Marika Abazadze*

Personal Data Protection in Scientific and Academic Research

With the enactment of the new Law of Georgia on Personal Data Protection, the need to balance a high standard of data security with the legitimate interest in processing data for academic research has become increasingly relevant. This article examines the legal aspects of personal data protection that researchers must consider when conducting scientific and academic studies. It explores key issues that arise in daily research activities and highlights relevant best practices.

Keywords: *Scientific and academic research, secondary data processing, validity of data subject consent, personal data security, data subject rights.*

1. Introduction

Scientific and academic research often involves collecting and storing information in both digital and physical formats. A key challenge in this process is ensuring that the use and sharing of personal data comply with data protection legislation.

The protection of personal data is a fundamental right of the data subject. Therefore, safeguarding personal data should be a priority from the very outset of academic research, including during the planning phase and when defining research objectives.[1] Notably, the concept of "confidentiality" can be

* Master of Law in Data Protection and Privacy - Dublin City University (DCU); Master of International Law - Georgian Institute of Public Affairs (GIPA); Researcher-Analyst in the Department of International Relations, Analytics and Strategic Development of the Personal Data Protection Service.

[1] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 5.

interpreted differently depending on cultural and contextual factors[2], making it essential to tailor data processing approaches to the specific research setting.

The research methodology should also be evaluated from a personal data protection perspective. For instance, in cases involving covert observation of data subjects, it is crucial to assess how the terms "public" and "private" apply within the research context. Such observation is permissible only if the researcher can clearly justify its necessity and demonstrate that achieving the research objectives through alternative methods would be extremely difficult or impossible. Additionally, the researcher must ensure that covert observation does not infringe upon the rights and freedoms of data subjects.

Compliance with personal data protection laws extends beyond defining research objectives and methodologies. It encompasses all stages of research implementation, including data collection, access, respondent communication, and data storage or erasure. Some institutions and organizations outline detailed data protection strategies that govern the entire data processing cycle, ensuring proper storage, accuracy, and security.[3]

Academic research may also involve international data transfers. While the General Data Protection Regulation (GDPR) seeks to standardize data protection rules across Europe, national regulations can introduce variations, particularly in the context of statistical or academic research. EU Member States have discretion in defining and regulating scientific research, leading to potential legal discrepancies that may complicate international data transfers and research collaborations.[4]

In Georgia, the Law on the Protection of Personal Data allows personal data processing for research purposes, provided that appropriate technical and organizational security measures are in place to safeguard the rights of data subjects. Furthermore, data controllers must comply with all relevant legislative requirements.[5]

[2] Law of Georgia "On Personal Data Protection", Article 27 (2).

[3] *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021.

[4] *Ducato R.,* Data Protection, Scientific Research, and the Role of Information, Computer Law & Security Review, Vol. 37, 2020, 14.

[5] Law of Georgia "On Personal Data Protection", Article 4(6).

2. Principles and Activities of Personal Data Processing

According to the Law of Georgia "On Personal Data Protection", any action involving personal data constitutes data processing. In the context of research projects, data processing includes activities such as compiling respondent email lists, creating and managing databases, and sharing data with third parties. The law defines "processing of personal data" as any action or set of actions performed on personal data, regardless of the form or means used. This includes both automated and non-automated processing methods, such as collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, transmission, dissemination, rectification, combination, blocking, erasure, or destruction.[6]

The consent of the data subject introduces different obligations depending on the field of application. In scientific or clinical research, for instance, at the data collection stage, the data controller may not always be able to define a single, specific purpose for data processing.[7] The relevant regulations acknowledge this challenge and allow data subjects to consent to data processing for broader research purposes, considering the scope and context of the processing.[8]

If an international transfer of data is required or a research project involves an international organization, researchers must ensure compliance with relevant data protection regulations. This includes adhering to local and international data protection laws, institutional data protection policies, and other applicable legal frameworks. Researchers should secure the necessary permissions before beginning data processing, notify relevant supervisory authorities or ethics committees, and fulfill any additional legal obligations imposed on them.[9]

A researcher is also responsible for maintaining data accuracy and updating it periodically. Data security measures must be upheld, and the rights of data subjects—such as the right to erasure, also known as the "right to be forgotten"—must be protected. Personal data should be stored in a way that prevents subject identification and should not be retained longer than

[6] Ibid, 3 (f).

[7] *Schaar K.,* Working Paper: What is important for Data Protection in science in the future? General and Specific Changes in Data Protection for Scientific Use Resulting from the EU General Data Protection Regulation RatSWD Working Paper, No. 258, 2016, 6.

