VILNIUS TECH
Vilnius Gediminas Technical University

12th International Scientific Conference

BUSINESS AND MANAGEMENT 2022

May 12–13, 2022, Vilnius, Lithuania

ISSN 2029-4441 / eISSN 2029-929X
ISBN 978-609-476-288-8 / eISBN 978-609-476-289-5
Article Number: bm.2022.927
https://doi.org/10.3846/bm.2022.927

*LEGAL BUSINESS ENVIRONMENT* *http://vilniustech.lt/bm*

# PRIVACY PROTECTION IN THE TRANSMISSION OF PERSONAL DATA IN BUSINESS – INSIGHTS FROM LITHUANIA

Darijus BEINORAVIČIUS, Violeta KERŠULIENĖ

*Faculty of Business Management, Vilnius Gediminas Technical University, Saulėtekio al. 11, Vilnius, Lithuania*

Received 21 March 2022; accepted 4 April 2022

**Abstract.** In recent decades extremely rapid technological advances have been seen that have changed many areas of daily life and the business environment. These technological advances are leading to the increasing use of electronic communications networks and cloud technologies by individuals, businesses, and organizations to provide services, store, and manage records, especially in the electronic space. The increasing use of these links offers an unprecedented opportunity to systematically collect and use a variety of data (including personal data) for different purposes. Information and data collected and processed with the help of technology are used not only for the purposes of meeting the needs of natural and legal persons but for various other reasons too. In the context of the collection and the use of personal data, which is very widespread in business relations, ensuring the individual's right to privacy becomes problematic, especially if the data have to be transferred to third countries outside the EU. The authors of the article provide an example of how the case of data transfer to a third party was resolved in the Lithuanian courts. It also provides insights into how data transfers to third (non-EU) countries will change according to the Standard Contractual Clauses (SCCs), which will take effect on December 27, 2022.

**Keywords:** personal data, privacy protection, legal regulation, GDPR (General Data Protection Regulation), SCCs (Standard Contractual Clauses).

**JEL Classification:** K20, K40.

## Introduction

A world where business is increasingly digital is based on data, knowledge and networks. In it, the sale of goods and services is not possible without intensive and accurate data transmission. The term "digital economy" adequately describes this change. Data, information and knowledge are key elements of production – in a figurative sense, they are the "new petroleum" of today's world (Possler et al., 2019). In some areas, data, information, and knowledge are at the heart of business: this concerns not only social networks, but also payment services, the information technology industry, and other areas. In today's world, the importance of data and information-based businesses to the economy and society is illustrated by the fact that out of the ten world's wealthiest people, there are as many as six information system-driven business owners, and without international data transfer there would not be an opportunity to use many over-the-top media services which availability is essential such as *Messenger, Instagram, Gmail, WhatsApp*, etc.

Letters from companies that flooded many people's emails after the entry into force of the GDPR in the EU asking for permission to continue using your data are just one of the signs that we often didn't even know who kept our data and for how long.

Despite the importance of data transfer between different legal systems (for example, the European Union and the USA), the legal regulation of data transfer is not straightforward. This area of data transfer is governed by the principles of international law, human rights, and state sovereignty, the regulatory objectives of which are often very different: protection of private data and privacy, protection of trade secrets, intellectual property, national security, freedom of expression, etc. Although transatlantic data transfer has been widely written about and debated by both EU and USA researchers (Boehm, 2013; Arenas et al., 2014) practice shows that finding a

* Corresponding author. E-mail: *darijus.beinoravicius@vilniustech.lt*

compromise for powerful economies such as the European Union and the USA is not easy on any issue, let alone a public and national significant issue such as the rights to protection of privacy.

Achieving a successful agreement is complicated not only by the difficult balance of economic interests of the contracting parties, but also by the different principles of legal regulation of data in the European Union and the third countries. For example, USA law is characterized by territorial privacy and specific rules for specific types of data (European Commission, 1999). This means that different legal regimes apply to different types of data and their holders (for example, information on a person's expenses may be considered confidential when it is collected by the person himself, but the same information when it is kept by a bank is no longer protected). The European Union regime, meanwhile, is based on one common category of personal data (which is understood very broadly) and their use is authorized according to different purposes for which the data are used, e.g. performance of the contract with the consent of the data subject, etc. (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016).

