European Journal of Cardio-Thoracic Surgery 2023, 64(3), ezad289
https://doi.org/10.1093/ejcts/ezad289 Advance Access publication 17 August 2023

REVIEW

Cite this article as: Bertolaccini L, Falcoz P-E, Brunelli A, Batirel H, Furak J, Passani S *et al*. The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database. Eur J Cardiothorac Surg 2023; doi:10.1093/ejcts/ezad289.

The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database

Luca Bertolaccini [a,*], Pierre-Emmanuel Falcoz [b], Alessandro Brunelli [c], Hasan Batirel[d], Jozsef Furak [e], Stefano Passani [f] and Zalan Szanto [g]

[a] Department of Thoracic Surgery, IEO, European Institute of Oncology IRCCS, Milan, Italy
[b] Department of Thoracic Surgery, Strasbourg University Hospital, Strasbourg, France
[c] Department of Thoracic Surgery, St. James's University Hospital, Leeds, UK
[d] Faculty of Medicine, Department of Thoracic Surgery, Biruni University, Istanbul, Turkey
[e] Department of Surgery, University of Szeged, Szeged, Hungary
[f] KData Clinical, Rome, Italy
[g] Department of Thoracic Surgery, University of Pecs, Pecs, Hungary

* Corresponding author. Department of Thoracic Surgery, IEO, European Institute of Oncology IRCCS, Via Ripamonti 435, 20141 Milan, Italy. Tel: +39-02-57489665; fax: +39-02-56562994; e-mail: luca.bertolaccini@gmail.com (L. Bertolaccini).

Received 22 July 2023; accepted 16 August 2023

The Significance of General Data Protection Regulation in the Compliant Data Contribution to the European Society of Thoracic Surgeons Database

Summary

Key Question

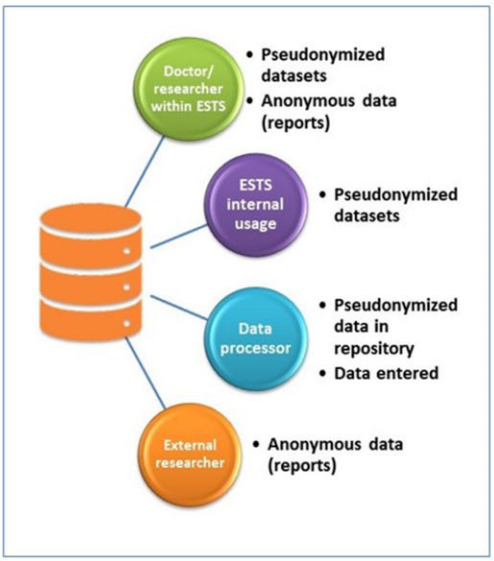
What are fundamental principles and implications of GDPR in context of data management, privacy rights, and compliance for organizations operating within European Union?

Key Finding

GDPR is a comprehensive data protection regulation implemented in the EU to harmonize and strengthen data protection regulations.

Take-Home Message

GDPR marks a pivotal shift in data protection and privacy practices. While challenges exist, embracing GDPR principles fosters a more secure and transparent digital environment and reinforces organizations' commitment to ethical data management.



Presented at the 31st European Conference on General Thoracic Surgery, Milan, Italy, 4–6 June 2023.

Abstract

The General Data Protection Regulation (GDPR), enacted in the European Union in 2018, has significantly transformed the landscape of personal data management and protection. This article provides an overview of GDPR's impact, focusing on its applicability, fundamental principles and influence on data management practices, particularly within the European Society of Thoracic Surgeons (ESTS) database.

GDPR's reach extends to all entities collecting and processing personal data of European Union residents, regardless of their location. It encompasses various data types, emphasizing meticulous handling and protection of identifiable information. Special categories of data, such as health and sensitive attributes, require even more stringent protection. The regulation sets legal, fair and transparent data processing principles, emphasizing accuracy, purpose limitation and data minimization. It also stresses accountability, leading to the appointment of Data Protection Officers and significant penalties for non-compliance.

The ESTS database, designed to enhance thoracic surgical research and care, collects data on European procedures. It follows GDPR principles by pseudonymizing data, ensuring secure data transmission and providing clear instructions for data submission. The database contributes to research, policymaking and practice improvement in thoracic surgery by offering a comprehensive dataset for analysis. Here, we aim to shed light on the complexities of GDPR implementation and emphasize the need for comprehensive data management strategies to ensure compliance and enhance privacy protection with the contribution to the ESTS database.

