TÉCNICO LISBOA

Blockchain-based Framework for Health Tourism That Follows the GDPR

Frederico Esteves Torrado de Pessoa Oliveira

Thesis to obtain the Master of Science Degree in

Computer Science and Engineering

Supervisors: Prof. Miguel Leitão Bignolas Mira da Silva

Prof. Paulo José Osório Rupino da Cunha

Examination Committee

Chairperson: Prof. Rui Filipe Fernandes Prada

Supervisor: Prof. Miguel Leitão Bignolas Mira da Silva

Members of the Committee: Prof. Miguel Nuno Dias Alves Pupo Correia

October 2022

Acknowledgements

I hereby express my sincere gratitude to my thesis supervisors and mentors, Professors Miguel Mira da Silva and Paulo Rupino da Cunha, for their persistent guidance and motivation whilst persuasively conveying a spirit of quest and accountability in achieving the desired outcome by decoding all the challenges presented to us throughout the research and scholarship.

I extend my deep appreciation to my colleagues, both at INOV – Instituto de Engenharia de Sistemas e Computadores Inovação and IST – Instituto Superior Técnico da Universidade de Lisboa, for the complicity and an enlightening adventure. May we persevere in sharing the dream in years to come.

On a last and more personal note, I cannot find the words to rightfully thank my family for always being there, no matter the circumstances, in particular my parents, Luís and Cristina, my siblings, Sofia and Francisca, and my grandparents, Carlos and Maria Luísa, the latter whom I may no longer share the moment in this lifetime.

Thank you all.

Abstract

Health tourism has grown significantly over the past few decades, with an estimated 20 to 24 million patients crossing borders each year to receive medical treatments. This emerging sector plays a key role in meeting the sensitive and vital needs and desires of health tourists by providing access to affordable healthcare services. However, the industry faces significant challenges: privacy and transparency concerns, lack of access to centralized health records, fraudulent practices, opportunistic behaviour of intermediaries and contractual/legal issues. While Blockchain technology has great potential to address and solve many of the industry's inherent challenges and inefficiencies, current understanding of its application in health tourism is fragmented. Furthermore, the technology itself has certain limitations and its implementation poses a number of challenges that must be considered when applying it to the health tourism sector, mainly related to regulatory compliance such as the General Data Protection Regulation.

Therefore, the main purpose of this thesis is to develop a GDPR-compliant Blockchain-based framework for healthcare data management, focused on the specific case of health tourism. Our goal is to help researchers and practitioners understand the challenges and requirements for developing GDPR-compliant Blockchain solutions for health tourism practice.

This document studies the practical implications of the GDPR on the development of Blockchain solutions for storing and sharing personal health data, clearly identifies the existing challenges and reviews the solutions proposed in the literature to address them.

Keywords

Blockchain; GDPR; Health Tourism; Personal Data; Health Data; PHR

Resumo

O turismo de saúde e bem-estar cresceu significativamente nas últimas décadas, com cerca de 20 a 24 milhões de pacientes a cruzar fronteiras a cada ano para receber tratamentos médicos. Este setor emergente desempenha um papel fundamental no atendimento das necessidades e desejos dos turistas, fornecendo acesso a serviços de saúde acessíveis. No entanto, o setor enfrenta desafios significativos: preocupações com privacidade e transparência, falta de acesso a registos de saúde centralizados, práticas fraudulentas, comportamento oportunista de intermediários e questões contratuais/legais. Embora a tecnologia Blockchain possua um grande potencial para resolver muitos dos desafios e ineficiências inerentes ao setor, a compreensão atual da sua aplicação no turismo de saúde e bem-estar é fragmentada. Além disso, a própria tecnologia possui certas limitações e sua implementação apresenta um conjunto de desafios que devem ser considerados ao aplicá-la ao setor de turismo de saúde e bem-estar, principalmente relacionados à conformidade regulatória, como o RGPD.

Posto isto, o principal objetivo desta tese é desenvolver uma Blockchain framework para gestão de dados de saúde que cumpre com os requisitos impostos pelo RGPD, focada no turismo de saúde e bem-estar. O nosso objetivo é ajudar investigadores e profissionais a entender os requisitos para desenvolver e implementar soluções Blockchain compatíveis com RGPD para a prática de turismo de saúde e bem-estar.

