Polski Merkuriusz Lekarski

POLISH MEDICAL JOURNAL

ISSN 1426-9686

VOLUME LIV, ISSUE 1, JANUARY-FEBRUARY 2026

Polski Merkuriusz Lekarski

POLISH MEDICAL JOURNAL

ISSN 1426-9686

VOLUME LIV ISSUE 1, JANUARY-FEBRUARY 2026

EDITORIAL BOARD

Polski Merkuriusz Lekarski cited by PUBMED/MEDLINE, SCOPUS, INDEX COPERNICUS, EBSCO, POLISH MEDICAL BIBLIOGRAPHY, Ministry of Science and Higer Education.

© **ALUNA PUBLISHING**
29 Z.M. Przesmyckiego St.
05-510 Konstancin-Jeziorna, Poland
tel. +48 604 776 311
a.luczynska@wydawnictwo-aluna.pl

www.polskimerkuriuszlekarski.pl

CONTENTS

ORIGINAL ARTICLES

REVIEW ARTICLES

CASE STUDY

VARIA

REVIEW ARTICLE

Protection of personal medical data in the context of GDPR implementation

Anzhela B. Berzina[1], Serhii S. Rozsokha[2], Olena P. Makhmurova-Dyshliuk[3], Alina O. Pletenetska[1]

[1]BOGOMOLETS NATIONAL MEDICAL UNIVERSITY, KYIV, UKRAINE
[2]SCIENTIFIC RESEARCH INSTITUTE OF MARITIME AND SPACE LAW, KYIV, UKRAINE
[3]KYIV UNIVERSITY OF INTELLECTUAL PROPERTY AND LAW, KYIV, UKRAINE

ABSTRACT

Aim: To analyse the challenges of protecting personal medical data in European Union (EU) Member States and other European countries during the implementation of Regulation 2016/679 (General Data Protection Regulation [GDPR]).

Materials and Methods: The study is based on an analysis of international and national legal frameworks governing personal medical data protection, focusing on the GDPR, the case law of the European Court of Human Rights (seven relevant judgments), and national data protection legislation. Statistical data from reports of national Data Protection Authorities were analyzed to identify dominant categories of infringements related to unlawful processing, storage, disclosure, and security breaches of medical data. The methodology included a comparative analysis of European Court of Human Rights judgments and an overview of enforcement activities of data protection authorities in 27 EU Member States. Dialectical, hermeneutic, comparative, analytical, and systemic analysis methods were applied.

Conclusions: To comply with the GDPR, healthcare institutions must ensure lawful and secure processing of personal medical data: organize internal procedures, appoint a Data Protection Officer, implement technical and organizational measures, obtain informed consent from patients, and guarantee their rights to access and protect such sensitive information. The protection of personal medical data is ensured through a multi-level system that combines the GDPR, the European Court of Human Rights case law, and national institutions. It is essential to develop and implement clear data protection policies that define responsibilities, data handling procedures and incident response. Many countries still have low awareness among medical personnel regarding personal data protection.

KEYWORDS: public administration, ethical standards, personal data

Pol Merkur Lek,2026;54(1):66-72 doi: 10.36740/Merkur202601110

INTRODUCTION

A growing number of countries are applying digitalization processes in healthcare systems, which leads to an increase in the volume of personal medical data processing. The protection of personal medical data is highly specific and requires legal regulation. This is important because medical information belongs to the sensitive category, and its illegal disclosure violates the rights of patients and may carry legal risks for the organization that has not provided such protection [1, 2].

AIM

The aim of the study is to analyse the challenges of protecting personal medical data in the European Union (EU) Member States and other European countries during the implementation of the General Data Protection Regulation (GDPR).

MATERIALS AND METHODS

This study was conducted to analyze the legal regulation of personal medical data protection, with a particular focus on the implementation of Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) and the relevant case law of the European Court of Human Rights (ECHR).

A comprehensive literature search was conducted using the following databases: Google Scholar, PubMed, Scopus, Web of Science, and SpringerLink. The search covered publications from 2016 to 2025, corresponding to the period of GDPR implementation, while the analysis of ECHR case law encompassed decisions from 1997 to the present.

The search included combinations of the following keywords: personal data protection, medical data, GDPR enforcement, healthcare privacy, data breaches in healthcare, public administration, ethical standards, personal data, and GDPR compliance.