GDPR compliance comes with challenges, including potential human dignity and privacy rights violations. Data breaches can result in unauthorized disclosures, and non-compliance can lead to substantial fines and reputational damage. The implementation of GDPR encourages organizations to prioritize ethical data practices, security measures and transparent data handling.

In conclusion, GDPR has revolutionized personal data protection by emphasizing accountability, transparency and individual rights. It has impacted organizations globally, promoting responsible data management practices. Adhering to GDPR ensures privacy protection, trust-building and overall enhancement of data management in today's data-driven environment.

Keywords: Lung cancer • Database • Privacy • General Data Protection Regulation • European Union

ABBREVIATIONS

DPOs	Data Protection Officers
ESTS	European Society of Thoracic Surgeons
EU	European Union
GDPR	General Data Protection Regulation

INTRODUCTION

The General Data Protection Regulation (GDPR) has revolutionized how personal data are handled and protected, bringing forth a new era of privacy rights for individuals within the European Union (EU). With its far-reaching scope and stringent principles, GDPR ensures that businesses and organizations treat personal data with the utmost care and responsibility [1]. GDPR stands for General Data Protection Regulation, a comprehensive data protection law implemented in the EU on 25 May 2018. GDPR replaced the previous data protection directive and is designed to harmonize and strengthen data protection regulations within the EU. The primary objective of GDPR is to provide individuals with greater control over their personal data and to establish a framework for how organizations manage and process such data. It applies to all businesses and organizations that collect and process the personal data of EU residents, regardless of whether the organization is located within the EU or not [2].

Some fundamental principles and provisions of GDPR include the following:

- Consent. GDPR requires enterprises to get individuals' affirmative, explicit consent before collecting and processing their personal data. Consent must be freely given, specific, informed and unambiguous.
- Data subject rights. GDPR grants several rights to individuals, including the right to access their personal data, the right to rectify inaccurate information, the right to erasure (or 'right to be forgotten'), the right to data portability and the right to object to certain types of data processing.
- Data breach notification. Organizations must notify relevant supervisory authorities and affected individuals within 72 h of becoming aware of a data breach that could risk individuals' rights and freedoms.
- Accountability and privacy by design. GDPR emphasizes the concept of accountability, requiring organizations to demonstrate compliance with data protection principles. It also encourages the implementation of privacy safeguards from the outset of any data processing activities.
- Data Protection Officers (DPOs). In some instances, organizations must appoint a DPO to oversee data protection activities within the organization.
- Penalties and enforcement. GDPR imposes severe penalties for non-compliance, including fines of up to 4% of an organization's annual global revenue or €20 million, whichever is greater [2].

GDPR has had a far-reaching impact on data protection and privacy practices globally, as many organizations outside the EU have also adjusted their policies and practices to comply with its requirements [1].

Here, we aim to shed light on the complexities of GDPR implementation and emphasize the need for comprehensive data management strategies to ensure compliance and enhance privacy protection with the contribution to the European Society of Thoracic Surgeons (ESTS) database.

APPLICABILITY OF GENERAL DATA PROTECTION REGULATION

One of the fundamental questions surrounding GDPR is its applicability. The regulation encompasses those who offer goods or services to individuals within the EU and those who control and process data pertaining to EU citizens. This wide net ensures that organizations cannot evade their obligations by operating outside EU borders. Whether it is an e-commerce platform targeting EU consumers or a multinational company with branches in Europe, all entities must adhere to GDPR [3]. GDPR's extensive scope encompasses various data forms, including physical and electronic records. From handwritten documents to e-mails, databases and spreadsheets, any information relating to an identified or identifiable individual falls under the purview of GDPR. This broad definition ensures that no stone is left unturned when safeguarding personal data [1].

In practice, the concept of personal data extends to different scenarios. It covers research subjects whose data are collected and retained and individuals who may be identified through additional information even if their identities were initially anonymized. GDPR recognizes the importance of protecting these individuals' privacy rights, irrespective of the context in which their data are used [4]. Moreover, GDPR introduces the notion of special categories of personal data, previously referred to as 'sensitive personal data'. This includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and sexual orientation, genetic data and biometric data for unique identification. These categories require even more care and consideration in processing, ensuring that individuals' most sensitive attributes are protected. The GDPR establishes critical principles to ensure the protection of personal data. Data must be processed legally, fairly and transparently [5].