Este documento estuda as implicações práticas do RGPD no desenvolvimento de soluções Blockchain para armazenamento e partilha de dados pessoais de saúde, identifica claramente os desafios existentes e revê as soluções propostas na literatura para enfrentá-los.

Palavras-chave

Blockchain; RGPD; Turismo de Saúde e Bem-estar; Dados Pessoais; Dados de Saúde; PHR

Contents

List of Figures

List of Tables

Acronyms

DLT Distributed Ledger Technology

EHR Electronic Health Record

GDPR General Data Protection Regulation

MLR Multivocal Literature Review

PHR Personal Health Record

SLR Systematic Literature Review

Chapter 1

1. Introduction

Over the past few decades, health tourism has witnessed significant growth, with an estimated 20 to 24 million patients crossing borders each year to receive medical treatments [1–3]. By health tourism we refer to phenomenon of patients travelling abroad in order to seek or avail medical and allied services and facilities [1]. The health tourism value chain is composed of three main phases: pre-procedure, procedure and post-procedure. Pre-procedure is the first phase of health tourism, which involves preparation by a medical tourist to receive medical service [4]. This phase consists of several important stages, including choice of health travel facilitator, medical providers like hospitals or doctors, and the destination country [1,3,4]. The procedure phase, which is the second phase, begins once the patient reaches the destination country [1]. In this phase, the patient visits the hospital, undertakes required tests and consultations, and undergoes treatment or procedure [3]. The post-procedure phase is the last and involves post-operative care and follow-up care of the medical tourists [1,3,4].

This emerging sector created a new tourist class by combining healthcare services with tourism and hospitality with access to affordable healthcare services [2]. Affordability, accessibility and availability are considered the primary drivers for searching for alternative healthcare and medical intervention options overseas [2]. The scope of health tourism ranges from medical procedures such as minor dental procedures, cosmetic surgery and significant interventions, often referred to as medical tourism, to the organized travel to maintain, enhance or restore the mind and body's wellbeing, which is referred as wellness tourism [1,2].

Although it plays a key role in meeting the sensitive and critical needs and desires of health tourists, there are still uncertainties at all stages of the health tourism process, including pre-procedure and post-procedure [4]. There are significant challenges facing the health tourism industry: privacy and transparency concerns, lack of access to centralized medical records, fraudulent practices, opportunistic behaviour of intermediaries, foreign currency risks, and contractual/legal issues [3].

Blockchain has been receiving increasing interest in recent years and is considered a disruptive technology [5] with the potential to redefine the way information is stored and disseminated, particularly sensitive information, such as personal health data [6]. Blockchain can address and solve many of the challenges and inefficiencies inherent to the health tourism industry [2,3,7]. It offers a

distributed and immutable leger for collecting, storing, and processing data [8,9]. Due to its distributed and immutable nature, Blockchains also enable the transparency, verifiability, and traceability of data stored on-chain [10,11].

However, the same architecture that grants multiple privacy-friendly qualities to Blockchain [11] is also the one that makes it subject to several different issues, mainly compliance with legal regulations [9]. The introduction of the General Data Protection Regulation (GDPR) brought some challenges to the designing and development of Blockchain solutions and changed the way personal data is perceived [12]. This is primarily due to the fact that during its development the GDPR did not consider emerging decentralized technologies, such as Blockchain [8], which resulted in tension between the technology and the regulation [13].

Furthermore, major legal or regulatory changes always had a great impact on social and economic activities, even more today considering the technological advances, rapid innovation and the increase of system's complexity in many fields. Healthcare is no exception, being extremely impacted by such changes. Accordingly, it came as no surprise that the introduction of GDPR caused an immediate impact on businesses and services that involve the processing and storage of personal data, as it is the case of healthcare related activities, such as health tourism.

The GDPR appoints obligations and responsibilities on how organisations collect, store and process personal data, and it requires organisations to be completely transparent with how they use, protect and safeguard that same personal data. In the case of healthcare organisations, this is all the more significant since data concerning health is considered "sensitive data" under the GDPR [14–19], which benefits from additional protection [15] and stricter requirements. According to Article 4, "data concerning health" means 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. In addition, some specific derogations are defined for this type of personal data, aiming at protecting the rights of individuals and the confidentiality of their personal health data, whilst preserving the benefits of processing data [20].

