Nino Tsagareishvili*

Legal Regulation of International Transfer of Personal Data (International and National Standards)

The cross-border transfer of personal data presents a complex challenge in both Georgian and international contexts. Notably, within the framework of international cooperation, substantial amounts of personal data are exchanged across various sectors. This reality necessitates effective regulation to ensure the protection of data subjects' rights. The article aims to explore the legal frameworks governing these transfers, focusing on both international standards and Georgia's national regulations.

Keywords: *International/Cross-Border Transfer of Personal Data, Personal Data Protection Service, Adequacy Decision, Appropriate Data Protection safeguards, Data Subject Rights.*

1. Introduction

In today's world, the transfer of personal data across borders is becoming increasingly significant. Continuous data exchanges between states and international organizations are essential for fostering cooperation across various sectors. While such transfers are beneficial for enhancing collaboration, they also introduce specific risks related to the protection of personal data. Balancing the benefits with the need for effective safeguards remains a critical challenge at both international and national levels.

First and foremost, an analysis of the compatibility between national personal data protection legislations is essential. Divergent approaches to key issues can lead to violations of data subjects' rights and undermine personal data protection standards. Consequently, several critical questions emerge: What national and international legal mechanisms govern the international transfer of personal data? If personal data is inadequately protected in a specific country, how is the transfer of such data restricted? In the absence of comprehensive legal regulation, what measures can be taken to ensure the protection of personal data? Additionally, what authority does the Personal Data Protection Authority wield in regulating cross-border data transfers?

This article will evaluate the legal aspects of the international transfer of personal data, with a focus on the requirements outlined in Chapter V[1] of the Law of Georgia "On Personal Data Protection." The discussion will analyze how these provisions regulate cross-border data

* Master of International Law at Ivane Javakhishvili Tbilisi State University, Faculty of Law; Researcher-Analyst in the International Relations, Analytics, and Strategic Development Department of the Personal Data Protection Service of Georgia.

[1] Law of Georgia "On Personal Data Protection", 14/06/2023.

transfers and ensure compliance with international standards. The international legal framework and standards, including recommendation documents developed by the European Commission[2] and the European Data Protection Board (EDPB)[3], as well as the practices of foreign data protection supervisory authorities, will be presented in this article. Through the analysis of these sources, answers to the posed questions will be provided.

2. National Regulation of International Data Transfer

On March 1, 2024, the Law of Georgia "On Personal Data Protection" (the Law) [4] came into force, with the primary objective of ensuring robust standards and guarantees for the protection of personal data. This new law addresses key issues in the field of data protection, including the regulation of international data transfers, to align Georgia with evolving global data protection norms. The transfer of personal data to another state or international organization is regulated by Article 37 of the Law of Georgia "On Personal Data Protection." According to this provision, such transfers are permitted only if the requirements for data processing, as outlined in the Law, are met, and the recipient state or international organization ensures adequate data protection standards. Furthermore, appropriate safeguards must be in place to protect the rights of the data subject.[5]

In addition to the above, according to paragraph 2 of Article 37, the transfer of data to another state or international organization is allowed if:

- The international agreements and treaties of Georgia provide for the transfer of personal data;
- The data controller provides appropriate guarantees for the protection of personal data;
- The data transfer is carried out in accordance with the legislation outlined in subsection "C," including the Criminal Procedure Code; the Law of Georgia "On the Legal Status of Aliens and Stateless Persons"; the Law of Georgia "On International Cooperation in the Field of Criminal Law"; the Law of Georgia "On International Cooperation in the Field of Law Enforcement"; and the Organic Law of Georgia "On the Prevention of Money Laundering and Terrorism Financing," adopted based on the Law of Georgia.
- After receiving information about the lack of adequate data protection guarantees and potential threats in the relevant state, the data subject requests written consent.
- The data transfer is necessary to protect the vital interests of the data subject, and the data subject is physically or legally unable to provide consent for data processing.
- There is a significant public interest in accordance with the law—such as crime prevention, investigation, detection, prosecution, execution of sentences, and the