Additionally, data should only be obtained for specified purposes and not further processed beyond those purposes. It emphasizes the importance of ensuring that the data being processed are adequate, relevant and limited to what is necessary [6]. GDPR also highlights the significance of data accuracy and encourages organizations to keep data up to date when necessary. It emphasizes that data should not be retained longer than necessary, promoting responsible data management practices [7]. Furthermore, GDPR stresses the need for appropriate measures to be in place to prevent unauthorized processing, loss or destruction of data. This ensures the security and integrity of personal information [8].

Overall, GDPR sets forth these principles to ensure that individuals' personal data are handled carefully and in a manner that respects their rights and privacy. Compliance with these principles is crucial for organizations to meet the requirements of the regulation and maintain data protection standards. The responsibility for complying with GDPR falls on both data controllers and data processors. Data controllers are the ones who determine the means and purposes of data processing, such as investigator-initiated research projects. They must ensure that the principles of GDPR are followed throughout the entire data lifecycle [9].

On the other hand, data processors, such as clinical research coordinators or database administrators, carry out data processing activities under the direction and responsibility of data controllers [10]. By establishing a clear distinction between controllers and processors, GDPR fosters a culture of accountability and transparency. It compels all parties to handle personal data responsibly, with a heightened focus on privacy protection. Data controllers must provide explicit guidance to processors and monitor their activities to ensure compliance with GDPR's principles [10]. GDPR's impact extends far beyond the legal realm. It has pushed organizations to re-evaluate their data management practices and prioritize individuals' privacy. Implementing GDPR-compliant measures protects data subjects and helps businesses build trust and foster stronger relationships with their customers. By placing the rights and interests of individuals at the forefront, organizations can demonstrate their commitment to ethical data practices and responsible stewardship [3]. In today's data-driven world, safeguarding personal information and upholding individual privacy rights cannot be overstated. The GDPR, implemented in the EU, has been widely recognized as a significant step towards establishing a robust framework for data protection. However, it is essential to recognize that health data GDPR compliance is not universally applicable across all countries [11].

UNDERSTANDING THE CONTEXT AND THE DATAFLOW

Managing data compliant with GDPR requires a comprehensive understanding of the rights, obligations and needs associated with data processing [10]. Effective data management involves careful assessment of data procession, collection, transfer and storage [4]. Adhering to the main requirements of lawful data collection, transfer, storage and usage are crucial for maintaining compliance and protecting individuals' rights. The GDPR establishes critical principles to ensure the protection of personal data. Data must be processed legally, fairly and transparently [10].

Additionally, data should only be obtained for specified purposes and not further processed beyond those purposes. It emphasizes the importance of ensuring that the data being processed are adequate, relevant and limited to what is necessary [2]. GDPR also highlights the significance of data accuracy and encourages organizations to keep data up to date when necessary. It emphasizes that data should not be retained for longer than necessary, promoting responsible data management practices [10]. Furthermore, GDPR stresses the need for appropriate measures to be in place to prevent unauthorized processing, loss or destruction of data. This ensures the security and integrity of personal information [11]. Overall, GDPR sets forth these principles to ensure that individuals' personal data are handled carefully and in a manner that respects their rights and privacy [4]. Compliance with these principles is crucial for organizations to meet the requirements of the regulation and maintain data protection standards [11]. The GDPR has added fundamental principles to ensure the lawful, fair and transparent processing of personal information. Organizations must have valid grounds for processing data and cannot rely on vague justifications like 'it may be useful'. The principle of fairness emphasizes that consent must be freely given, specified, informed and unambiguous, clearly indicating the individual's wishes [11]. Transparency is another crucial aspect of GDPR. Organizations must provide individuals with information about the location of their data and clearly explain the purpose of data collection, as well as the legal basis for processing it. Data minimization is a fundamental principle encouraging organizations to collect and use only the data

necessary to fulfil the intended purpose. It discourages the practice of collecting or holding data 'just in case it might be useful', promoting a more focused and limited approach to data collection. Accuracy is essential in handling personal data. Organizations must ensure that any personal or special category data they collect are recorded accurately, minimizing the risk of errors or misleading information [4].