Studies were selected based on the following inclusion criteria: peer-reviewed scientific articles, official EU legal acts, analytical and monitoring reports of data protection authorities, and ECHR judgments related to personal medical data protection. The following were excluded from the review: conference abstracts, editorials, opinion pieces, non-peer-reviewed publications, and unofficial commentaries.

The initial search yielded more than 60 potentially relevant sources. After relevance screening, 28 sources were included in the final review, fully corresponding to the reference list. In addition, the study provided a comparative overview of enforcement activities of data protection authorities in 27

EU Member States, with an analysis of administrative fines imposed for unlawful processing, storage, disclosure, or security breaches of medical data, enabling identification of dominant categories of violations and enforcement trends in healthcare.

The research employed dialectical, hermeneutic, comparative, analytical, synthetic, and system analysis methods.

ETHICS

This review article is based on an analysis of publicly available scientific data published in peer-reviewed journals, clinical guidelines, and databases. No patient-identifying data were used during the work, and no approval from an ethics committee was required, as the study did not involve new clinical interventions or primary collection of patient information. The authors adhered to the ethical principles of the Declaration of Helsinki of the World Medical Association and international standards for publication in medical journals, including the recommendations of the ICMJE (International Committee of Medical Journal Editors).

No element of the work contains plagiarism or fabrication of data. All sources of information are appropriately cited and properly formatted.

FRAMEWORK

The study was conducted as a fragment of the complex scientific project of the Bogomolets National Medical University «Forensic medical assessment of the impact of subclinical alcohol intoxication on human cognitive functions» (state registration number 0125U000571; term: 2025-2027).

REVIEW AND DISCUSSION

Personal medical data are subject to legal protection that establishes a special regime of compliance with confidentiality and security standards. This is important for medical institutions. Any action with such data (collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction) may be carried out exclusively in accordance with the law [1-4].

The protection of personal medical data within the EU is ensured through a multi-level system that combines the ECHR, the EU institutions, and national supervisory bodies. At the national level, these principles are implemented by Data Protection Authorities (DPAs) and courts, which apply both the GDPR and national legislation, guided by the case law of the ECHR. National courts frequently refer to both the GDPR and the ECHR's case law when resolving disputes related to personal medical data. Among the case law of the ECHR are Z. v. Finland (1997) [5], M.S. v. Sweden (1997) [6], Von Hannover v. Germany (2002) [7], Poltoratsky v. Ukraine (2003) [8], Birzykowski v. Poland (2006) [9], S. and Marper v. the United Kingdom (2008) [10], and Jilberg v. Sweden (2012) [11], which are compared in Table 1.

Table 1 illustrates the growing body of case law of the ECHR concerning the protection of the right to privacy and the confidentiality of personal medical data. The ECHR, both in practice and in principle, recognizes that personal medical data constitute sensitive information and that the protection of this right is closely linked to safeguarding human dignity and personal integrity. Beginning with the case Z. v. Finland (1997) [5], the ECHR emphasized that any disclosure of medical information must be justified, necessary, and proportionate, as derived from Article 8 of the Convention for the Protection of Human Rights

Table 1. ECHR Cases Protecting Personal Medical Data

ECHR Case	Z v. Finland [5]	M.S. v. Sweden [6]	Von Hannover v. Germany [7]	Poltoratsky v. Ukraine [8]	Birzykowski v. Poland [9]	S. and Marper v. the United Kingdom [10]	Jilberg v. Sweden [11]
Year	1997	1997	2002	2003	2006	2008	2012
Country Involved	Finland	Sweden	Germany	Ukraine	Poland	United Kingdom	Sweden
Core Issue	Disclosure of HIV status during criminal proceedings	Sharing of medical data by authorities without consent	Publication of private health and family details of public figures	Improper access to prisoner's medical records	Disclosure of hospital medical reports in court	Retention of DNA and biometric data by authorities	Use of patient records for research without proper anonymization
ECHR Findings (Article 8)	Violation of the right to respect for private life	Violation found	Violation found	Violation found	Violation found	Violation found	Violation found
Content	Medical data is highly sensitive; any disclosure must be justified, necessary, and proportionate	Protection of health data requires strict confidentiality and limiting the purposes of disclosure	Even public figures enjoy protection of private and medical information	State must ensure confidentiality of medical data even in detention settings	Unauthorized sharing of hospital records breaches privacy rights	Genetic and biometric data fall under sensitive personal data requiring strict safeguards	Research use of medical data must ensure effective anonymization and consent mechanisms

Source: compiled by the authors based on [5-11]

and Fundamental Freedoms (1950). The case law is not limited to a single decision; the specificities of different types of personal medical data are emerging in new ECHR judgments (for example, in cases related to the retention or use of genetic data).