[8] *Chassang G.,* The Impact of the EU General Data Protection Regulation on Scientific Research, Ecancer Medical Science, 2017, <https://pubmed.ncbi.nlm.nih.gov/28144283/> [20.02.2025].

[9] Recommendations of the Personal Data Protection Service on the Development of a Privacy Policy Document, 2025, 11.

necessary for the intended research purpose.[10] While access to data may be required for reporting purposes after a study's completion, indefinite data storage is not considered an acceptable practice.[11]

To ensure compliance, it is crucial to establish a clear data retention and deletion plan at the outset of the study. If necessary, an automated data deletion function should be implemented. The retention period of personal data should align with the original purpose of collection or any justified re-processing needs. Once data is no longer necessary for the research, it should be deleted or archived in a depersonalized form.[12]

Internationally, the burden of proving compliance with data protection principles rests with researchers, research project leaders, and institutions. For example, the UK's Information Commissioner's Office (ICO) imposed an administrative fine on the University of Greenwich for a personal data security breach linked to a student-led research project.[13] The breach occurred because the student failed to implement proper security measures for a research-related website, allowing hackers to access the personal data of 20,000 individuals, including special category data subjects. This case underscores the importance of conducting thorough risk assessments, enforcing data security policies, and maintaining strict compliance controls for personal data processing.

The processing of special categories of personal data for academic research purposes is generally based on the explicit consent of the data subject. These special categories include, among others, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and information related to health, sexual orientation, or sexual activity.[14] When processing such sensitive data, researchers must submit a valid legal basis for processing to the relevant ethics committee. It is essential to justify the necessity of data collection within the research framework and assess the proportionality of data processing to ensure compliance with legal and ethical standards. Additionally, personal data collected from different sources may only be combined if explicitly permitted by law.

[10] EDPS, Preliminary Opinion on Data Protection and Scientific Research, 2020, 23.
[11] ICO, Guideline on Principle of Storage Limitation, <https://ico.org.uk/> [20.02.2025].
[12] European University Institute, Guide on Good Data Protection Practice in Research, 2022.
[13] MDPI and ACS Style, *Lallie H. S., Thompson A., Titis E., Stephens P.,* Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector, 2025, 20.
[14] Article 9, 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).

3. Obtaining Informed Consent for Personal Data Processing

For data processing to be lawful, the data subject's consent is generally required. However, processing personal data without consent is permissible in exceptional cases, such as when the processing does not adversely affect the legitimate interests of the individual, the public interest in conducting the research outweighs the data subject's rights, or the research objectives cannot be achieved otherwise or would require disproportionate effort. The lawfulness of processing without consent often depends on balancing the right to confidentiality with the potential benefits of the research.[15] In some situations, under fundamental regulations, processing may be permitted without specifying the exact purpose[16]—such as during a public health emergency—provided that ethical research standards are upheld.[17]

The data subject has the right to withdraw consent at any time without providing a reason. They also have the right to request the erasure or blocking of their processed information.[18] If a researcher fails to obtain valid consent, they may face legal challenges or liability. "Valid" consent must be freely given, without coercion, intimidation, or misleading information. It must be specific, clearly defined in relation to the purpose and scope of data processing. It must also be informed, meaning the data subject must understand what information is being processed and why, and unambiguously, demonstrated through an explicit and affirmative act.[19]

A valid consent process ensures that data subjects have a genuine choice regarding the collection and use of their data. It is not sufficient if consent is influenced by any form of pressure or manipulation[20]. The respondent's consent needs to be specific, clearly identified, accurately respond to, and agree with the purpose and results of the data processing.[21]

[15] *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021, 26.
[16] *Malgieri G.,* Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic, Computer Law & Security Review, 2020, 3.
[17] Recital 33, 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).
[18] Guideline 05/2020 on consent, under Regulation 2016/679, 9.
[19] Recital 32, 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).
[20] EDPS, A Preliminary Opinion on Data Protection and Scientific Research, 2020, 19.
[21] Guideline 05/2020 on consent, under Regulation 2016/679, 21.

In some cases, a single consent may cover multiple processing operations if the data subject, based on the provided information, can reasonably anticipate how their data will be used. Research participants must receive comprehensive and accurate information regarding the purpose of data processing, the categories of data being processed, the duration of data processing and storage, any secondary data processing or transfers, and their rights as data subjects, including the right to object to data processing.[22]

Research participants must receive comprehensive and accurate information regarding the purpose of data processing, the categories of data being processed, the duration of data processing and storage, any secondary data processing or transfers, and their rights as data subjects, including the right to object to data processing.[23]

The data controller bears the responsibility of proving that valid consent has been obtained for a specific research purpose.[24] Several factors should be considered in this regard, including the relationship between the researcher and the data subject, such as whether there is a power imbalance or dependency, any economic or legal influence on the data subject, as well as the vulnerability of the research participant and the potential impact of the research on them or society.