THE EUROPEAN SOCIETY OF THORACIC SURGEONS DATABASE

To promote clinical research and improve patient care, the ESTS has established a comprehensive and robust database called the ESTS database [12]. The primary objective of the ESTS database is to collect, analyse and disseminate high-quality data related to thoracic surgical procedures performed across Europe [13]. It is a valuable resource for thoracic surgeons, researchers and policymakers to gain insights into thoracic surgery practice outcomes, trends and variations [14]. By capturing a vast array of data, the database enables evidence-based decision-making, quality improvement initiatives and benchmarking of surgical performance [15]. The ESTS database operates voluntarily, with participating centres across Europe contributing data on thoracic surgical procedures. The database collects clinical and surgical data, encompassing domains such as patient demographics, preoperative risk factors, intraoperative details, postoperative outcomes and long-term follow-up information. A standardized data dictionary, developed collaboratively by the ESTS and participating centres, ensures consistency and comparability of the collected data. Data entry is facilitated through a secure online platform, ensuring data integrity, privacy and adherence to relevant data protection regulations. Participating centres typically enter data prospectively, although retrospective data collection is also possible. Regular data audits and validation checks are performed to maintain data quality and reliability. The ESTS database consists of modules focusing on specific thoracic surgical procedures or disease entities [16]. These modules include but are not limited to:

a. General Thoracic Surgery Module. This module encompasses a wide range of general thoracic surgical procedures, such as lobectomy, pneumonectomy, segmentectomy and mediastinal tumour resection.
b. Lung Cancer Module. Dedicated to lung cancer surgery, this module collects data on diagnostic workup, staging, surgical approach (open or minimally invasive), the extent of resection, lymph node dissection and adjuvant treatments.
c. Esophageal Cancer Module. Focusing on oesophageal cancer surgery, this module captures data on tumour location, histology, neoadjuvant therapy, surgical technique (oesophagectomy or endoscopic resection) and perioperative outcomes.

The ESTS database is a valuable tool for research and clinical applications, driving advancements in thoracic surgery. Its vast dataset allows for comprehensive analyses, including risk assessment models, comparative effectiveness studies and evaluation of novel surgical techniques. Researchers can leverage the database to explore perioperative complications, long-term survival and surgical outcome factors. Furthermore, the database supports quality improvement initiatives by providing participating centres with benchmarking reports, highlighting variations in practice and outcomes [17]. This facilitates the identification of areas for improvement, fosters collaboration and enhances the overall quality of thoracic surgical care. The ESTS Database has significantly contributed to thoracic surgery practice, research and policy-making. Its data-driven insights have influenced clinical guidelines, shaped treatment protocols and improved patient outcomes. The database has also facilitated collaborations among thoracic surgeons, researchers and international societies, fostering the exchange of knowledge and expertise [18, 19].

GENERAL DATA PROTECTION REGULATION COMPLIANT DATA TRANSFER TO ESTS

Organizations can promote responsible data management practices, respect individuals' privacy rights and comply with the requirements set forth by GDPR. An independent data controller, such as a hospital, private clinic or biobank, handles the personal data of individuals who have received treatment within their respective activities. Their main priorities lie in establishing a cooperative framework with the ESTS, providing transparent information to data subjects and ensuring the lawful collection of data. By prioritizing these aspects, the data controller aims to uphold data protection standards and maintain a trustworthy relationship with individuals whose data they process (Table 1).

ESTS, as an independent data controller, plays a crucial role in the management of data by selecting the primary objective of building an international research database and the appropriate tools for this purpose, such as hosting and IT framework. In this process, the organization places significant emphasis on 3 main priorities: pseudonymization, ensuring a secure channel for data transmission and establishing a secure interface for data access. These priorities are essential in safeguarding the privacy and security of the data being managed by ESTS (Table 2).

Data storage is a crucial aspect of ESTS processes, mainly due to the sensitive nature of healthcare data. Organizations have the option to store data internally or outsource it to a reliable data processor. However, to ensure transparency and maintain control over the data, strict regulations should be imposed on the use of additional processors by the primary processor. The primary processor should be prohibited from employing additional processors for its core data storage service. The primary focus in this context is ensuring robust data security measures to safeguard the stored information (Table 3).

