The difference is that in the latter case identification requires some additional operations combining data from different sources, e.g. combining the consignment number with the address of the consignee (Fajgielski 2018; Krzysztofek, 2016; Mednis, 1999). However, as far as personal identification is possible, data should be protected in accordance with the standards adopted in the General Data Protection Regulation 2016/679[i].

Personal data are divided into ordinary, special categories of data and data on the violation of the law [Articles 9-10 of the GDPR]. Among the special categories of data, for example, information about an employee's disability (which is related to the payment of fees to the PFRON or restrictions at work) may be relevant for a freight forwarding company[ii] and biometric data, i.e. data which concern the physical, physiological or behavioural characteristics of an individual and enable or confirm the unequivocal identification of that individual, such as a facial image or dactyloscopic data or the voice [Article 4(14) of the GDPR]. These data result from specific technical processing, that is, using biometric techniques, which is automated (Jaroszewska-Choraś, 2016).

The necessity of processing data on violations in the activities of freight forwarding companies is obvious. First of all, when liability is established for a traffic violation registered by an automatic recording device, or when the driving license is suspended.

The consequence of distinguishing between ordinary and other data is, first and foremost, that there are different rationale for their processing. The rationale for data processing is when the processing becomes possible. In other words, they raise the ban on data processing (Fajgielski, 2018; Hoc and Szewc, 2014). The following rationale will be particularly relevant in the activity of a freight forwarding company:

a) in reference to ordinary data:
   - the consent of the data subject (e.g. to the processing of the IP address when browsing the company website),
   - execution of the contract concluded with the data subject (e.g. providing the driver with the data of the consignor who is a natural person in order to collect the consignment, accounting for drivers' working time on the basis of tachographs, giving the dimensions for the selection of working clothing),
   - execution of a legal obligation imposed on a freight forwarding company (e.g. storing customer data for accounting purposes),
   - execution of legally justified business — this is every legitimate business (Lubasz, and Bielak-Jomaa, 2018) of the controller or a third party (on the basis of this rationale you can e.g. carry out direct marketing or provide the consignors of shipments with drivers' data in order to make the person collecting the shipment from the consignor credible and thereby protect it against theft of shipments),
b) in reference to special categories of data:
   - the consent of the data subject,
   - the fulfilment of obligations and specific rights in the field of labour law, social security and social protection, as far as this is allowed under national law and provides for adequate safeguards for the interests of the data subjects (on the basis of this rationale, data of disabled employees will be processed),
   - processing is necessary for the identification, assertion or defence of claims or in the exercise of justice by the courts (in this case, data may be processed, e.g. of the perpetrators or victims of damage),
c) in reference to data on infringements — only if the regulations allow it (when hiring for positions with no criminal record, e.g. customs agent, licensed security officer).

3.4. The status of the freight forwarder in relation to the processing of personal data

In relation to the personal data processed, the freight forwarder may be involved in one of three roles: the controller, the co-controller or the processor. It depends on the form of a contract with the principal, as a result of which he/she can act on his/her behalf or on his/her own behalf. Such a possibility is provided by Article 794(2) of the Civil Code (Górski, 1976).

The status of controller and co-controller is relatively similar. The controller is an entity which decides on its own about the purpose and method of data processing [Article 4(7) of the GDPR]. The status of a co-controller will occur when two or more entities mutually take these decisions (which may be the case if two or more freight forwarding companies cooperate). The processor processes data on behalf of the controller.

The freight forwarder will act as a data processor, especially in case of execution of the forwarding contract on the basis of which he/she acts on behalf of the principal and if he/she receives the data of their employees (e.g. drivers, so they are not "own" data of the freight

forwarding company) from these subcontractors. In other cases, however, the freight forwarder acts as controller or co-controller (especially with regard to their employees or customers).