When the EU adopted the GDPR in 2016 [12], it incorporated many of the safeguards already formulated in ECHR judgments. The legal framework for the protection of personal medical data of EU citizens was harmonised, as each national regime had its own specific features, which in turn required unification. Since 2016, EU healthcare institutions have been obliged to write their internal compliance policies in such a way that they comply with the GDPR. First of all, this rule requires the appointment of data protection officers (DPOs) and the implementation of technical and organisational measures (TOMs) to ensure the lawful processing of medical data, notification of breaches of personal medical data protection to supervisory boards within 72 hours, etc. Core GDPR principles: explicit consent, data minimisation, purpose limitation, and security of processing – reflect the same rationale developed through ECHR jurisprudence: that the handling of personal medical data must always be lawful, transparent, and proportionate to a legitimate purpose. The GDPR represents not a departure from, but rather a continuation of the human rights-based standards for medical data protection first established by the ECHR.

The GDPR is mandatory for organizations that work with personal medical data of EU residents (including residents located outside the EU). Such strictness is not accidental; it should ensure adequate "legal steps" to change social relations towards their digital transformation (namely, the rapid growth of data processing on the Internet and the development of "big data" systems, as well as the gradual unification of medical information systems). Thus, it is important that:

– firstly, the GDPR has an extraterritorial principle of operation and applies to all organizations (including medical institutions, private clinics, pharmaceutical companies, research centers and non-profit organizations) that process, use or store personal medical data of EU residents [13, 14]. Even if the organization has no physical establishment in Europe, it is still required to implement appropriate legal, organizational, and technical measures to ensure the protection of personal medical data. In other words, if a medical company, clinic or telemedicine platform does not have an office in the EU, but provides remote consultations or laboratory services to patient's resident in the EU, uses their medical data (anamnesis, test results, electronic prescriptions, telemedicine consultation records etc.) or stores this data in its information systems, such activities automatically fall under the GDPR. For example, if a Ukrainian private laboratory performs tests for patients from Poland or Germany, sending results by email or via an online platform, then despite the fact that the laboratory is physically located outside the EU, it processes personal medical data of EU residents and therefore must comply with the GDPR requirements;
– secondly, compliance (or GDPR compliance programs) plays a crucial role in mitigating these risks. Establishing a robust compliance framework enables medical institutions and organizations to systematically implement all necessary legal, technical, and organizational measures [15, 16]. If the personal data controller has not implemented appropriate technical and organizational measures to ensure the protection of the rights of data subjects, has not taken into account data protection by design or has not notified the data breach incident to the supervisory authority within 72 hours of becoming aware of the breach, and such incident has resulted in a violation of the rights or freedoms of individuals, fines of up to 20 000 000 euros or 4% of the company's global annual revenue (whichever is higher) are provided for. The supervisory authority has the right to apply additional corrective measures, such as issuing an order to stop processing personal data, temporarily or permanently restricting access to the data or requiring the deletion of data that was processed in violation;
– thirdly, in order to minimize the risk of liability, it is advisable for medical institutions processing personal medical data of EU residents to take the following steps:
  1) ensure compliance of internal processes with the requirements of the GDPR, namely to determine that the full cycle of processing personal medical data (from collection to storage and transfer or destruction) must comply with the principles of proportionality and data minimization. In case of processing outside the EU, the destination country must be granted the status of one that ensures an adequate level of data protection;
  2) take the necessary measures to ensure appropriate security measures, for example, by including special clauses in contracts with partners, suppliers, laboratories or insurance companies, special conditions for processing and storing personal medical data should be provided, as well as determine the liability of the subjects for violation of these conditions. Internal policies of medical institutions should contain provisions on the role and responsibilities of the DPO;
  3) receive and/or process personal medical data with the informed consent of the individual whose data is being processed. Such consent must be clear, freely and consciously given, in writing or in electronic form with the possibility of its verification and withdrawal. Exceptions are permitted only in cases expressly provided by law, such as for the protection of an individual's life or public health;
  4) inform the subject of medical data about the purpose of processing, storage periods, categories of persons to whom the data may be transferred, and also ensure the patient's right to access their data, correct or delete inaccurate information, restrict or object to processing, and transfer data (data portability);
  5) ensure compliance with technical and organizational requirements for the implementation of the above rights, in particular through electronic patient acco-