[2] European Commission, the Executive Body of the European Union, <https://commission.europa.eu/about-european-commission_en> [03.08.2024].
[3] The European Data Protection Board, <https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en> [03.08.2024].
[4] Law of Georgia "On Personal Data Protection", 14/06/2023.
[5] Ibid. the first paragraph of Article 37.

implementation of operational-search measures—and the data transfer is deemed a necessary and proportionate measure in a democratic society.[6]

It should be noted that if the data controller provides appropriate guarantees[7] in accordance with the contract, data can be transferred only after obtaining permission from the Personal Data Protection Service, the procedure for which is established by a normative act issued by the head of the Personal Data Protection Service.[8] In this case, the data transfer agreement should include enforceable conditions with legally binding force.[9] In addition, when transferring data on the listed grounds, the controller/processor is obliged to implement the necessary organizational and technical measures to ensure the safe transfer of data.[10] According to paragraph 6 of the same article, further transfer of data to another state or international organization by a third party is permitted only if it aligns with the original purposes, complies with the grounds for data transfer outlined in this article, and ensures appropriate data protection guarantees.

3. Supervisory Mechanisms of the Personal Data Protection Service regarding Cross-Border Data Transfers

One of the main functions of the Personal Data Protection Service (hereinafter referred to as 'the Service') is to supervise the lawfulness of cross-border transfers of personal data. Specifically, when international agreements or agreements to be concluded on behalf of Georgia provide for the possibility of cross-border personal data transfers, the Service conducts a legal examination of these documents upon the request of the relevant agency.

During the examination of a contract, the Service considers whether appropriate data protection guarantees exist in the relevant state or international organization. In this process, the Service reviews the drafts of the submitted agreements, as well as the legislative and institutional mechanisms related to personal data protection in the party state. Based on this review, if necessary, the Service will issue recommendations for amendments to the draft agreement.

The Personal Data Protection Service of Georgia assesses the existence of appropriate data protection guarantees in another state and/or international organization based on their international obligations and data protection laws, the guarantees for the rights and freedoms of data subjects (including effective legal protection mechanisms), the rules for further international data transfers, and an analysis of the existence, powers, and activities of the independent data protection supervisory authority.[11]

According to Order No. 23 of February 29, 2024, issued by the President of the Personal Data Protection Service, a list[12] of countries with appropriate guarantees for personal data protection has been approved. In these countries, data transfers are considered safe if proper

[6] Ibid. paragraph 2 of Article 37.
[7] Ibid. Article 37, Paragraph 2, Sub-paragraph “b”.
[8] Ibid. paragraph 3 of Article 37.
[9] Ibid. paragraph 5 of Article 37.
[10] Ibid. paragraph 4 of Article 37.
[11] Ibid. the first paragraph of Article 38.
[12] Order No. 23 of February 29, 2024 of the President of the Personal Data Protection Service “On approval of the list of countries with appropriate guarantees of personal data protection”.

grounds exist. The list includes both EU member states and countries for which the European Commission has adopted an adequacy decision. [13]

In accordance with Article 38, Paragraph 3 of the Law of Georgia "On Personal Data Protection", the specified list must be reviewed at least once every three years. If a state and/or international organization no longer meets the legal requirements, appropriate changes must be made to the list as determined by the normative act, which will not have retroactive effect.