The ESTS has specific guidelines for processing stored data. Pseudonymization, which protects individual identities, cannot be undone under any circumstances. If the data are to be used for a purpose other than its original collection or transfer, it must be compatible with the original purpose. ESTS is responsible for appointing a DPO to oversee data protection activities. The DPO is the ESTS Director of the database and is responsible for ensuring that data processing activities within ESTS adhere to the principles of lawfulness, fairness and transparency. The DPO can be contacted for any inquiries or concerns regarding data protection. ESTS has implemented various technical and organizational measures to maintain data integrity and confidentiality.

Access to the ESTS database is strictly controlled and limited to authorized personnel with a legitimate need to access the data. User authentication mechanisms, such as unique usernames and strong passwords, prevent unauthorized access. When dealing with third-party imports, whether from individual units or National societies, ESTS follows a strict vetting process. Before

Table 1: Main requirements of lawful data collection

Institution	Having a research ethics license under the law of that country	Having written permission from the clinical/research site supervisor	Obtaining the support and cooperation of local DPO	Fulfilling the obligation to inform the data subject of GDPR rights	Obtaining the data subject's written statement regarding the data process
Both parties	The requirement to enter the data process into records of processing activities	Complying with procedures in the event of a data breach, data subject request or complaint	Providing a declaration of compliance	Establish a data transfer agreement including the following requirements: • To only send and accept lawfully collected data • To take all organizational and technical measures to ensure the security of data collected for transfer • To transmit data only through a secure channel and interface provided by ESTS	
ESTS	Show commitment to not to use data for any purpose other than that indicated	Provide a dynamic online environment through which data subject can flexibly review what it has agreed to		Protect data throughout the process in a manner proportionate to the risks involved and only handle data in pseudonymized form.	

DPO: Data Protection Officer; ESTS: European Society of Thoracic Surgeons; GDPR: General Data Protection Regulation.

Table 2: Main requirements of lawful data transfer

Institution	The transfer must be indicated on information material and in records of data processes	Data must be submitted using an electronic system provided by ESTS	Transmission should be carried out by designated persons, with limited possibility of substitution
Both parties	Data transferred must not contain any personally identifiable information	Data should be pseudonymized as the first step in the data transfer process to ensure that ESTS only has access to the amount of data strictly necessary to achieve its purpose	
ESTS	The interface must be designed not to accept more data than necessary and requires pseudonymization	Channel used to transmit data should provide a high level of security according to the current state of technology and science. Especially against the following: Interruption, modification, interception, falsification	

ESTS: European Society of Thoracic Surgeons.

Table 3: Main requirements of lawful data storage

ESTS	Data processing agreement under GDPR must include (i) instructions, (ii) cooperation with a controller in the investigation and assessment of data breaches, (iii) actively facilitating the exercise of rights of data subjects by putting in place appropriate organizational and technical measures and (iv) the obligation to tolerate audits carried out by the controller		
Storage provider	Carry out a Data Protection Impact Assessment of its operations and, upon request, contribute to the data controller's own Impact Assessment	The processor must assess whether it needs to appoint a Data Protection Officer and, if so, ensure one is appointed	The processor must establish a risk management system and carry out risk identification and analysis at regular intervals in a verifiable and measurable way
	Processors must implement and maintain all necessary measures to protect data proportionate to risk. Established to an outside observer	Must ensure complete, sealed and continuous information protection for all data (automated and non-automated)	The processor is required to monitor its operating environment and draw conclusions from changes (external and internal circumstances, stakeholder needs)
	The processor must ensure compliance with confidentiality, integrity and availability requirements, including (i) the security of the connection, (ii) protection of the physical environment, (iii) algorithmic and administrative protection of data, (iv) backup and archiving system fit for purpose, (v) establish event control functions and (vi) provide logging facilities and ability to analyse and evaluate data		
	The processor must have the following procedures in place and allocate the following functions within its organization: (i) Data Management and Security Policy, (ii) Business Continuity Protocol, (iii) Disaster Recovery Plan, (iv) Incident Response Plan, (v) Data Loss Prevention mechanics and (vi) while also appointing Chief Information Security Officer and Chief Risk Officer		

GDPR: General Data Protection Regulation; ESTS: European Society of Thoracic Surgeons.