1.1. Research Problem

As discussed above, even though Blockchain is viewed as a technology capable of redefining the way information is stored and disseminated, particularly sensitive information [6], its implementation introduces a significant amount of challenges, encompassing compliance with privacy regulations, privacy issues, and scalability limitations. Thus, the Blockchain must be integrated along with other technologies in order to solve several of these challenges. Further, since compliance with the GDPR must be assessed on a case-by-case basis, there is a need to examine the implications of the regulation on the different types and specific domains of Blockchain applications.

In the particular case of the health tourism industry, some of these concerns become even more increasingly alarming since health data is subject to stricter regulatory, security and legal requirements, a key factor limiting Blockchain adoption in the sector [21]. Although Blockchain technology holds the potential to provide serious improvements for healthcare data management compared with current information management systems, there are inherent issues when integrating traditional Blockchain solutions with healthcare data storage and sharing [21]. That being said, there is a need to assess these specific challenges and the implications of the legal regulations on health data in order to better align Blockchain's capabilities with healthcare data management and, consequently, ease the development of compliant healthcare Blockchain solutions.

1.2. Proposed Solution

To address the identified research problems, we intend to develop a GDPR-compliant Blockchain-based framework for healthcare data management, focused on the specific case of health tourism. The framework will be built on the knowledge gathered from the literature reviews and will serve as support for designing GDPR-compliant blockchain architectures for health tourism. Inside the health tourism domain, we will devote our attention to the fields of medical tourism and wellness tourism.

Our aim with this solution is to provide a widely accepted framework to assist researchers and practitioners in understanding the requirements for developing GDPR-compliant healthcare Blockchain solutions, focused on health tourism. This framework is expected to enable users to own their data and easily share their healthcare data while assuring its privacy and protection, and complying with legal regulations. Moreover, it is meant to tackle existing limitations, such as scalability, and the security and privacy of data stored and transferred.

1.3. Objectives

The objectives to be pursued with this dissertation are:

- To assess existing challenges between Blockchain technology and GDPR, and the review of current techniques and solutions to deal with those same challenges. Thus, we conduct a Systematic Literature Review (SLR) to identify the benefits and challenges of using Blockchain technology to store personal data, and review the current state-of-the-art for implementing GDPR-compliant Blockchain solutions;

- To assess the impact and existing implications of the GDPR on healthcare practice and research in order to clarify researchers, healthcare organisations and other institutions that process or intend to process health data of individuals about their obligations under the

regulation and the measures that they need to take to fulfil them. Another SLR is performed with the goal of identifying the main benefits and challenges of compliance with the GDPR in the healthcare sector, as well as existing derogations from the regulation;

- To assess current developments on the use of Blockchain for the practice of health tourism. This would support researchers and practitioners in better understanding the full potential of blockchain use in health tourism, increase its acceptability and assist in the implementation of solutions. A Multivocal Literature Review (MLR) is carried out to summarize the existing evidence on both the state-of-the-art and practice on the use of blockchain solutions for health tourism;

1.4. Dissertation Structure

The remainder of this document is organized as follows. Chapter 2 describes the applied research methodologies, detailing the distinct phases that comprise each of the research processes. An overview of the main concepts discussed throughout this investigation is provided in Chapter 3. The literature reviews are conducted in Chapters 4, 5 and 6. Chapter 7 explains how the findings of this investigation were communicated to researchers and other relevant audiences. Finally, the last chapter concludes our work and outlines future research directions.

Chapter 2

2. Research Methodology

In this chapter, the research methodologies used to guide the research are described.

2.1. Systematic Literature Review

In this dissertation, two Systematic Literature Reviews (SLR) are conducted following the guidelines and recommendations by [22–24]. A systematic literature review is a means of identifying, evaluating and interpreting all available research relevant to a topic area, or phenomenon of interest. Individual studies contributing to a systematic review are called primary studies while a systematic review is a form a secondary study [23,24]. This research methodology was selected due to its structured search approach, which provides fairness to the work and seeks to eliminate any research bias [23,24]. Moreover, since it is a systematic approach and follows a predefined search strategy, it can be easily replicated.