In addition, based on Order No. 33 of March 1, 2024, issued by the President of the Personal Data Protection Service, the procedure for issuing permission for the transfer of personal data to another state or international organization has been developed, and the application form has been approved. This procedure outlines the process for submitting the application and relevant documentation, reviewing them, making a decision, and issuing permissions, along with their terms and conditions.[14]

4. International Standards for Cross-Border Transfer of Personal Data

4.1. General Overview of the International Legal Framework

Article 12 of the Council of Europe Convention 108, "On the Protection of Individuals with regard to Automatic Processing of Personal Data"[15] (hereinafter "Convention 108"), addresses the cross-border transfer of personal data. It establishes conditions for transferring personal data across borders by any means. According to paragraph 3, parties generally may not obstruct the transfer of personal data to the territory of another party or require specific authorization for such transfers solely for data protection reasons. However, paragraph 3 also specifies certain exceptions in which a party may deviate from the principles set out in paragraph 2:

- The legislation of a party contains specific provisions for certain categories of automated personal data files, provided that equivalent protection is not already ensured under the legislation of the receiving party.
- The data transfer is routed through an intermediary in another country, ultimately reaching a state that is not a party to the Convention.

The Additional Protocol to Convention 108 of the Council of Europe[16] addresses issues related to supervisory authorities and the cross-border exchange of personal data. The preamble emphasizes the importance of safeguarding human rights and fundamental freedoms, particularly the right to privacy, amid the increasing flow of personal data between

[13] See 3.2. Chapter: "Transfer of personal data to a non-EU country based on a adequacy decision taken by the European Commission".

[14] Order No. 33 of the President of the Personal Data Protection Service dated March 1, 2024 "On the procedure for issuing permission for the transfer of personal data to another state and international organization and the approval of the application form for the transfer of personal data to another state and/or international organization".

[15] CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981.

[16] CoE, Additional Protocol to the Convention for The Protection Of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Crossborder Data Flows, European Treaty Series - No. 181, 2001, <https://rm.coe.int/1680080626> [03.08.2024].

states. Article 2 of this Protocol governs the transfer of personal data to recipients outside the jurisdiction of a Convention party. According to the first point, the recipient state or organization must ensure an adequate level of data protection during such transfers. Pursuant to paragraph 2, each party may transfer personal data if:

- The transfer is based on domestic legislation, particularly where specific interests are tied to the content of the data or involve overriding legitimate interests.
- The data controller, in line with contractual provisions, implements security measures that align with the domestic legal requirements set by the relevant authorities.

Article 14 of the modernized Council of Europe Convention 108[17] includes provisions governing the cross-border transfer of personal data, aiming to facilitate the free flow of information. This article defines international data transfer as the sharing of personal data with recipients in other jurisdictions. Such transfers to recipients outside the jurisdiction of a Contracting State are permitted only when an adequate level of data protection is ensured.[18]

Chapter 5 of the EU General Data Protection Regulation[19] (GDPR) sets out rules for transferring personal data to third countries[20] or international organizations. When making such transfers, data protection standards must be upheld.[21] This process follows a "two-step approach":[22] first, the transfer must comply with EU data protection laws and be based on the data subject's consent or another lawful authorization. Second, the transfer must meet the specific conditions outlined in the regulation. If adequate data protection safeguards are not in place, the transfer of personal data is prohibited.[23]

Under EU law, the exchange of personal data with countries in the European Economic Area (EEA) for purposes such as the prevention, investigation, detection, prosecution, or enforcement of criminal offenses is governed by the Directive on the processing of personal data in the police and criminal justice sectors.[24] The goal is to ensure that the exchange of personal data between authorized bodies within the European Union is not prohibited or restricted due to data protection concerns. [25]

[17] CoE, Convention 108 +, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.

[18] CoE, Council of Europe Treaty Series - No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, §102 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> [03.08.2024].

[19] EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201 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/eli/reg/2016/679/oj> [03.08.2024].

[20] Third countries are non-EU countries.

[21] Ibid. Article 44.

[22] The EU General Data Protection Regulation (GDPR), A Practical Guide, 117.

[23] Ibid.

[24] Directive (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.

[25] Handbook on European data protection law, Luxembourg, 2018, 287.