4. "Secondary Processing" of Personal Data

When personal data is processed again for a purpose different from its original intent, it constitutes secondary data processing. Such processing is unlawful if data collected for one research project is used for another without the data subject's knowledge and consent.[25] However, it is lawful if the data subject's initial consent explicitly includes permission for further processing in new research or if researchers obtain fresh consent for the new study.[26]

Researchers are responsible for fully informing data subjects when collecting personal information, emphasizing the importance of informed consent. Additionally, if publicly available data is used, it is advisable to cite the

[22] WP29 Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251), point IV.B, pages 20 et seq.

[23] See also GDPR Preamble, paragraph 42: "[...] In order for consent to be informed, the data subject must be informed, at least, of the identity of the controller and the purposes of the processing. [...]."

[24] Article 7 and Recital 32, 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).

[25] Ibid, Recital 50.

[26] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 7.

source. Throughout the research process, correctly identifying and adequately protecting personal data categories is essential. Personal data may include a subject's name, home address, email address, or geographic location, while special categories—such as religious beliefs, political opinions, or medical data—require heightened protection due to the potential harm that unauthorized disclosure may cause.[27]

The selection of technical and organizational measures for data protection should consider the identity of the respondents, as different categories of data subjects may require tailored safeguards. Research participants may include patients, volunteers in surveys or medical studies, employees (e.g., laboratory staff), fellow researchers, minors, or adolescents, each necessitating varying levels of data protection.[28]

When secondary processing is not based on consent or a legal requirement, the controller may still process data in line with the original purpose if a "compatibility test" is satisfied.[29] This test assesses whether the new purpose aligns with the initial one, taking into account factors such as the relationship between the original and new purposes, the context in which the data was collected, the sensitivity of the data, the impact on the data subjects' rights, and whether adequate safeguards[30] mitigate the risks of processing.[31]

Article 4 of the Law of Georgia on Personal Data Protection outlines exceptions where further data processing is deemed compatible with the original purpose. These exceptions include processing for archiving, scientific, historical research, or statistical purposes[32] in the public interest. However, even in such cases, controllers must evaluate the lawfulness of further processing, particularly by assessing its compatibility with the initial purpose of data collection

[27] Personal Data Protection Service, Personal Data Protection Guidelines and Recommendations for Small and Medium-Sized Entrepreneurs, 2024, 11.
[28] Recommendations of the Personal Data Protection Service on the Principles of Personal Data Processing, 2024, 17.
[29] *Mészáros J., Ho Chih-hsing,* Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, 2018, 4.
[30] Art. 89, 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).
[31] Ibid, art. 5(1).
[32] Recommendations of the Personal Data Protection Service "On the Principles of Personal Data Processing", 2024, 17.

5. Key Considerations During the Planning and Implementation Stages of Research

To comply with data protection legislation, researchers must carefully consider the information provided to study participants. This information should be presented in clear and accessible language, ensuring that respondents can make an informed and voluntary decision about their participation. One effective way to inform participants is by providing a pre-prepared information sheet[33] about the study, along with an informed consent protocol attached to the questionnaire.[34]

A crucial aspect of informing respondents about data processing is establishing initial contact and inviting them to participate. Even when respondents are family members or friends, it remains essential to share all relevant information and obtain explicit consent for data processing. If a person cannot provide consent—such as in the case of minors—permission must be obtained from their parent, guardian, or legal representative.

For research involving fieldwork, obtaining informed consent may be an ongoing process rather than a one-time procedure. The process may evolve as new, unforeseen issues arise during the study. In such cases, researchers may need to renegotiate consent, especially if additional information is required during an interview or questionnaire. At the outset of communication, respondents should also be informed about possible exceptions to obtaining informed consent and the potential need for renegotiation, depending on the conversation's direction or the study's evolving needs.

Cultural and ethical norms must be taken into account when obtaining consent. In some communities, written consent may not align with local ethical standards, or it may be impractical to obtain. In such cases, alternative consent mechanisms—such as verbal consent records or the presence of a witness—should be considered. Regardless of the method used, proper documentation of the consent procedure must be maintained. When respondents cannot clearly express their wishes or fully comprehend the information, informed consent should be replaced with an appropriate alternative measure.