unts in the system (for example, in Ukraine, this is the eHealth and Health24 systems);

– fourthly, the main problems that remain unresolved in countries that are at the stage of implementing the GDPR (in particular, Ukraine) include:
  1) insufficient awareness of medical personnel with the principles of personal medical data protection. A significant part of doctors, nurses and administrative staff do not have proper training in the practical application of GDPR requirements. Most medical institutions lack training programs on confidentiality and ethical handling of patient data. As a result, medical personnel often violate the principles of data minimization, incorrectly determine the purpose of their processing or violate the security of their transmission;
  2) technical vulnerability of electronic medical data storage systems. The vulnerability of such systems makes them a target for cybercriminals. There is also a lack of effective control over illegal data dissemination.

Promising directions identified in recent regulatory practice include the harmonisation of standards for the exchange of medical data, ensuring the right of patients to confidentiality. Each person who transfers their personal data should be granted the rights (and not only declaratively):

a) to request the destruction of their personal data if they are no longer needed for the purposes for which they were collected;
b) to receive information about what data is processed, for what purpose, and to request their correction;
c) to request the temporary cessation of data processing under certain conditions (for example, if the data is contested);
d) to object to the use of data, for example, for direct marketing purposes.

Each medical institution that processes patients' medical data must develop and approve an internal privacy policy [17–19]. Such a document must determine the procedure for collecting, storing, processing, transferring, and destroying personal data; categories of persons who have access to information; and responding to incidents of leakage or unauthorised access. Internal regulations and contracts must be reviewed and adapted to the requirements of the law. This applies to both contracts with clients and with IT contractors and services. It is important to develop a clear procedure for reporting data leaks. It is seen that the introduction of certification of medical information systems according to international standards (ISO/IEC 27701, which is a certification for Privacy Information Management Systems), in particular for countries that are not EU members, will increase their compatibility with European platforms.

The protection of personal medical data is a right guaranteed to everyone. In Article 4 of the GDPR, the term "data concerning health" is used. Such data are classified as special categories of personal data that require a higher level of protection. These include information about «personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status» [12]. The processing of such data is permitted only if there is a clear legal basis – the consent of the data subject or the need to provide medical services in accordance with the requirements of the law.

The issues of personal medical data protection are relevant both at the general theoretical [20-25] and regulatory levels [12]. The relevance of scientific research is confirmed by statistical data on the volume of fines imposed for violations of the GDPR. National data protection authorities of EU member states [26], including the Spanish Data Protection Agency, the French Commission Nationale de l'Informatique et des Libertés, and the Italian Garante per la protezione dei dati personali, among others, apply sanctions to medical institutions, pharmaceutical companies, and individual medical practices for violating the GDPR.

Fig. 1 and Fig. 2 present the data from the EnforcementTracker.com database for the period 2018-2025, illustrating the distribution of GDPR administrative fines by economic sector and by type of violation [27]. These figures reflect both the scale and the diversity of challenges related to personal data protection, including the healthcare sector. The analysis is based on publicly available enforcement decisions adopted by national data protection authorities under Regulation (EU) 2016/679. The data systematized by the authors according to sector, number of cases, and total amount of fines. Only finalized enforcement decisions were included in the analysis.

As we can see, although the healthcare sector is not among the leaders in terms of the total amount of fines, it has a large number of incidents (257), which indicates existing problems in the processing of personal medical data (for comparison: in the financial sector there are fewer cases, but significantly larger fines. However, these indicators may be affected by the type of activity and the size of the user base, and the amount of financial liability depends on this) (Fig. 1).