4.2. Transfer of Personal Data to a Non-EU Country Based on an Adequacy Decision by the European Commission

Under Article 45 of the EU General Data Protection Regulation (GDPR), the European Commission is empowered to decide whether a non-EU country, territory, or specified sector ensures an adequate level of data protection. The process of adopting an adequacy decision involves the following steps:

- A proposal by the European Commission;
- An opinion from the European Data Protection Board (EDPB);
- Adoption of adequacy decision by European Commission.

Based on an adequacy decision, personal data can be transferred to third countries without the need for additional safeguards. In this case, the same data protection standards that apply within EU member states will be upheld in the recipient country, ensuring equivalent levels of protection.

The European Commission is required to periodically review adequacy decisions to ensure ongoing compliance, and must report the findings of these reviews to the European Parliament and the Council. If the requirements under the GDPR are violated, the European Parliament or the Council may, at any time, request that the Commission maintain, amend, or revoke the adequacy decision.[26]

4.3. Transfer of Personal Data to Non-EU Countries Based on Appropriate Data Protection Guarantees

In non-EU countries where no adequacy decision has been made, the transfer of personal data is not categorically prohibited. In such cases, the data controller must ensure adequate protection for personal data through alternative measures. Additionally, individuals must still be able to exercise their rights as granted under the GDPR.[27]

Article 46 of the GDPR outlines various mechanisms that private organizations can utilize to ensure appropriate safeguards in the absence of an adequacy decision. Specifically, the following measures should be developed:

- Standard data protection clauses;[28]
- Binding corporate rules;[29]
- Codes of conduct;
- Certification mechanisms;
- Standard contractual clauses for direct data transfers[30].[31]

Additionally, the transfer of personal data to third countries without an adequacy decision may be permitted based on the following grounds: the explicit consent of the data

[26] European Commission, Adequacy decisions, <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> [03.08.2024].
[27] GDPR, Third Countries, <gdpr-info.eu> [03.08.2024].
[28] Standard data protection clauses (SCCs).
[29] Binding corporate rules (BCRs).
[30] Ad hoc contractual clauses.
[31] EDPB, International Data Transfers, <edpb.europa.eu> [03.08.2024].

subject, which must be freely given; the necessity of fulfilling contractual obligations; the protection of vital public interests; or other specified legal bases under the GDPR.[32]

In relation to this issue, it is important to note the decision of the Court of Justice of the European Union (CJEU) in the "Maximillian Schrems" case[33], which emphasized the necessity of implementing additional measures when transferring personal data outside the European Economic Area, alongside the presence of appropriate safeguards. According to the court's assessment, data controllers and processors must evaluate the potential impact of the legislation and practices of the non-EU country on the effectiveness of these safeguards during data transfers.[34]

The European Data Protection Board (EDPB) has developed guidelines for the transfer of personal data between EU member states and organizations, as well as to non-member countries and organizations. The purpose of these guidelines is to regulate international data transfers in the absence of an adequacy decision, while taking into account the requirements established by the GDPR. The parties to the agreement are encouraged to include additional guarantees in their contracts. The document outlines key issues that should be addressed in the agreement, including: terms of the contract, principles of data processing, rights of the data subjects, obligations of the parties, restrictions on data transfers, and more.[35]

The European Commission has issued a document[36] outlining standard contractual clauses for the transfer of personal data to third countries, in line with the requirements of the General Data Protection Regulation (GDPR). It emphasizes that, in the context of modern technologies, the demand for cross-border data transfer is increasing to promote international cooperation and trade. In this process, ensuring the proper protection of personal data is essential.[37]

According to the first paragraph of Article 46 of the General Data Protection Regulation (GDPR), in the absence of an adequacy decision, the transfer of personal data is permissible if appropriate data protection guarantees are in place, including the rights of the data subjects and legal remedies. These guarantees must be aligned with the standard data protection clauses adopted by the European Commission, as outlined in Article 46, paragraph 2, subparagraph (c).[38]