## 1. Differences in the regulation of personal data protection in the EU and in third countries

For the understanding of the regulation of personal data processing, it is important to distinguish the different categories of personal data processing: for law enforcement purposes (currently regulated by Directive 2016/680), national security purposes (not covered by European Union law), and processing of personal data for other purposes (e.g. electronic communications services, roaming services in the performance of commercial contracts – currently governed by the General Data Protection Regulation of the European Union, hereinafter – GDPR).

For the purpose of disclosing the subject of this study, the legal framework for the transfer of personal data from the European Union to the third countries, specifically regulated by the GDPR, is relevant, as it is not only the most factually and commercially sensitive area, but, as the current case law practices of the European Court of Justice show, particularly problematic in legal terms (transatlantic data flows between the European Union and the United States are the fastest and largest in the world, accounting for more than half of European data transfers and about half of all US data transfers; the US and the European Union are the main commercial partners for digital services).

It is for this reason that the authors analyze in this work the problems of data transfer to the USA as typical for data transfer to other third countries with the help of document analysis and comparative methodology.

In general, the right of a person to privacy is a popular topic among legal scientists. The legal doctrine states that researchers' interest in the protection of personal data in the field of intelligence and law enforcement is influenced by information leaked to the public about the extent of personal data collection and its (un)lawful use. Such an assumption must be accepted in light of the change in legal regulation and legal doctrine in the field of personal data protection since Edward Snowden's 2013 leaked information about US surveillance programs.

One of the popular areas of research on the right to privacy was the relationship of the individual with the state regarding the protection of personal data. The researchers focused on the information revealed by Edward Snowden about state surveillance measures and their relationship to the right to privacy (Bauman et al., 2014).

Another popular area of research has emerged since the ruling of the Court of Justice of the European Union in the *Schrems* case [7a], which annulled the *Safe Harbor* Agreement. The topic of the protection of the right to privacy in the interaction of different legal systems then gained wider interest. Then, the work of scientists on the possibilities and legitimacy of data transfer from the European Union to the USA appeared (Lam, 2017).

Research in this area includes significant books on the systematic analysis of legal issues in the transfer of personal data between the European Union and the United States (Gray & Henderson, 2017; Mcleod & Shah, 2014) analyzes the nature and essence of the tension between national security and civil liberties. Svantesson and Kloza's (2017) analyzes the cross-border data flow regime, which is based on European Union regulatory instruments such as GDPR, *Safe Harbor* and affects the day-to-day processing of data across the Atlantic and how they limit the scope of data transactions. This book has helped to understand the different approaches of European and US legal scientists to the legal regulation of the transfer of personal data under the *Safe Harbor* Agreement, which expired in 2015. Also noteworthy are Macnish (2016), Halbert and Larsson (2015), Preibusch (2015), Lyon (2014), Loideain (2015), Murphy (2014) those dealt with aspects of data transmission after the Snowden case. Hare (2016) and Frasher (2013) analyzed the balance between data transfer and security, the differences in data transfer policy and culture between the EU and the USA.

Birkinshaw's (2010) book *Freedom of Information: The Law, Practice, and the Ideal* provided a broader understanding of the historical relationship of governments to data protection and their inherent interest in accessing personal data as a necessary requirement for public security. Carr and Bellia's (2017) book *The Law of Electronic Surveillance* reviews the legal nature of USA federal-level personal data collection. This book has helped to understand how the surveillance mechanism works in the US legal system.

It is worth mentioning Santanen (2019), who has analyzed privacy issues in the context of technology deployment and development, while Draper and Raymond (2020) proposed a Draper's Catastrophe Value Curve to

ensure the security of corporate data as a tool to achieve this goal.

The topic of data transfer is also popular among Lithuanian legal scholars. Among the dissertation relevant works, the defended by Stankevičiūtė on the topic "Regulation of personal data collection in electronic space for law enforcement and intelligence purposes" should be mentioned (Stankevičiūtė, 2020). In it, the researcher analyzes the general and continental legal traditions of countries and the supranational level of personal data collection in the electronic space with the peculiarities of the legal framework related to ensuring the right to personal protection for law enforcement and intelligence purposes. This paper, as well as a review of privacy in the United States (Bignami, 2015) and the above-mentioned books, provide a detailed analysis of USA law on the collection of personal data for law enforcement and intelligence purposes. However, given the subject matter of this study, it does not contain any analysis addressing the issues of interoperability between these different legal systems in the context of privacy protection and possible solutions.