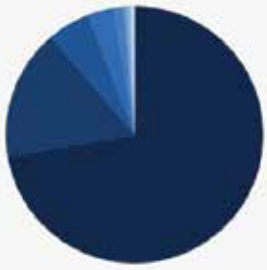
Fig. 2 presents the distribution of administrative fines by main categories of GDPR infringements, including unlawful processing, violations of general data processing principles, and insufficient technical and organisational measures. An analysis of the three main categories shows that most violations stem from unlawful or insufficiently legal grounds for data processing (e.g., processing without proper patient consent or unlawful transfer to third parties). The high rate of non-compliance with the general principles of processing indicates violations ranging from opaque privacy policies to data retention longer than necessary. The third most important category, insufficient technical and organisational protection, directly affects healthcare institutions, which often lack modern encryption systems, access auditing, or leak response procedures.

In the annual report Protecting Personal Data in a Changing Landscape (2024), it is stated that the 2024-2027 Strategy provides a comprehensive roadmap to address emerging challenges, safeguard fundamental rights, and adapt to the rapid evolution of digital technologies. National DPAs

Statistics: Fines by sectors
The following statistics show how many fines and what sum of fines have been imposed to date in each sector.

Note: Only fines with valid information on the amount of the fine and on the the corresponding sector are taken into account.

1. By total sum of fines:



Sector	Sum of Fines
Media, Telecoms and Broadcasting	**€ 4,905,920,868** (at 346 fines)
Industry and Commerce	**€ 1,120,852,727** (at 540 fines)
Employment	**€ 360,498,217** (at 174 fines)
Transportation and Energy	**€ 222,367,521** (at 153 fines)
Finance, Insurance and Consulting	**€ 82,423,108** (at 297 fines)
Health Care	**€ 31,093,279** (at 257 fines)
Public Sector and Education	**€ 30,885,763** (at 290 fines)
Accomodation and Hospitality	**€ 22,699,248** (at 83 fines)
Individuals and Private Associations	**€ 4,257,481** (at 323 fines)
Not assigned	**€ 3,614,609** (at 198 fines)
Real Estate	**€ 3,001,571** (at 79 fines)

Fig. 1. Statistics on GDPR administrative fines for 2018-2025, including the health care sector

Source: compiled by the authors based on [27]

Statistics: Fines by type of violation
The following statistics show how many fines and what sum of fines have been imposed per type of GDPR violation to date.

Note: Only fines with valid information on the amount of the fine and on the type of violation are taken into account.

1. By total sum of fines:

Violation	Sum of Fines
Insufficient legal basis for data processing	**€ 3,004,692,817** (at 773 fines)
Non-compliance with general data processing principles	**€ 2,511,690,330** (at 717 fines)
Insufficient technical and organisational measures to ensure information security	**€ 877,952,537** (at 508 fines)
Insufficient fulfilment of information obligations	**€ 252,723,860** (at 202 fines)
Insufficient fulfilment of data subjects rights	**€ 103,012,766** (at 274 fines)
Unknown	**€ 24,325,341** (at 19 fines)
Insufficient cooperation with supervisory authority	**€ 7,089,169** (at 154 fines)
Insufficient fulfilment of data breach notification obligations	**€ 3,985,392** (at 48 fines)
Insufficient data processing agreement	**€ 1,128,510** (at 14 fines)
Insufficient involvement of data protection officer	**€ 978,000** (at 25 fines)
Lack of appointment of data protection officer	**€ 35,670** (at 6 fines)

Fig. 2. Distribution of fines by type of GDPR violations for 2018-2025

Source: compiled by the authors based on [27]

should prioritise the information security of medical IT systems that use personal health data, including electronic patient records, telemedicine services, mobile applications for health monitoring, and information exchange systems between hospitals [28]. European regulators consider such breaches to be among the most dangerous, since the leakage of even a limited amount of health data can lead to a violation of personal dignity, discrimination, misuse of medical information, or a violation of medical confidentiality. For example, in 2024, the Croatian Data Protection Authority conducted 623 investigations, received 1 280 complaints, issued 153 compliance orders, and adopted 191 sanctions, including 38 fines. Several complaints were filed by data subjects who had requested copies of their health data. The hospital concerned failed to provide these copies, claiming that the requested medical documentation had been irretrievably lost. As the hospital had not implemented adequate backup mechanisms for personal data, access to the data subjects' information was permanently lost, constituting a breach of Article 32(1)(b) of the GDPR. Furthermore, the Agency concluded that the hospital had violated several provisions concerning data security and integrity. The Croatian DPA imposed an administrative fine of €190 000 [28].