The purpose of the standard data protection clauses developed by the European Commission is to ensure appropriate guarantees during the international transfer of personal data. The parties to the agreement are not restricted from including additional measures to enhance data protection within the contract. The accompanying document includes an appendix that outlines the standard contractual terms related to international data transfers.[39]

Additionally, the European Data Protection Board (EDPB) has produced a document detailing appropriate data protection safeguards for the cooperation between data

[32] Ibid.
[33] CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.
[34] EDPB, International Data Transfers, <edpb.europa.eu> [03.08.2024].
[35] EDPB, Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and non-EEA Public Authorities and Bodies, 15/12/2020, <edpb.europa.eu> [03.08.2024].
[36] European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, <eur-lex.europa.eu> [03.08.2024].
[37] Ibid.
[38] Ibid.
[39] Ibid.

protection supervisory authorities within the European Economic Area (EEA) and third countries. The standards outlined in this guidance are based on Articles 70(1)(u) and 50(a) of the General Data Protection Regulation (GDPR).[40]

4.4. Overview of Practices of Data Protection Supervisory Authorities in Foreign Countries on International Data Transfers

Data protection supervisory authorities in various countries have addressed issues related to the international transfer of personal data in numerous cases. This chapter presents the practices of several countries as illustrative examples, providing a general overview of the existing approaches to international data transfers.

a. Sweden

The Swedish Data Protection Authority (IMY) has examined the legality of personal data processing through Google Analytics by a data controller. In this case, personal data was transferred to the United States via the platform.

The supervisory authority assessed the compatibility of this data transfer with the requirements of Chapter V of the GDPR, specifically Article 44. Drawing from the "Schrems II" case, the authority noted that merely having standard contractual clauses is insufficient for ensuring adequate data protection; a thorough analysis of the national legal framework is also necessary.

Ultimately, the supervisory authority concluded that the data transfer did not comply with the requirements established by Chapter V of the GDPR, as the data controller failed to adequately protect the rights of data subjects, resulting in a violation of Article 44 of the General Data Protection Regulation.[41]

b. Spain

The Spanish Data Protection Authority has investigated the legality of personal data processing by the telecommunications company Vodafone, particularly in the context of international data transfers.

In this case, Vodafone had a contract with a data processor required to process data in Peru, resulting in the transfer of personal data to a third country. However, the agreement did not address the issues related to international data transfers, thereby failing to provide adequate data protection guarantees.

Considering these circumstances, the supervisory authority determined that the data controller violated Article 44 of the GDPR.[42]

[40] EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14/03/2022, <edpb.europa.eu> [03.08.2024].
[41] Decision of the Swedish DPA (IMY), 30/06/2023, <gdprhub.eu> [03.08.2024].
[42] Decision of Spanish DPA, 10/03/2021, <gdprhub.eu> [03.08.2024].

c. Austria

The decision of the Austrian Data Protection Authority pertains to the transfer of personal data to the United States by a company through Facebook, conducted without a relevant legal basis.

The supervisory authority evaluated the legality of the international data transfer and its compliance with the requirements set forth in Chapter V of the GDPR. Similar to other supervisory bodies, reference was made to the CJEU's ruling in the "Schrems II" case[43]. Following this analysis, it was concluded that there was no legal basis for the transfer of personal data. Specifically, the adequacy decision issued by the European Commission regarding data transfers from the European Union to the United States was deemed invalid. Consequently, both the data receiver and transmitter could not rely on Article 45 of the GDPR.

The supervisory authority determined that the data controller violated the requirements of Chapter V of the GDPR due to the unlawful transfer of personal data to the United States.[44]

d. Italy

The Italian Data Protection Authority (Garante) has examined the legality of transferring personal data to the United States by a website operator utilizing Google Analytics.

In its assessment, the supervisory authority noted that there was a low probability of access to personal information by U.S. authorities; however, this was not sufficient to absolve the data controller of responsibility for ensuring adequate safeguards. The authority determined that the encryption of personal data was an inadequate technical security measure.