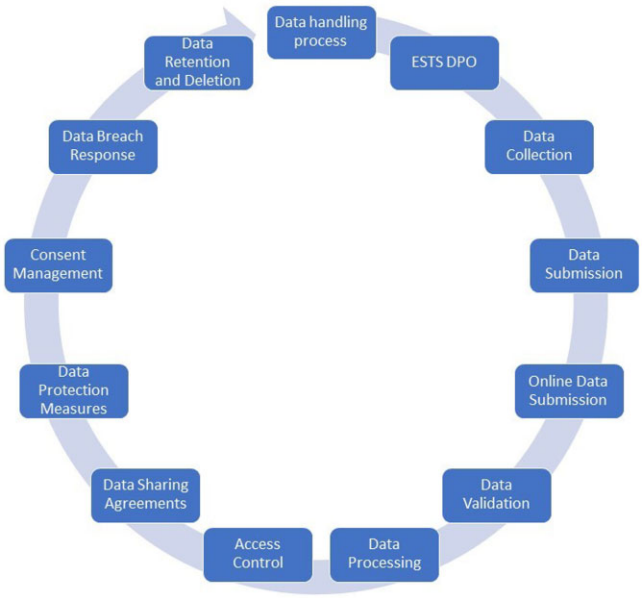


Figure 1: Processes within the ESTS database to adhere to GDPR. The process begins with data handling in the database. ESTS DPO oversees GDPR compliance. Data are collected from various sources, including units and National societies. Requirements for data submission are defined, along with standardized formats. Secure online channels are provided for data submission. Submitted data are validated for accuracy and consistency. Data are processed following the principles of lawfulness, fairness and transparency. Strict access controls limit database access to authorized personnel. Data-sharing agreements are established with third parties, outlining terms and conditions. Measures are implemented to ensure data integrity and confidentiality. Consent management options are provided to individuals. Procedures for handling data breaches and notifying relevant parties are defined. Guidelines for data retention and secure deletion are established. DPO: Data Protection Officer; ESTS: European Society of Thoracic Surgeons; GDPR: General Data Protection Regulation.

importing data, ESTS ensures that appropriate data-sharing agreements are in place with these entities. These agreements outline the terms and conditions for data transfer, specifying the purposes for which the data will be used and the measures to protect data privacy. In the case of individual online data submissions, ESTS employs secure and encrypted channels to ensure the confidentiality and integrity of the data. Data submitted by individuals undergo a validation process to verify its accuracy and consistency.

Additionally, ESTS provides clear instructions to units and societies on the specific data requirements for submission, such as standardized formats and necessary documentation. ESTS takes personal data protection seriously and has implemented a comprehensive framework to comply with GDPR. By appointing a DPO, employing technical and organizational measures, establishing data-sharing agreements and providing clear instructions to units and societies, ESTS aims to maintain the highest standards of data privacy and security (Fig. 1). The summarized data in the ESTS database must also be made available to external parties for scientific research purposes. However, when transmitting data to these external parties, the data must be thoroughly anonymized and presented in aggregated and statistical formats, along with reports. It is important to note that pseudonymized data should not be disclosed to protect individual privacy (Table 3).

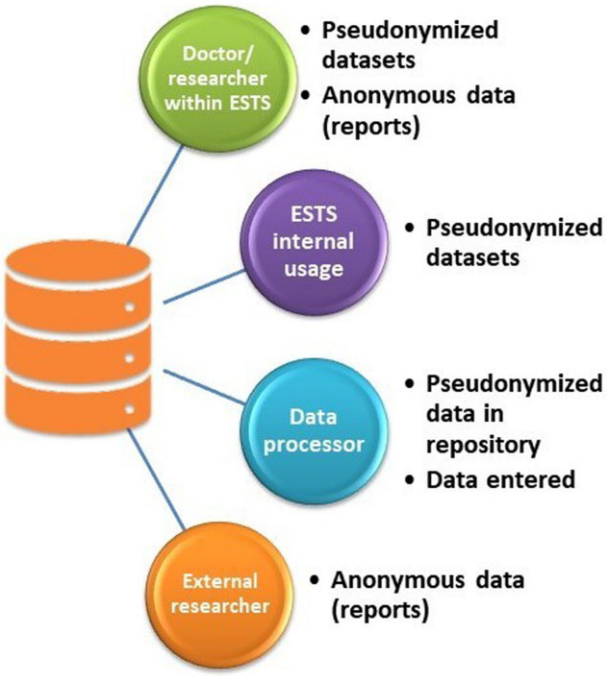


Figure 2: Mapping of (optimal) data access levels. ESTS: European Society of Thoracic Surgeons.