With regard to the legal regulation of data transfers to other countries, it should be noted that EU data transfers are governed by the GDPR, which is a directly applicable law in EU Member States.

But there is no one legal framework for the protection of personal data in non-EU countries. In addition, regulation is a dynamic process. A distinction must therefore be made between safe and unsafe third countries. Secure third countries are those for which the European Commission has adopted an appropriate level of data protection based on an adequacy decision. In these countries, national laws ensure a level of protection of personal data that is similar to EU law. Third countries providing an adequate level of protection: Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom, and South Korea. The transfer of data to these countries is expressly permitted.

Thus, BDAR divides the world into two groups:

- the European Economic Area (EEA) – there are no particular obstacles to the processing of personal data in these countries;
- non-EEA countries, data flows outside the EEA (including cloud services, shared access to databases, etc.) are strictly regulated and subject to special protection mechanisms.

## 2. Data transfer to third parties: data protection versus business interests

In view of international trade and cooperation, it is essential these days to be able to also transmit data to third countries.

The GDPR stipulates that personal data which are processed or are intended to be processed following a transfer to a third party or an international organization may be transferred only if the controller and the processor comply with the conditions set out in Chapter V in accordance with other provisions of the GDPR, without inter alia, in relation to the onward transfer of personal data from that third state or international organization to another third party or to another international organization.

There is a separate Chapter V of the GDPR for regulating the transfer of personal data to third parties or international organizations. This section of the GDPR sets out a number of autonomous means of validating the transfer of personal data: transfer on the basis of an adequacy decision, transfer of data with appropriate safeguards, other conditions for the transfer of personal data to a third party or to an international organization. It should be noted that these grounds for the transfer of personal data have a hierarchy (the highest – the European Commission's decision on adequacy enshrined in Article 45) and the subsequent legal basis for the transfer of personal data can be applied only if a higher legal basis does not exist.

Attention is drawn to the general principle that the provisions of Chapter V of the GDPR apply in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined. The Court of Justice of the European Union has stated that the purpose of this provision is to ensure the continuity of this high level of protection of personal data when personal data are transferred to a third party, regardless of the legal basis set out in Chapter V of the GDPR.

The concept of personal data in the electronic space well before the entry into force of the GDPR was examined by Civilka and Šlapimaitė (2015); Frasher (2013).

Zaleskis (2019) analyses the legal regulation of the GDPR as legal rules to protect individuals from the risks posed by data processing. Zaleski's monograph explains the regulation of the GDPR, but does not analyse the problems of the interaction of the GDPR with the legal systems of third countries. Pakutinskas (2009) examined the models of legal regulation of electronic communications, but this is not directly relevant to this study, as it does not reveal the problems of interaction of different legal relations.

In the presence of such legal regulation we cannot disagree with the view that the EU must recognize that data protection standards vary with cultural norms and will likely have no choice but to ignore breaches of Privacy Shield for the sake of economic stability (Lam, 2017).

The *Schrems* case was very significant in terms of the transfer of personal data to other countries. 2020 July 16 The Court of Justice of the European Union (ECJ) in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (known as the "Schrems II case") declared the EU-US privacy shield (agreement on the transfer of personal data to the United States) invalid. The court questioned the extent to which the transfer of data could be legalized under the

European Commission's Standard Contract Terms (SCC) for the transfer of personal data to the United States and worldwide. Following this court decision, data transmissions to the USA cannot therefore be based on the Privacy Shield. Data transfers to the USA require other guarantees to create an appropriate level of data protection.

Following the ruling in the *Schrems* case, the European Data Protection Board issued guidelines on the transfer of personal data, which set out six-step compliance mechanisms for companies transferring data outside the European Economic Area.

To meet current EU data protection standards, companies must meet the following 6 requirements:

- Track transfers of personal data;
- Identify the personal data transmission mechanisms used;
- Assess whether the chosen mechanisms for the transfer of personal data are appropriate in the third country to which the personal data will be transferred;
- Introduce additional measures to ensure the same level of security of personal data as in the European Economic Area;
- Take formal procedural steps to ensure that the additional measures do not violate other formal requirements;
- Carry out monitoring and surveillance.

However, such a system is completely unprofitable for both business and private consumers, as it has placed a very formal burden on businesses, but has in no way increased the protection afforded to data subjects. This means that the current legal framework does not contribute to greater data protection for individual consumers, but only significantly increases the business costs of compliance.