For observational research, consent must be obtained from both data subjects and any responsible supervisors, guardians, or authorities before the study begins. However, observations conducted in public spaces may not

[33] *Katulic T., Katulic A.,* GDPR and the Reuse of Personal Data in Scientific Research, International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, 1311-1316.
[34] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 15.

always require consent. In these cases, researchers must ensure that their study does not alter people's behavior or infringe upon their privacy rights.[35]

Special considerations apply when conducting research involving children. Researchers should use child-friendly methods to explain data processing, such as audio or video materials or simplified information leaflets. Additionally, researchers must have the authority to process personal data. If reprocessing data initially collected for another study, new consent must be obtained unless the original consent explicitly covers further processing. When using a database created for a previous project, researchers must assess whether the initial informed consent applies to the new study. Ethical committees, data protection officers, or supervisory authorities should be consulted for guidance on these matters.

6. Data Security

To ensure the secure processing of personal data, it is essential to implement appropriate technical and organizational measures to prevent unauthorized access.[36] In academic and scientific research, one effective method for safeguarding data security is maintaining access records, known as "logging," which track who accessed specific information, when, and what data was accessed. Additional security measures may be applied based on the research context, such as user authentication, password protection for electronic files, or encrypting databases—storing data in a form that is unreadable without a decryption key.

Regardless of where data is stored—whether on a personal computer, memory card, or cloud platform—the same legal requirements for data protection apply. Clear and periodically updated rules for secure access to personal data should be in place, proportional to the level of risk and the category of data being processed. For instance, special categories of data or research involving vulnerable respondents may require stricter security measures. It is advisable to document access rules and security protocols, including encryption, password protection, and other safeguards. In some cases, data should be separated from other information to enhance security. For example, segregating databases can prevent unauthorized individuals from

[35] Ibid.
[36] EDPS, Preliminary Opinion on Data Protection and Scientific Research, 2020, 24.

identifying data subjects, and special categories of personal data may be stored separately for added protection. Additionally, an action plan may be required for handling unplanned data that researchers unexpectedly acquire during the study.[37]

To protect against unauthorized access, it may be necessary to separate personal data from other information. One effective method is the partitioning of databases, ensuring that unauthorized individuals cannot identify data subjects. Special categories of personal data may require additional safeguards, such as separate storage from general personal data. Additionally, researchers should develop an action plan for handling data that was not originally intended to be collected but became available unexpectedly during the research process.

When transferring data, the data controller must assess the adequacy of the recipient's data protection measures. Research participants should be informed if their data will be transferred to third countries. While the data controller may verbally explain international data transfers to the data subject, this can make it difficult to document consent. Therefore, it is advisable to obtain written consent reflecting the respondent's agreement to the processing of their personal data. Before transferring data abroad, the adequacy of data protection in the recipient country should be evaluated, considering the methods of transfer.[38] The Personal Data Protection Service assesses whether appropriate safeguards exist in the receiving country or international organization based on an analysis of relevant legislation and practices.[39]

Depersonalization is an effective tool for protecting personal data security, as it enables research while preserving confidentiality.[40] This process involves removing direct identifiers, such as names, birthdates, or addresses. However, it does not entirely eliminate the risk of re-identification, as data subjects may still be identifiable through the combination of different data points.[41]

A commonly used depersonalization technique is randomization, which removes any direct link between the data subject and the information.[42] If data

[37] Article 4(13), (14) and (15) andArticle 9 and Recitals (51) to (56), 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).

[38] *Tsagareishvili N.,* Legal Regulation of International Transfer of Personal Data (International and National Standards), Journal of Personal Data Protection Law, №1, 2024, 84.

[39] Law of Georgia "On Personal Data Protection", Article 42.

[40] Recommendations on the principles of personal data processing, 2024, 27.

[41] Ibid, Article 3(c).

[42] AEPD, 10 Misunderstandings relating to Anonymisation, 2021, 5.

is presented in a sufficiently vague manner, it becomes difficult to associate it with an individual.[43] Another approach is generalization, which reduces the likelihood of identification by broadening data categories. For example, instead of specifying a city of residence, the researcher may indicate only a broader region, or instead of listing a respondent's exact age, they may categorize them into an age group. However, these methods alone may not fully prevent re-identification, making it essential to choose data protection strategies tailored to the specific research context.