One of the key challenges in achieving GDPR compliance lies in navigating the differences in legislation across various countries. Harmonizing individual legislations under a unified structure, such as an ESTS database, can streamline compliance efforts and ensure consistent adherence to GDPR guidelines. Establishing clear policies and including GDPR template language when appropriate can also contribute to compliance efforts, especially in health research involving sensitive data. Transferring personal data within or between institutions must be undertaken with utmost care and only if necessary for the legitimate performance of tasks falling within the recipient's competence. Joint liability between the sender and recipient is crucial, highlighting the need for open dialogue and cooperation to ensure compliance throughout the data transfer process. By maintaining transparency and accountability, institutions can mitigate the risks associated with data transfers and uphold GDPR standards (Fig. 2).

THE RISK OF THE GENERAL DATA PROTECTION REGULATION PROCESS

There are several risks inherent in the GDPR process. The right to human dignity can be violated when data, particularly health data, are unlawfully or accidentally disclosed. This unauthorized disclosure can lead to the potential for severe violations and compromises of an individual's dignity. The right to personal data protection can be violated when data are unintentionally or unlawfully linked within a database, resulting in data processing that goes against established principles. Ensuring transparency in data processing is crucial and can be effectively achieved primarily at the local level. The violation of the right to physical and mental health can happen through excessive data collection or the perception that disclosing such data are mandatory. This can be especially burdensome for individuals already vulnerable due

to their health condition, impacting their well-being and mental health. Unlawful disclosure of data can occur through security breaches resulting from errors or unlawful attacks. Such breaches can happen during the collection process when authorized users lose control over login credentials or the interface, during data transfer to and from servers and during data storage on servers. These violations highlight the importance of safeguarding personal data, respecting privacy rights and implementing robust security measures to protect individuals' dignity, personal data and physical and mental health [20].

GDPR non-compliance can have significant repercussions, both financially and in terms of brand reputation. Organizations failing to establish a lawful basis for data processing or obtain sufficient consent may face fines of up to €20,000,000 or 4% of their annual revenue, whichever is higher. Additionally, being unable to facilitate individuals' exercise of their rights or failing to maintain proper data records can result in 2% of annual revenue fines. Therefore, organizations must prioritize GDPR compliance to avoid such penalties. Although GDPR compliance presents challenges, it also offers numerous benefits. By adhering to GDPR standards, data contributors and researchers can enhance data security and protect the privacy of individuals in the database [21]. GDPR compliance fosters trust among data subjects, promoting a culture of transparency and respect for privacy. Furthermore, GDPR's emphasis on data protection encourages organizations to establish robust data management policies, leading to more efficient and responsible data handling practices [3].

CONCLUSIONS

In an era where data are increasingly valuable, GDPR-compliant data management is an essential aspect of modern research and data governance. By embracing GDPR principles, organizations can ensure the security of personal information, protect privacy rights and cultivate trust with data subjects. However, achieving GDPR compliance requires a comprehensive understanding of the intricacies involved in data processing, transfer, storage and usage. Researchers and organizations must establish transparent data management policies and adopt best practices to navigate the challenges and reap the benefits of GDPR compliance in an ever-evolving data landscape. The GDPR has introduced a paradigm shift in handling and protecting personal data. Its broad scope, encompassing various forms of data and categories of personal information, along with its stringent principles, emphasizes the importance of safeguarding privacy rights. By adhering to GDPR's regulations, organizations can build trust, enhance their reputation and contribute to a safer and more secure digital environment.

ACKNOWLEDGEMENTS

This work was partially supported by the Italian Ministry of Health with *Ricerca Corrente* and *5x1000* funds.

Conflict of interest: The Authors have no conflict of interest to declare.

DATA AVAILABILITY

No new data were generated or analysed in support of this research.

Author contributions

Luca Bertolaccini: Conceptualization; Data curation; Supervision; Writing—original draft; Writing—review & editing. **Pierre-Emmanuel Falcoz:** Investigation; Methodology; Writing—review & editing. **Alessandro Brunelli:** Writing—original draft; Writing—review & editing. **Hasan Batirel:** Conceptualization; Supervision; Writing—original draft; Writing—review & editing. **Jozsef Furak:** Writing—original draft; Writing—review & editing. **Stefano Passani:** Software; Writing—original draft; Writing—review & editing. **Zalan Szanto:** Supervision; Writing—original draft; Writing—review & editing.