CONCLUSIONS

1. The protection of personal medical data within the EU is ensured through a multi-level system that combines the ECHR, the EU institutions, and national supervisory bodies. National courts frequently refer to both

the GDPR and the ECHR's case law when resolving disputes related to personal medical data.

2. The GDPR has extraterritorial effect and covers any activity related to the processing of personal medical data of EU citizens, even if such processing is carried out outside its territory.
3. In order to comply with the GDPR, healthcare providers must ensure the lawful, transparent, and secure processing of personal medical data. This entails appointing Data Protection Officers, implementing appropriate technical and organizational measures, obtaining valid informed consent from patients where required by law, and effectively guaranteeing data subjects' rights to access, rectify, erase, restrict, or object to the processing of their personal medical data. Furthermore, healthcare institutions should develop and implement comprehensive internal data protection policies that clearly define responsibilities, data handling procedures, incident response mechanisms, and staff training programs to ensure consistent and effective GDPR compliance. At the same time, many European countries continue to face persistent challenges in GDPR implementation within the healthcare sector, including insufficient awareness among medical personnel regarding personal data protection requirements, technical vulnerabilities of healthcare information systems, and inadequate oversight of confidentiality compliance.

REFERENCES

1. Fatehi F, Hassandoust F, Ko RKL, Akhlaghpour S. General Data Protection Regulation (GDPR) in Healthcare: Hot Topics and Research Fronts. Stud Health Technol Inform. 2020;270:1118-1122. doi: 10.3233/SHTI200336.
2. Conduah AK, Ofoe S, Siaw-Marfo D. Data privacy in healthcare: Global challenges and solutions. Digit Health. 2025;11:20552076251343959. doi: 10.1177/20552076251343959.
3. McGraw D, Mandl KD. Privacy protections to encourage use of health-relevant digital data in a learning health system. NPJ Digit Med. 2021;4(1):2. doi: 10.1038/s41746-020-00362-8.
4. Jones MC, Stone T, Mason SM et al. Navigating data governance associated with real-world data for public benefit: an overview in the UK and future considerations. BMJ Open. 2023;13(10):e069925. doi: 10.1136/bmjopen-2022-069925.
5. Z. v. Finland, Application no. 22009/93, Judgment of 25 February 1997. European Court of Human Rights. HUDOC. https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-58033%22]} [Accessed 30 December 2025]
6. M.S. v. Sweden, Application no. 20837/92, Judgment of 27 August 1997. European Court of Human Rights. HUDOC. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-8905%22]} [Accessed 30 December 2025]
7. Von Hannover v. Germany, Application no. 59320/00, Judgment of 24 June 2004. European Court of Human Rights. HUDOC. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-61853%22]} [Accessed 30 December 2025]
8. Poltoratskiy v. Ukraine, Application no. 38812/97, Judgment of 29 April 2003. European Court of Human Rights. HUDOC. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-61059%22]} [Accessed 30 December 2025]
9. Byrzykowski v. Poland, Application no. 11562/05, Judgment of 27 June 2006. European Court of Human Rights. HUDOC. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-76066%22]} [Accessed 30 December 2025]
10. S. and Marper v. the United Kingdom, Applications nos. 30562/04 and 30566/04, Judgment of 4 December 2008. European Court of Human Rights. HUDOC. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]} [Accessed 30 December 2025]
11. Gillberg v. Sweden, Application no. 41723/06, Judgment of 3 April 2012. European Court of Human Rights. HUDOC. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-110144%22]} [Accessed 30 December 2025]
12. European Union. 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). 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 30 December 2025]
13. Vukovic J, Ivankovic D, Habl C, Dimnjakovic J. Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. Arch Public Health. 2022;80(1):115. doi: 10.1186/s13690-022-00866-7.
14. Molnár-Gábor F, Sellner J, Pagil S et al. Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden. Semin Cancer Biol. 2022;84:271-283. doi: 10.1016/j.semcancer.2021.12.001.
15. Berzina A, Pozhodzhuk T, Demchenko I et al. Compliance and due diligence in healthcare: international experience and implementation challenges. Wiad. Lek. 2025;78(11):2450-2455. doi: 10.36740/WLek/214795.
16. Barbaria S, Jemai A, Ceylan Hİ et al. Advancing Compliance with HIPAA and GDPR in Healthcare: A Blockchain-Based Strategy for Secure Data Exchange in Clinical Research Involving Private Health Information. Healthcare. 2025;13(20):2594. doi: 10.3390/healthcare13202594.
17. Jurczuk M, Suprunowicz M. Consent in Data Privacy: A General Comparison of GDPR and HIPAA. Adam Mickiewicz University Law Review. 2025;16:07. doi: 10.14746/ppuam.2024.16.07.
18. Hussein R, Wurhofer D, Strumegger EM et al. General Data Protection Regulation (GDPR) Toolkit for Digital Health. Stud Health Technol Inform. 2022;290:222-226. doi: 10.3233/SHTI220066.