The activities of the controller must comply with data processing principles. These principles are certain values considered by the legislator to be the most vital, and any activities of the controller should always respect them, especially those undertaken on the basis of specific provisions of the GDPR (Kuba, 2016; Fajgielski, 2008; Fajgielski, 2018). The principles of data processing include:

a. lawfulness, requiring all data processing activities to be lawful,
b. reliability, according to which data processing must be socially acceptable, i.e. it must not infringe the rights and freedoms of the individual,
c. transparency, requiring that processing operations are organised in such a way that they are transparent to the data subject (which primarily relates to information and messages to data subjects — they must be clear and understandable),
d. purpose limitation, requiring that the data must be collected only for the purposes explicitly indicated by the controller (they must therefore be articulated), legally justified (i.e., as can be expected when looking at the subject of the activities of a particular controller) and used only in accordance with that purpose (and therefore, for instance, a database of recipients of the consignments cannot be created in order to send them promotional materials),
e. data minimisation, prohibiting the collection of excessive amounts of data; instead, the scope of the data processed should be as limited as possible as long as it is sufficient to achieve the purpose of the processing (in this case, it is excessive to provide the sender of the consignment with the driver's identity card number, since the first and last name is sufficient),
f. accuracy, according to which the data should be truthful and constantly updated — this imposes an obligation on the managers of a freight forwarding company to introduce mechanisms allowing for immediate deletion or rectification of data (such a mechanism may be the possibility to change the address or delivery date on-line),
g. storage limitation, which refers to time, and therefore data may be stored as long as necessary to achieve the purpose, but this does not mean that immediately after the execution of the contract, the data should be deleted, various claims may be associated with the execution of the contract, and therefore the end date of storage of data should be the expiry of the claims limitation period, which for the contract of forwarding is one year from the delivery of the shipment (in case of damage or loss), or from the date on which it was to be delivered (in case of delay or non-delivery, or from the date of execution of the order (in case of other types of claims),
h. integrity and confidentiality — assuming data security (preventing access to the data by unauthorised persons) and its protection against unauthorised or unlawful processing (which occurs e.g. when a courier hands over a shipment in the absence of the consignee

to a neighbour asking for it to be handed over to the consignee) and accidental loss, destruction or damage (e.g. as a result of a hacking attack on the customer database or theft of addressed shipments from the means of transport) — by implementing appropriate safeguards,

i. accountability, requiring the controller to demonstrate the fulfilment of the requirements set out in the GDPR, and thus it will be essential to implement procedures to ensure compliance with the regulations, prepare documentation setting out the measures taken, and record that the processing operations were carried out in accordance with the law (Lubasz, and Bielak-Jomaa, 2018).

The accountability principle therefore entails an obligation to record processing operations. Such a register should contain the elements listed in Article 30(1) of the GDPR. While there is an exemption from this obligation for entities employing fewer than 250 people, even such entities have to keep a register if this may lead to a risk of violation of the rights and freedoms of the data subjects (it seems that in the case of a freight forwarding company such a risk does not occur), if it is of a permanent nature or covers specific categories of data (and such situations already occur in a freight forwarding company). Therefore, it can be presumed that, as a rule, a freight forwarding company is obliged to keep such a register[iii].

Further responsibilities of the data controller may include:

a. cooperation with the supervisory authority [Article 31],
b. notification to the supervisory authority of a breach of data security, unless the breach is unlikely to result in a risk to the rights or freedoms of the data subject [Article 33],
c. notifying the data subject of a breach of data security likely to cause a high risk to infringe the rights or freedoms of individuals [Article 34].

If the freight forwarder is one of the co-controllers, this requires agreement between them and a clear and transparent definition of their respective responsibilities for carrying out the obligations defined in the regulation [Article 26], e.g. indicating who keeps a register of processing operations.

The status of a contract processor entails a number of obligations, such as:

a. the conclusion of a contract with the data controller, authorising the processing and setting out the specific issues listed in Article 28(3) of the GDPR,
b. obtaining authorisation to subcontract data processing,
c. implementing the required safeguards for personal data by technical and organisational measures,
d. keeping a register of processing activities [Article 30(2) of the GDPR],
e. assisting the controller in fulfilling the obligations of Articles 32-36 of the GDPR and to respect the rights of the data subject,
f. notifying the controller of a breach of data security [Article 33(2)],
g. allowing the controller to control the processing [Article 28(3)(h)].

3.5. Respect for the rights of data subjects

The protection of personal data does not take the form of orders and bans addressed only to administrators and processors, but also implies the active participation of the data subject, granting him/her a number of powers to influence the conduct of those who process his/her data. Furthermore, it is worth mentioning that the exercise of the rights of the data subject must take place within the relevant time limits [Article 12 of the GDPR].