Reviewer information

European Journal of Cardio-Thoracic Surgery thanks the anonymous reviewer(s) for their contribution to the peer review process of this article.

REFERENCES

[1] European Commission. Data protection. European Commission. https://ec.europa.eu/info/law/law-topic/data-protection_en (22 July 2023, date last accessed).
[2] 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). Off J Eur Union 2016;L119:1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[3] GDPR.eu. What is the GDPR? https://gdpr.eu/what-is-gdpr/ (22 July 2023, date last accessed).
[4] Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR). https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (22 July 2023, date last accessed).
[5] European Commission. Special categories of personal data. 2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/special-categories-personal-data_en (22 July 2023, date last accessed).
[6] European Parliament and Council of the European Union. General Data Protection Regulation (GDPR) (No. 2016/679). Off J Eur Union. 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj (22 July 2023, date last accessed).
[7] European Commission. Accuracy and data minimization. 2018. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/accuracy-and-data-minimisation_en (22 July 2023, date last accessed).
[8] European Commission. Security of personal data. 2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/security-personal-data_en (22 July 2023, date last accessed).
[9] European Commission. Rights of individuals. 2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_en (22 July 2023, date last accessed).
[10] European Data Protection Supervisor. Roles and responsibilities. 2021 https://edps.europa.eu/data-protection/our-role-supervisor/role-controller-or-processor/roles-and-responsibilities_en (22 July 2023, date last accessed).
[11] European Commission. Health data. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/specific-processing-situations/health-data_en (22 July 2023, date last accessed).
[12] European Society of Thoracic Surgeons. ESTS Database https://www.ests.org/research/ests-database/ (22 July 2023, date last accessed).
[13] Brunelli A, Cicconi S, Decaluwe H, Szanto Z, Falcoz PE; Database Committee. Parsimonious Eurolung risk models to predict cardiopulmonary morbidity and mortality following anatomic lung resections: an updated analysis from the European Society of Thoracic Surgeons Database. Eur J Cardiothor Surg 2019;57:455–61.
[14] Brunelli A, Rocco G, Szanto Z, Thomas P, Falcoz PE; Database Committee. Morbidity and mortality of lobectomy or pneumonectomy after neoadjuvant treatment: an analysis from the ESTS database. Eur J Cardiothorac Surg 2020;57:740–6.

[15] Begum SSS, Papagiannopoulos K, Falcoz PE, Decaluwe H, Salati M, Brunelli A. Outcome after video-assisted thoracoscopic surgery and open pulmonary lobectomy in patients with low Vo 2 max: a case-matched analysis from the ESTS database. Eur J Cardiothor Surg 2015;494:1054–8.
[16] Brunelli A, Falcoz PE. The European Society of Thoracic Surgeons (ESTS) database: role, content and use. J Thorac Dis 2018;10:S3539–S3541.
[17] Hickey GL, Grant SW, Cosgriff R, Dimarakis I, Pagano D, Kappetein AP *et al.* Clinical registries: governance, management, analysis and applications. Eur J Cardiothorac Surg 2013;44:605–14.
[18] Gooseman MR, Falcoz P-E, Decaluwe H, Szanto Z, Brunelli A; Database Committee. Morbidity and mortality of lung resection candidates defined by the American College of Chest Physicians as 'Moderate Risk': an analysis from the European Society of Thoracic Surgeons Database. Eur J Cardiothorac Surg 2021;60:91–7.
[19] Falcoz PE, Brunelli A, Cerfolio R. European Society of Thoracic Surgeons Database: unlocking the potential of European collaborative thoracic surgical research. Ann Thorac Surg 2021;112:716–9.
[20] GDPR and Human Dignity. European Data Protection Supervisor. https://edps.europa.eu/data-protection/our-work/our-work-topic/health-and-genetic-data_en#governance-of-genetic-data (22 July 2023, date last accessed).
[21] GDPR Compliance. European data protection supervisor. https://edps.europa.eu/data-protection/our-work/our-work-topic/enforcement-and-sanctions_en (22 July 2023, date last accessed).