Adhering to the principles of data minimization and security is a crucial aspect of research ethics. A notable example is the Swedish Data Protection Supervisory Authority's decision to fine Umeå University for storing special categories of personal data on a cloud platform without implementing adequate security measures. This case underscores researchers' obligation to ensure proper data protection mechanisms, such as encryption or anonymization, when handling sensitive personal data.[44]

Another effective security measure is pseudonymization,[45] where personally identifiable characteristics are replaced with coded identifiers. If personal data is stored by a third party or in a cloud system, it is necessary to verify that the data has been securely deleted after use.[46] Additionally, when personal data is transferred to a third party, it is recommended to confirm that they have erased the information once the processing purpose has been fulfilled.

[43] Article 29 WP Opinion on Anonymisation Techniques, 2014.
[44] Decision of the DPA (Sweden), DI-2019-9432, 2020, <https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-9432> [24.02.2025].
[45] *Manis M. L.,* The Processing of Personal Data in the Context of Scientific Research, The New Regime under the EU-GDPR, BioLaw Journal, 3/2017, 344.
[46] EDPB Guidelines 01/2025 on Pseudonymisation, 2025, 36.

7. Conclusion

With the enactment of the new Law on Personal Data Protection, maintaining high standards of data security while balancing research interests has become increasingly important. Researchers now bear the burden of demonstrating compliance with data protection laws at every stage of research planning and implementation.

Respecting the confidentiality of data subjects and obtaining informed consent are fundamental aspects of the research process. In academic and scientific research, secondary data processing—where data is used for purposes beyond those originally specified—is common. In such cases, researchers must either obtain new consent from the data subject or ensure a valid legal basis for processing.

Personal data must be processed in accordance with core data protection principles: it must be handled lawfully and transparently, collected for specific, explicit, and legitimate purposes, and maintained accurately and up to date where necessary. Data should only be retained for as long as required for the intended purpose, and appropriate technical and organizational measures must be implemented to safeguard its security. Special categories of data, such as health-related or religious information, require heightened caution and explicit consent from the data subject.

Ensuring data security requires both technical and organizational safeguards, including encryption, password protection, and controlled access. Additionally, depersonalizing or pseudonymizing data can help minimize the risk of identifying individuals.

Adhering to personal data protection principles in scientific and academic research is not merely a legal obligation but also an ethical responsibility. Upholding these standards safeguards the rights of data subjects and reinforces the integrity and credibility of research.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 14/06/2023.
2. 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 Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.
3. *Chassang G.,* The Impact of the EU General Data Protection Regulation on Scientific Research, Ecancer Medical Science, 2017, <https://pubmed.ncbi.nlm.nih.gov/28144283/> [20.02.2025].
4. *Ducato R.,* Data protection, Scientific Research, and the Role of Information, Computer Law & Security Review, Vol. 37, 2020.
5. EDPB Guidelines 01/2025 on Pseudonymisation, 2025.
6. EDPS, Preliminary Opinion on Data Protection and Scientific Research, 2020.
7. European University Institute, Guide on Good Data Protection Practice in Research, 2022.
8. Guideline Recommendation 05/2020 on Consent, under Regulation 2016/679.
9. ICO, Guideline on Principle of Storage Limitation, <https://ico.org.uk/> [20.02.2025].
10. *Katulic T., Katulic A.,* GDPR and the Reuse of Personal Data in Scientific Research, International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018.
11. *Lallie H. S., Thompson A., Titis E., Stephens P.,* Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector, 2025, 20.
12. *Manis M. L.,* The Processing of Personal Data in the Context of Scientific Research, The New Regime under the EU-GDPR, BioLaw Journal, 3/2017.
13. *Malgieri G.,* Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic, Computer Law & Security Review, 2020.
14. *Mészáros J., Ho Chih-hsing,* Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, 2018.
15. Personal Data Protection Service, Recommendations on the Principles of Personal Data Processing, 2024, 7.
16. Personal Data Protection Office, Personal Data Protection Guidelines for Small and Medium-sized Enterprises, 2024, 11.

17. Personal Data Protection Service of Georgia, Recommendations on the Development of a Privacy Policy Document, 2025.
18. *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021.
19. *Schaar K.,* Working Paper: What is important for Data Protection in science in the future? General and Specific Changes in Data Protection for Scientific Use Resulting from the EU General Data Protection Regulation RatSWD Working Paper, No. 258, 2016.
20. *Tsagareishvili N.,* Legal Regulation of International Transfers of Personal Data (International and National Standards), Journal of Personal Data Protection Law, №1, 2024.
21. Working Party 29 Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251).
22. Decision of the DPA (Sweden), 2020, <https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-9432> [24.02.2025].