The research process comprises the planning, conducting, and reporting phases as proposed by [23,24] and depicted in figure 1.

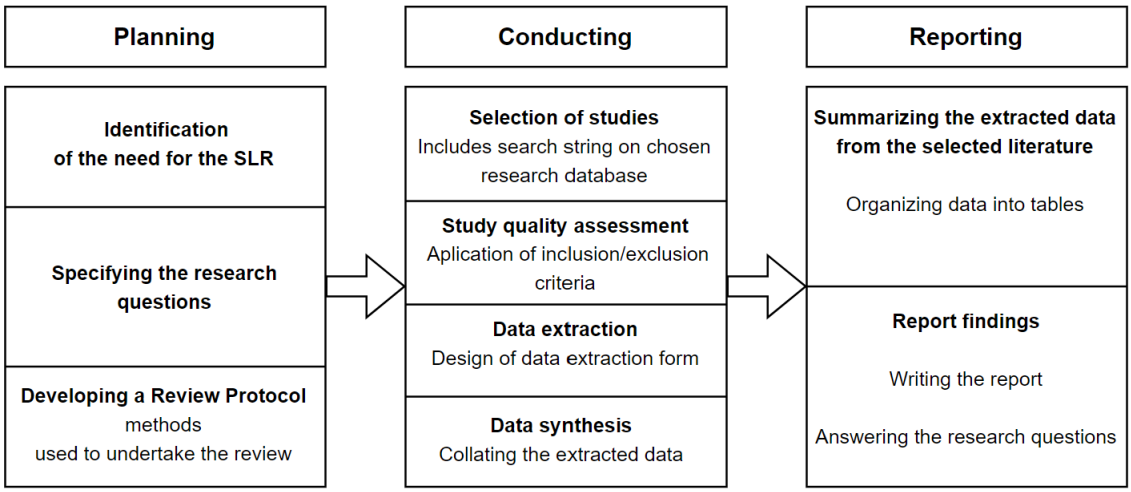

Figure 1 - Systematic Literature Review (SLR) phases

1. The SLR **planning** phase consists of the following 3 stages:

    - Identification of the need for the SLR in the given topic;
    - Specifying the research questions;
    - Developing a review protocol.

2. The SLR **conducting** phase consists of the following 3 stages:

    - **Selection of studies** for undertaking the review;
    - **Study quality assessment** to determine the extent to which a study is valid and free of bias;
    - **Data extraction** from the selected studies through the design of a data extraction form;
    - **Data synthesis** with chosen qualitative and quantitative techniques.

3. The SLR **reporting** phase is a single stage phase:

    - Summarizing the extracted data from the selected literature and report findings by answering the research questions.

2.2. Multivocal Literature Review

A Multivocal Literature Review (MLR) is conducted following the guidelines and recommendations by [25]. A MLR is a form of Systematic Literature Review (SLR) that includes grey literature like blogs, videos, web-pages and white papers, which are constantly produced by SE practitioners outside academic forums, in addition to the published formal literature such as journal articles and conference papers [25]. Therefore, MLRs are important to the expansion of the research by including literature that normally would not be included due to its "grey" nature. As shown in figure 2, an MLR in a given subject field is a union of the sources that would be studied in an SLR and in a Grey Literature Review (GLR) of that field. As the name implies, GLR only consider GL sources in their pool of reviewed sources. As a result, an MLR, in principle, is expected to provide a more complete picture of the evidence as well as the state-of-the-art and practice in a given field than an SLR or a GLR [25].

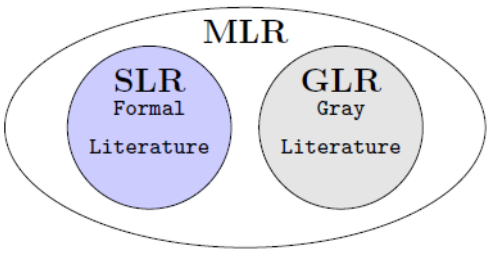

Figure 2 - The relationship of SLR, GLR and MLR studies [25]

When considering conducting a literature review from formal literature in the specific topic of blockchain in health tourism, the author realized that broadening the scope and including grey literature (GL) would add value and benefits to the study as well as close the gap between academic research and professional practice. It is expected that the GL will provide essential knowledge regarding the use of blockchain for professional practice, but the evidence provided is often based on experience and opinion, so it is understandable that including such relevant literature presents particular challenges.