## 3. Problems of privacy protection in business relations due to the interaction of different legal systems: Lithuanian experience

Lithuania is a member of the European Union, therefore the regulation of GDPR is directly applied in it. As analyzed in the previous sections of this study, in the interaction of the European Union and other legal systems, personal data can only be transferred in accordance with certain rules laid down in the GDPR.

Therefore, the same legal issues that are analyzed in the previous sections of this paper are relevant for the protection of privacy in the electronic space in Lithuania due to the interaction of different legal systems.

However, as in each country and legal system, the application of specific rules also raises problems and legal disputes in Lithuania, which, although varying in their importance and significance, can be considered unique. Taking into account the topic of this study, the authors in this section seek to determine whether there have been problems with the protection of privacy in Lithuania due to the interaction of different legal systems.

Prior to the entry into force of the GDPR, in the European Union and Lithuania, the transfer of personal data to third parties and organizations was regulated by Directive 95/46. In Lithuania, it was implemented by the Law on the Legal Protection of Personal Data of the Republic of Lithuania. The provision of personal data to data recipients located in foreign countries was regulated by Article 35 of this Law. Paragraph 5 of this Article established a list of cases when the transfer of personal data to a recipient to a foreign state was allowed, Paragraph 2 provided for the obligation to obtain a permit from the State Data Protection Inspectorate for the transfer of personal data in other cases.

Due to the legal mechanism of such transfer of personal data to third parties, during the research, the authors could not find any Lithuanian court practice that could indicate the problems of privacy protection in the interaction of different systems. From May 2018 the regulation of Directive 95/46 has been replaced by the GDPR. Given that this is a directly applicable legal act throughout the European Union, it has also entered into force in Lithuania. Consequently, the Law on the Legal Protection of Personal Data of the Republic of Lithuania was clarified, coordinating it with the regulation of GDPR.

Since the entry into force of the GDPR, a number of legal disputes have already arisen in Lithuania regarding the application of the GDPR regulation, but only one problematic case can be considered relevant for the disclosure of the topic of this study. The Supreme Administrative Court of Lithuania in May 2020, examined a dispute based on a complaint of a natural person regarding improper processing of his personal data. The applicant alleged that his personal data (information on maternity and paternity benefits for his family) had been unreasonably transferred to public institutions of the Republic of Belarus by the Vilnius City Municipality Administration and the State Social Insurance Fund Board under the Ministry of Social Security and Labor (SODRA). Thus, in the case law of Lithuanian courts, a dispute arose regarding the protection of privacy in the interaction of the Lithuanian and third country – Belarusian legal systems.

It should be noted that the transfer of personal data in this case took place in 2017. Therefore, the case analyzed the legal regulation relevant for that period – the Law on the Legal Protection of Personal Data of the Republic of Lithuania and Directive 95/46, which is implemented by thesaid law. The defendants in this case took the position that personal data could be transferred under bilateral agreements between the Republic of Lithuania and the Republic of Belarus: (I) under the Social Security Agreement between the Republic of Lithuania and the Republic of Belarus and (II) the Ministry of Social Security and Labor the Agreement on the Grant of Pensions and Benefits and the Procedures for the Granting, Transfer and Payment of Benefits, also concluded in accordance with 4$^{th}$ February, 1999 Agreement between the Republic of Lithuania and the Republic of Belarus on Social Security.

In this case, the Supreme Administrative Court of Lithuania considered that the act of transferring personal data to the Republic of Belarus should be considered as processing of personal data as understood under the Law on Legal Protection of Personal Data of the Republic of Lithuania. The court then tried to resolve the issue of the lawfulness of personal data transfer by applying Article 6 of the Law on Legal Protection of Personal Data of the Republic of Lithuania, which states that "Personal data shall be provided in the cases established by this Law in accordance with the personal data provision agreement concluded between the data controller and the data recipient (in case of multiple supply) or at the request of the data recipient (in case of single supply). The contract must specify the purpose of the use of personal data, the legal basis for the provision and receipt, the conditions, the procedure, and the scope of the personal data to be provided. The request shall specify the purpose for which the personal data will be used, the legal basis for their provision and receipt, and the scope of the personal data requested."