These rights include:

a. the controller's ex officio fulfilment of the information obligation to provide the data subject with information concerning the controller and data processing, the scope of this obligation varies depending on the collection of data directly (directly from the data subject) or indirectly (the scope of the required information is indicated by Articles 13 and 14 of the GDPR). As far as the activity of a freight forwarding company is concerned, this obligation should be fulfilled with regard to employees, customers, consignors and consignees;
b. confirmation of the processing of personal data by a particular controller, obtaining actual access to the data and a range of information related to the processing (e.g. about the purpose), as listed in Article 15 (this is a similar entitlement to the information obligation of the controller, although not ex officio, but at the request of the person concerned). Hence, it is necessary to answer people's inquiries whether their data are processed by a freight forwarding company;
c. the rectification of data (implementing the accuracy principle), according to which the data subject has the right to request from the controller the rectification of data which are inaccurate [Article 16]. The company should then provide for procedures for easy rectification and amendment of the data;
d. the transfer of data processed by automated means between administrators, where the data are processed either on the basis of consent or in connection with the execution of a contract. For instance, the customer can change the freight forwarder and all information concerning the shipment, addresses, etc. should be given to the new freight forwarder;
e. objection to the processing of data for the purpose of pursuing legitimate interests. Such objection is absolutely binding if the purpose of the processing was direct marketing of the services of the freight forwarding company, in case of the other grounds, the data may be processed if it is sufficiently justified and overrides the interests, rights and freedoms of the data subject [Article 21];
f. the restriction of processing to data storage, which can be used mainly in case of incorrect processing [Article 18];

g. right to erasure (right to be forgotten) — this is the possibility for data subjects to request from a particular controller the deletion of data (and thus literally 'forgetting' that person), however, its implementation depends on whether the controller does not actually need further processing of that person's data [Article 17][iv]. As mentioned, the statute of limitations for claims under a freight forwarding contract occurs one year after its execution, thus after such a period of time the data subject can effectively claim forgetting;
h. exclusion from automated (i.e. without human intervention, solely by machine or software) decision making in cases which significantly affect or produce legal effects on the data subject [Article 22]. This power cannot be exercised if the data are necessary for the conclusion or performance of a contract between the data subject and the controller, or if the law allows for such decision making. In the case of a freight forwarding company, an example can be the calculation of the amount due for a shipment using an on-line form. Since this is necessary for the conclusion of a contract, it is not possible to demand a person to calculate such a fee. On the other hand, the allocation of a consignment by a computer program to a particular means of transport will not entitle the data subject to exercise this right, as it does not have any real impact or legal effects on him/her.

The exercise of the right of rectification, restriction of processing and the right to be forgotten implies the obligation for the controller to notify all data subjects to whom the data have been transferred, so that they can also ensure the exercise of the data subject's rights.

3.6. Data transfers to third countries

The execution of a freight forwarding contract may require the shipment or transport of goods outside the EU, to so-called third countries (which obviously also involves the transfer of personal data). In this case, the GDPR tightens the conditions for this form of data processing by devoting a separate chapter to it. From the point of view of the freight forwarder, Article 49 will be the most relevant here and the basic rationale for transferring the data to a third country can be considered to be the necessity of the transfer for the performance of a contract between the data controller and the data subject (if, for instance, the sender dispatches the shipment to his/her own address in the third country) or a contract concluded in the interest of the data subject (if the consignee acts as a third party). For matters related to the functioning of the freight forwarding company as a business entity, the transfer of data in order to establish, pursue or protect claims (e.g. damage to a car), the protection of the vital interests of the data subject (e.g. information on the driver injured in an accident) may also be involved. It is also likely that there would be a transfer for important reasons of public interest, e.g. an investigation by third country authorities into drug smuggling in consignments sent by a freight forwarder.

3.7. Creation of a personal data protection system

Several fundamental guidelines need to be taken into account when creating a personal data protection system:

a. considering data protection already at the design stage [*privacy by design* — Article 25(1) of the GDPR], which means taking into account appropriate data protection at the early stage of the design of data processing (Cavoukian; Wiewiórowski, 2012),
b. setting data protection as a default [*privacy by default* — Article 25(2)], according to which maximum protection is to be guaranteed to the data subject from the start of the processing and the possible weakening of protection is to depend on his/her decision (Krzysztofek 2016),
c. carrying out risk assessment of the risks of violation of individuals' rights and freedoms according to the likelihood and severity of the threat, on the basis of which appropriate (proportionate) security measures are implemented, taking into consideration the state of knowledge and costs,
d. appointing of a Data Protection Officer (DPO), in accordance with Article 37.