19. Peloquin D, DiMaio M, Bierer B, Barnes M. Disruptive and avoidable: GDPR challenges to secondary research uses of data. Eur J Hum Genet. 2020;28(6):697-705. doi: 10.1038/s41431-020-0596-x.
20. Tschider C, Compagnucci MC, Minssen T. The new EU–US data protection framework's implications for healthcare. J Law Biosci. 2024;11(2):lsae022. doi: 10.1093/jlb/lsae022.
21. Diorditsa I, Kovalenko I, Koval' O. Pravova okhorony personal'nykh danykh u sferi okhorony zdorov''ya v Ukrayini. [Legal protection of personal data in the healthcare in Ukraine]. Uzhhorod National University Herald. Series: Law. 2024;24(1):141-146. doi:10.24144/2307-3322.2024.82.2.22. (Ukrainian)
22. Illyushyk O. Zakhyst personal'nykh danykh u telemedytsyni. [Protection of personal data in telemedicine]. Medical Law. 2024;1(33):9-21. doi:10.25040/medicallaw2024.01.009. (Ukrainian)
23. Conduah AK, Ofoe S, Siaw-Marfo D. Data privacy in healthcare: Global challenges and solutions. Digit Health. 2025;11:20552076251343959. doi: 10.1177/20552076251343959.
24. Revenco T. European Union Regulation on Personal Data Protection in Medical Writing. AMWA. 2024;39(3). doi:10.55752/amwa.2024.346.
25. Riou C, El Azzouzi M, Hespel A et al. Ensuring General Data Protection Regulation Compliance and Security in a Clinical Data Warehouse From a University Hospital: Implementation Study. JMIR Med Inform. 2025;13:e63754. doi: 10.2196/63754.
26. Kraus M. Health care. GDPR Enforcement Tracker Report 2024. CMS; 2024 May 15. https://cms.law/en/mco/publication/gdpr-enforcement-tracker-report-2024/health-care [Accessed 30 December 2025]
27. GDPR Enforcement Tracker: Insights. https://www.enforcementtracker.com/?insights [Accessed 30 December 2025]
28. European Data Protection Board. Protecting personal data in a changing landscape: Annual report 2024. Brussels: EDPB. 2025;55. https://www.edpb.europa.eu/system/files/2025-04/edpb-annual-report-2024_en.pdf [Accessed 30 December 2025]

CONFLICT OF INTEREST
The Authors declare no conflict of interest

CORRESPONDING AUTHOR
Anzhela B. Berzina
Bogomolets National Medical University
13 Taras Shevchenko Ave., 01601 Kyiv, Ukraine
e-mail: anzhela.kasumova@gmail.com

ORCID AND CONTRIBUTIONSHIP
Anzhela B. Berzina: 0000-0002-9885-309X A D E F
Serhii S. Rozsokha: 0000-0001-6039-3174 A D E F
Olena P. Makhmurova-Dyshliuk: 0000-0002-0969-8797 A E F
Alina O. Pletenetska: 0000-0002-7029-3377 A B F

A – Work concept and design, B – Data collection and analysis, C – Responsibility for statistical analysis, D – Writing the article, E – Critical review, F – Final approval of the article