Consequently, it found violations of Articles 44 and 46 of the GDPR. The supervisory body issued a re to the data controller, instructing them to achieve compliance with Article 46 within 90 days. Failure to do so would result in the cessation of the personal data transfer.[45]

e. Finland

The Finnish Data Protection Authority has also assessed the legality of personal data processing using the Google Analytics platform. In this case, personal data was transferred to the United States by the data controller, the Meteorological Institute. Citing the "Schrems II" decision, the supervisory authority evaluated the legality of the data transfer.

According to its findings, the transfer of personal data by the data controller did not have an appropriate legal basis under Chapter V of the EU General Data Protection Regulation, and adequate data protection guarantees were not provided.

As a result, the data controller unlawfully transferred personal data of the data subjects to the United States using Google Analytics. The supervisory authority determined that Articles 44 and 46 of the GDPR were violated. Consequently, it issued a reprimand to the data controller and ordered the deletion of the personal data transferred to the United States without a legal basis.[46]

[43] CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.
[44] Decision of Austrian DPA, 06/03/2023, <gdprhub.eu> [03.08.2024].
[45] Decision of Italian DPA, 9/06/2022, <gdprhub.eu> [03.08.2024].
[46] Decision of Finnish DPA, 24/03/2023, <gdprhub.eu> [03.08.2024].

5. Conclusion

The intensive exchange of personal data between states and international organizations necessitates effective regulation to adequately protect the rights of data subjects. The issues addressed in this article, including the practices of the Court of Justice of the European Union and foreign data protection supervisory authorities, highlight the significance of international data transfers and the challenges associated with them.

As noted, if no adequacy decision has been made regarding a non-EU country and adequate data protection guarantees are not in place, the transfer of personal data is still possible, provided that the issue can be addressed through an agreement. In this case, it is advisable to include in the contract definitions of key terms, principles of data processing, rights of the data subject, obligations of the parties, and other relevant provisions.

Before transferring personal data, it is crucial to assess the national legislation and data protection standards of the specific country. Additionally, it is important to determine the existence of appropriate safeguards. For this purpose, the international legal framework and standards discussed in this article should be considered, along with the requirements set out in Chapter V of the Law of Georgia "On Personal Data Protection."

Bibliography:

1. Law of Georgia "On Personal Data Protection", 14/06/2023.
2. Order No. 23 of the President of the Personal Data Protection Service "On approval of the List of Countries with Appropriate Guarantees of Personal Data Protection", 29/02/2024.
3. Order No. 33 of the President of the Personal Data Protection Service, "On the Procedure for Issuing Permission for the Transfer of Personal Data to Another State and International Organization, and Approval of the Application Form for the Transfer of Personal Data to Another State and/or International Organization," 01/03/2024.
4. CoE, Additional Protocol to the Convention for The Protection Of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Crossborder Data Flows, European Treaty Series - No. 181, 2001.
5. CoE, Convention 108 +, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.
6. CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981.
7. CoE, Council of Europe Treaty Series - No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018.
8. Directive (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.

9. EDPB, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, 15 December 2020.
10. EDPB, Overview of International Data Transfers.
11. EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14 March 2022.
12. EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201 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).
13. European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
14. European Commission, Information Regarding the Adequacy Decisions.
15. GDPR, Information Regarding the Third Countries.
16. Handbook on European data protection law, Luxembourg, 2018, 287.
17. The EU General Data Protection Regulation (GDPR), a Practical Guide.
18. Case of the Data Protection Authority (Sweden), 30/06/2023.
19. Case of the Data Protection Authority (Spain), 10/03/2021.
20. Case of the Data Protection Authority (Austria), 06/03/2023.
21. Case of the Data Protection Authority (Italy), 09/06/2022.
22. Case of the Data Protection Authority (Finland), 24/03/2023.
23. CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.