Taking into account this legal regulation, it must be held that the Supreme Administrative Court of Lithuania considered that the provision of personal data according to these requests should be considered as one-time submission requests according to the data recipient's requests under Article 6 of the Law on Legal Protection of Personal Data. The court then agreed with the trial court's assessment that the recipient's request for personal data must specify the details for whom the received personal data will be used and provide a legal basis for obtaining and processing personal data, but the requests of the Belarusian authorities did not contain such data (Supreme Administrative Court of Lithuania, 2020).

Thus, taking into account that (I) the agreements concluded between the Republic of Lithuania and the Republic of Belarus do not regulate in detail the conditions and procedures for personal data transfer, such agreements cannot be considered long-term personal data supply agreements under Article 6 of the Law on Legal Protection of Personal Data, and (II) the requests received from the Belarusian authorities do not provide a basis for obtaining and processing personal data, the court concluded that such processing of the applicant's personal data (i.e. transfer to the authorities of the Republic of Belarus) could not be considered lawful.

First of all, the question arises regarding the qualification of the legal basis for the transfer of personal data chosen by the Supreme Administrative Court of Lithuania. As indicated above, the transfer of personal data to foreign countries during the performance of the dispute actions was regulated by Article 35 of the Law on the Legal Protection of Personal Data of the Republic of Lithuania provisions. Article 6 of the Law on Legal Protection of Personal Data of the Republic of Lithuania lays down general rules on the legal basis for the provision of personal data, while Article 35 established rules applicable to the transfer of personal data when the recipient is in a foreign country. Thus, Article 35 of the Law on the Legal Protection of Personal Data of the Republic of Lithuania provisions must be considered *lex specialis* to the general rules on the provision of personal data to recipients requesting them. As mentioned above, according to Article 35 of the Law on Legal Protection of Personal Data of the Republic of Lithuania personal data may be transferred to a third party (I) with the permission of the State Data Inspectorate (Article 35 (2)), or (II) in the presence of one of Article 35 of the said Law part 5 conditions.

Between Article 35 of the Law on the Legal Protection of Personal Data of the Republic of Lithuania, part 5 establishes possible legal bases for the transfer of personal data to a third party that are relevant and relevant to the dispute, such as "the provision of personal data is necessary (or required by law) in the overriding public interest" or "necessary to prevent or investigate criminal offenses".

In the course of the proceedings, the defendants learned, upon request from the Belarusian authorities, that the applicant had sought to obtain benefits related to the birth of a child fraudulently (by concealing information about benefits received in Lithuania), including in Belarus. Therefore, the defendants considered their decision to provide information about the applicant to the Belarusian authorities to be a legitimate act in the public interest.

Lithuanian and Belarusian institutions, acting in accordance with the requirements of legal acts, administer social benefits to satisfy important public interests. In order to be able to perform these functions in accordance with legal requirements (*inter alia* without paying state benefits to those who are not entitled to them), it may be objectively necessary for them to exchange personal data in certain cases. Moreover, acts by applicants seeking to obtain benefits paid by the states on the same basis may even be considered a criminal offense or a misdemeanor (such as fraud). Therefore, taking into account the circumstances established during the proceedings, the transfer of the applicant's personal data had to be considered lawful in accordance with Article 35 of the Law on the Legal Protection of Personal Data of the Republic of Lithuania part 5 page 4 and/or page 6 (in the event that the claimant's wish to receive benefits from two states is proven). In Lithuania, there was a dispute over the protection of privacy, with the interaction of the Lithuanian and foreign legal systems, which was resolved by Lithuanian courts, even without applying the legal basis for the transfer of personal data to a third party and unreasonably qualifying the transfer of personal data.

This case illustrates that similar problems in the transmission of data to third parties inevitably have to be addressed by businesses. Experience has shown that the main issues of uncertainty for businesses are the scope and format of the information provided to data subjects, the control of third parties (for example, the lack of data processing contracts in companies and the difficulty of

finding a mutually satisfactory solution) and the challenges caused the inventory of personal data in companies' IT systems, the setting of data retention deadlines, and the enforcement of these deadlines.

## 4. Will Standard Contractual Clauses facilitate the transfer of data to third parties?

It should be noted that the GDPR prohibits the transfer of European personal data outside the European Union unless adequate protection is provided for personal data in a third country. To this end, the European Commission has adopted Standard Contractual Clauses (SCCs) which replaced the old SCCs, approved in 2001.