RECEIVED: 08.09.2025
ACCEPTED: 17.01.2026

Wielka Księga Balneologii, Medycyny Fizykalnej i Uzdrowiskowej

Tom I Część ogólna

Tom II Część kliniczna

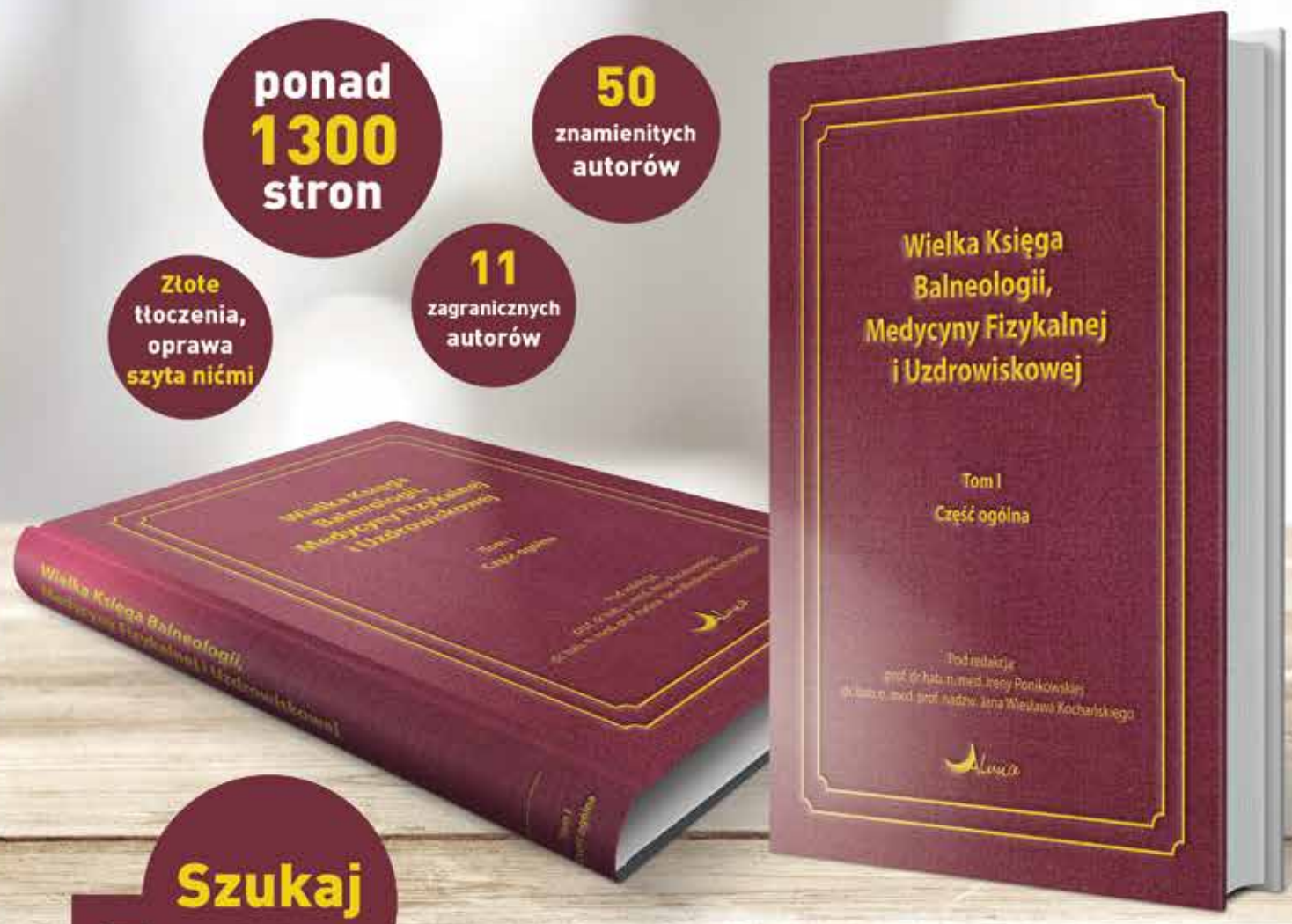
Pod redakcją:
prof. dr hab. n. med. Ireny Ponikowskiej
dr. hab. n. med. prof. nadzw. Jana Wiesława Kochańskiego

ponad 1300 stron

50 znamienitych autorów

11 zagranicznych autorów

Złote tłoczenia, oprawa **szyta nićmi**



Szukaj na

www.actabalneologica.pl