The appointment of a DPO is as a general rule optional. However, in some cases it is obligatory and it is also necessary to consider whether such an obligation will apply to the freight forwarding company. This may be the case under Article 37(1)(b), according to which a controller or processor shall appoint DPO where their main activity consists of large-scale processing operations which, by their nature, scope or purpose, require regular and systematic monitoring of data subjects. The activity of a freight forwarding company certainly meets these conditions — such companies usually operate on a large scale (they serve thousands of domestic or international customers), and the nature of the activity also entails the risk of data security breaches (data are made available to numerous entities, there is a wide use of new technologies, personal data on shipments are moved, which involves the risk of traffic accidents and data loss or damage, there are specific data such as tachographs, driver cards, etc.). The DPO can also be designated for a group of companies, as long as this does not prevent him/her from being contacted. The DPO shall perform the tasks indicated in Article 39.

4. Summary

Intensive personal data processing in a freight forwarding company is combined with a high risk of data threatening and is a challenge for the managerial staff. It also triggers additional management processes with high financial responsibility.

When considering the issue of personal data protection in the freight forwarding activity, it should be stated that the implementation of the rules of the GDPR requires following a specific scheme. Firstly, it is necessary to identify and classify personal data occurring in the company and the ways of data processing. For this reason, it will be essential to know such notions as "personal data", types of personal data and "processing". Afterwards, it must be determined whether processing is permitted on the basis of one of the rationale and whether the principles of processing are observed. The type of data and the rationale for processing are management problems because, if there is consent, there is an additional need to implement procedures to obtain the data properly, and to waive it if another rationale entitles the data to be processed (then consent is unnecessary). It is further required to verify whether personal data are shared with third parties as well as with third countries. Then it is necessary to consider how to secure the data and the procedures to be followed in case of data loss and how to delete them (i.e. building a data protection system). The data protection must be appropriate to the results of the risk analysis. The rights of the data subjects must also be respected within the time limits imposed and the notification procedures to the supervisory authority and data subjects.

Another issue which has a strong impact on management processes is the presence of a freight forwarding company in many roles in relation to personal data (i.e. controller, co-controller, or contract processor). Acting as a controller, a freight forwarding company may, of course, delegate the related tasks to another entity (outsourcing), but must select it with due diligence. In the case of co-administration, it will be required to share responsibilities with the possibility of creating a contact point for data subjects. Theoretically it is feasible to divide tasks here, but it must not be forgotten that these people can exercise their rights by applying to any of the co-administrators, which also requires the creation of appropriate procedures.

They will also be demanded in case of loss of the status of controller following the transfer of data to another entity, since the GDPR requires the transfer of data 'in a structured, commonly used machine-readable format', which indicates at least the need to convert the data into such a format, unless commonly used software has to be implemented for data processing.

References

1. Bartczak, K., and Barańska, A. (2016). Tendencje rozwojowe na rynku usług spedycyjnych w Polsce. *Autobusy, 4*, 109-114.
2. Cavoukian, A. *Privacy by Design. The 7 Foundational Principles*. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf, 24.06.2019.
3. Fajgielski, P. (2018). *Ogólne rozporządzenie o ochronie danych osobowych, ustawa o ochronie danych osobowych. Komentarz*. Warszawa: Wolters Kluwer.