The Court of Justice of the European Union (CJEU) has annulled an agreement on the transfer of personal data to the US, and the European Commission has adopted new Standard Contractual Clauses (SCCs), which will take effect on December 27, 2022. Individuals who transfer personal data in the course of their activities to third countries outside the EU on the basis of SCCs may find it easier to relax and start preparing for the signing of new SCCs.

The SCCs must have mechanisms in place to ensure that:

- Third-country authorities will not have unjustified access to European personal data;
- Data subjects will be able to claim redress for violated rights if a third party authority unreasonably accesses personal data.

These additional requirements should help to avoid situations where the European controller or processor, such as e-mail archive, shall transmit all or part of the information in the archive to a company located in China or Belarus, which shall provide access to the location of such data in accordance with national law. To prevent such or similar situations, several safeguards are in place in the SCCs. For example, a data importer (recipient) established in a third country must agree that the personal data supervisory authorities of the European Union will have jurisdiction over his or her activities and will be required to cooperate. In addition, the data importer (recipient) and exporter (EU-based controller or processor) will have to assess whether the third country legislation allows compliance with the SCC conditions according to the duration of the contract, the nature of the data transferred, the type of recipient, and the purpose of the processing.

Although the SCC provides more clarity on what is specifically taken into account when selecting a data exporter's partner from a third country, this does not preclude BDAR's individual risk assessment when the controller has to assess the sensitivity of the personal data processed.

Such uncertainty could jeopardize the rights and freedoms of data subjects and would oblige the controller to take the most appropriate organizational and technical measures to avoid that risk.

It can therefore be concluded that although the procedures for transferring data to third countries are becoming clearer, businesses cannot fully breathe a sigh of relief because it is not yet clear how deep and comprehensive they will need to assess the third countries legal framework.

## Conclusions

The provisions of Chapter V of the GDPR, which apply to all legal bases for the transfer of personal data to third parties, shall have the common objective of ensuring that the level of protection of natural persons guaranteed by this Regulation is not undermined. The purpose of this provision is to ensure the continuity of this high level of protection of personal data when personal data is transferred to a third party, regardless of the legal basis set out in Chapter V of the GDPR.

Data controllers or processors who wish to a transfer data to third party once the Privacy Shield Agreement has been annulled by the Court of Justice of the European Union cannot themselves provide data subjects with a substantially equivalent level of protection that the European Union guarantees for data subjects, which could improve the position of data subjects in relation to unrestricted access by the authorities of the third country to their personal data and the mass collection of personal data. This is confirmed by Lithuanian case law, which shows that the main issues of business uncertainty are the scope and format of information provided to data subjects and the control of third parties.

An analysis of the case law of the Court of Justice of the European Union leads to the conclusion that the obligation of electronic communications entities to retain available traffic and location data for a specified period is disproportionate and illegal for the prevention, detection, investigation or prosecution of criminal offenses. This position of the court suggests that the mass and unrestricted collection of data (even metadata and not the content of the communication itself) and access to it by law enforcement or intelligence authorities cannot be considered lawful.

The GDPR shall apply to the transfer of personal data by an economic operator established in a Member State to another economic operator established in a third party, provided that the authorities of that third party are able to process such data for public security, defence, and national security purposes. Therefore, the main challenge for possible data transfer agreements between the European Union and third countries is to assess the compliance of the third countries national security measures with the GDPR.

SCCs, which will enter into force in 2022 December 27 will avoid situations where a controller or processor operating in Europe will have to transfer information to a company located in a third country, which will have to grant access to such data to local authorities in accordance with national law.

## References


Arenas, M., Barcelo, P., Libkin, L., & Murlak, F. (2014). *Foundations of data exchange.* Cambridge University Press.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology, 8*(2), 121–144. https://doi.org/10.1111/ips.12048

Bignami, F. (2015). *The US legal system on data protection in the field of law enforcement. Safeguards, Rights and Remedies for EU Citizens. Study for the LIBE Committee, 2015* (GWU Law School Public Law Research Paper No. 2015-54, GWU Legal Studies Research Paper No. 2015-54). https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215

Birkinshaw, P. (2010). *Freedom of information: The Law, the practice, and the ideal* (4th ed.). Cambridge University Press. https://doi.org/10.1017/CBO9780511844904

Boehm, F. (2013). *Information sharing and data protection in the area of freedom, security and justice: Towards harmonised data protection principles for information exchange at EU-level*. Springer. https://doi.org/10.1007/978-94-007-2903-2_8

Carr, J., & Bellia, P. (2017). *The law of electronic surveillance* (2 ed., Part 1). Clark Boardman Callaghan.

Civilka, M., & Šlapimaitė, L. (2015). The concept of personal data in cyberspace. *Teisė*, *96*(2015), 126–148. https://doi.org/10.15388/Teise.2015.96.8761

Draper, C., & Raymond, A. H. (2020). Building a risk model for data incidents: A guide to assist businesses in making athical data decisions. *Business Horizons*, *63*, 9–16. https://doi.org/10.1016/j.bushor.2019.04.005

European Commission. (1999). *Article 29 Working group opinion of January 26, 1999 Nr. 5092/98/EN/final*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf

Eur-Lex. (2016a). *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)*. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679

Eur-Lex. (2016b). *Regulation (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

e-tar. (1996). *Law on the Legal Protection of Personal Data of the Republic of Lithuania*. https://www.e-tar.lt/portal/en/legalAct/TAR.5368B592234C/asr (in Lithuanian).

Frasher, M. (2013). Adequacy versus equivalency: Financial data protection and the U.S. – EU divide. *Business Horizons, 56*, 787–795. https://doi.org/10.1016/j.bushor.2013.08.004

Gray, D., & Henderson, S. E. (2017). *The Cambridge handbook of surveillance law*. Cambridge University Press. https://doi.org/10.1017/9781316481127

Halbert, D., & Larsson, S. (2015). By policy or design? Privacy in the US in a Post-Snowden World. *Journal of Law, Technology and Public Policy, 1*(2), 1–17.

Hare, S. (2016). For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection. *Business Horizons, 59*, 549–561. https://doi.org/10.1016/j.bushor.2016.04.002

InfoCuria. (2020). *Judgment of the Court (Grand Chamber) of 16 July 2020 (request for a preliminary ruling from the High Court (Ireland) – Ireland) – Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (C-311/18)*. https://curia.europa.eu/juris/document/document.jsf?text=&docid=230683&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=299692

Lam, C. (2017). Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner. *Boston College International and Comparative Law Review, 40*(3), 1.

Loideain, N. L. (2015). EU law and mass internet metadata surveillance in the Post-Snowden era. *Media and Communication (Lisboa), 3*(2), 53–62. https://doi.org/10.17645/mac.v3i2.297

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society, 1*(2). https://doi.org/10.1177/2053951714541861

Macnish, K. (2016). Government surveillance and why defining privacy matters in a Post-Snowden world. *Journal of Applied Philosophy, 35*(2), 417–32. https://doi.org/10.1111/japp.12219

McLeod, D. M., & Shah, D. V. (2014). *News frames and national security. Communication, society and politics*. Cambridge University Press.

Murphy, M. H. (2014). The Pendulum effect: Comparisons between the Snowden Revelations and the Church Committee. What Are the Potential Implications for Europe? *Information & Communications Technology Law, 23*(3), 192–219. https://doi.org/10.1080/13600834.2014.970375

Pakutinskas, P. (2009). *Models of Legal Regulation of electronic communications*. Mykolas Romeris University.

Possler, D., Bruns, S., & Niemann-Lenz, J. (2019). Data is the new oil – but how do we drill it? Pathways to access and acquire large data sets in communication science. *International Journal of Communication*, *13*(2019), 3894–3911. https://ijoc.org/index.php/ijoc/article/download/10737/2763

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM,* 58(5), 48–55. https://doi.org/10.1145/2663341

Santanen, E. (2019). The value of protecting privacy. *Business Horizons*, *62*, 5–14. https://doi.org/10.1016/j.bushor.2018.04.004

Stankevičiūtė, S. (2020). *Regulation of the collection of personal data in cyberspace for law enforcement and intelligence purposes* [Doctoral dissertation, Mykolas Romeris University]. ELABa.

Supreme Administrative Court of Lithuania. (2020). *2020 May 14 order in administrative (case Nr. eA-531-822/2020)*. Liteko. http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9562e239-012c-49d8-9adc-91dfa77ebd46

Svantesson, D. J. B., & Kloza, D. (2017). *Trans-Atlantic data privacy relations as a challenge for democracy*. Intersentia. https://doi.org/10.1017/9781780685786

Zaleskis, J. (2019). *The general data protection regulation of the European Union and the Law on the protection of personal data: Monograph*. Registrų Centras. ELABa.