4. Fajgielski, P. (2008). Zasady ogólne przetwarzania danych osobowych. In: G. Goździewicz, M. Szabłowska (Eds.), *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych* (pp. 17-26). Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora".
5. Fijałkowska, A. *Ochrona danych osobowych w branży transportowej – zalety procesu wdrażania RODO*. Retrieved from http://www.prawoilogistyka.pl/aktualnosci/ochrona-danych-osobowych-w-branzy-transportowej-zalety-procesu-wdrazania-rodo/, 24.06.2019.
6. Górski, W. (1976). Spedycja. In: S. Grzybowski (Ed.), *System prawa cywilnego. Tom III, cz. 2 – Prawo zobowiązań – część szczegółowa* (pp. 576-604). Ossolineum.
7. Gudowski, J. (2013). *Kodeks cywilny. T. III, cz. 2. Zobowiązania*. Warszawa: Lexis Nexis.
8. Hammer, M. (1999). *Reinżynieria i jej następstwa.* Warszawa: PWN.
9. Hoc, S., and Szewc, T. (2014). *Ochrona danych osobowych i informacji niejawnych*. Warszawa: C.H. Beck
10. Jaroszewska-Choraś, D. (2016). *Biometria. Aspekty prawne*. Gdańsk: Uniwersytet Gdański.
11. Kędzior-Laskowska, M. (2014). Transport i spedycja – zakres pojęciowy. In: T. Wierzejski, and M. Kędzior-Laskowska (Eds.), *Transport i spedycja* (pp. 7-26). Olsztyn: Uniwersytet Warmińsko-Mazurski.
12. Kruczek, M., Przybylska, E., and Żebrucki, M. (2015). Założenia do badania potencjału innowacyjnego przedsiębiorstwa branży transport-spedycja-logistyka. *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 78*, 221-234.
13. Krzysztofek, M. (2016). *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*. Warszawa: C.H. Beck.
14. Kuba, M. (2016). Zasady prawa ochrony danych osobowych. In: T. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków* (pp. 99-120). Warszawa: Difin.
15. Lubasz, D., and Bielak-Jomaa, E. (2018). *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warszawa: Wolters Kluwer.
16. Maleszka, A. (2000). *Wprowadzenie do statystycznego zarządzania procesem.* Poznań: Akademia Ekonomiczna.
17. Manganelli, R., and Klein, M. (1998). *Reeingineering. Metoda usprawniania organizacji.* Warszawa: Wydawnictwo Ekonomiczne.
18. Mednis, A. (1999). Ochrona prawna danych osobowych a zagrożenia prywatności – rozwiązania polskie. In: M. Wyrzykowski (Ed.), *Ochrona danych osobowych* (pp. 167-196). Warszawa: Instytut Spraw Publicznych.
19. Müller, R., and Rupper, P. (2000). *Process Reengineering.* Warszawa: Astrum.
20. Porter, M. (1985). *Competitive Advantage.* New York: Free Press.
21. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz.Urz. L 119 (2016).
22. Salomon, A. (2013). Spedycja a komodalność transportu. *Zeszyty Naukowe Politechniki Śląskiej. Transport, 80,* 113-124. doi: https://doi.org/10.20858/sjsutst.1983.1.1.
23. Słowiński, B. (2008). *Wprowadzenie do logistyki*. Koszalin: Politechnika Koszalińska.
24. *Słownik języka polskiego PWN*. Available online https://sjp.pwn.pl/szukaj/spedycja.html, 24.06.2019.
25. Szpor, G. (2008). Pojęcie informacji a zakres danych osobowych. In: P. Fajgielski (ed), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia* (pp. 7-20). Lublin: Katolicki Uniwersytet Lubelski.
26. Szymczak, M. (1981). *Słownik języka polskiego, t. III*. Warszawa: PWN.
27. Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, Dz.U. poz. 1145 (2019).
28. Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz o zatrudnianiu osób niepełnosprawnych, Dz.U. poz. 511 (2018).
29. Ustawa z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o działalności gospodarczej i punkcie informacji dla przedsiębiorcy, Dz.U. poz. 674 (2018).
30. Wiewiórowski, W. (2012). Privacy by Design jako paradygmat ochrony prywatności. In: G. Szpor, W. Wiewiórowski (Eds.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług* (pp. 13-30). Warszawa: C.H. Beck.
31. Wojciechowski, A. (2012). Rynek usług logistycznych w Polsce – analiza, perspektywy rozwoju. *Logistyka, 4*, 1382-1395. Retrieved from https://www.logistyka.net.pl/bank-wiedzy/logistyka/item/download/78523_fcac31e10b2baef88da727a2393a5f65, 27.06.2019.

Footnotes

[i] The obligation to protect data is not unlimited. According to Recital 26 of the GDPR, „to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, […] either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". This means that if there is any objectively possible and accessible way of identifying a person from the data held, that data must be protected.

[ii] According to Article 21(1) of the Act on Occupational and Social Rehabilitation, each employer with more than 25 full-time employees is obliged to pay a fee to the State Fund for Rehabilitation of Disabled People, unless it employs at least 6% of disabled people. The working time of disabled people is limited by Article 15 et al. of this Act.

[iii] Recording of processing activities does not exhaust the documentation obligations. It can also be mentioned that the documentation of personal data protection breaches [Article 33(5) of the GDPR], the documentation of the notification obligation to the President of the Personal Data Protection Office [Article 33(3)] and the documentation of the risk assessment of data processing using new technologies [Articles 35 and 36].

[iv] The same effect has the objection to data processing and the withdrawal of consent to data processing.