The separation of several types of literature is seen in Table I, where is listed “White” and “Grey” literature sources into 1st tier, with high credibility, and 2nd tier with moderate credibility. For our research, we decided to include 2nd tier in addition to 1st tier, given that there is valuable expertise and knowledge on those sources. It is also necessary to exclude literature that corresponds to ideas, concepts and thoughts, like tweets or emails from the 3rd tier, which have low credibility.

Table I - Spectrum of the "white", "grey" and excluded literature [25]

“White” literature	**“Grey” literature**	**Excluded “Black” literature**
Published journal papers	Preprints	Ideas
Conference proceedings	e-Prints	Concepts
Books	Technical reports	Thoughts
	Lectures	
	Data sets	
	Audio-Video (AV) media	
	Blogs	

There are several guidelines in the literature for conducting SLR studies in SE, e.g., [23,24]. However, several phases of MLRs differ from those of traditional SLRs. In particular, the process of researching and assessing the quality of sources. Therefore, the SLR guidelines are only partially helpful in conducting MLR studies, as shown in Figure 3. The research process comprises the planning, conducting, and reporting phases as proposed by [25].

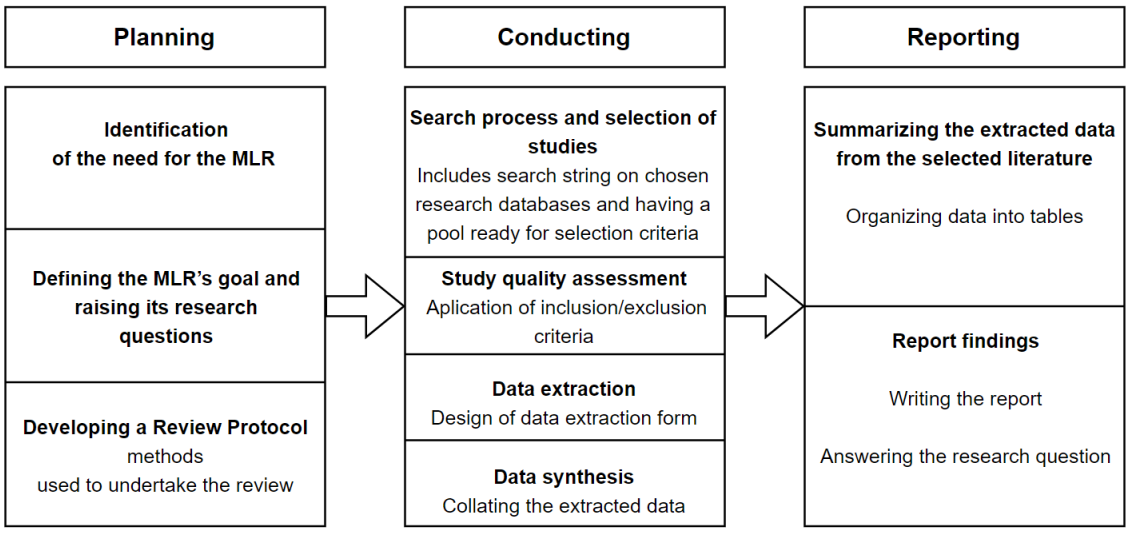

Figure 3 - Multivocal Literature Review (MLR) phases

1. The MLR **planning** phase consists of the following 3 stages:

    - Identification of the need for the MLR in the given topic;
    - Defining the MLR's goal and raising its research questions;
    - Developing a review protocol.

2. The MLR **conducting** phase consists of the following 3 stages:

    - **Search process** for formal or GL is typically done via means of using defined search strings;
    - **Source selection** normally includes determining the selection criteria and performing the selection process;
    - **Study quality assessment** to determine the extent to which a study is valid and free of bias;
    - **Data extraction** from the selected studies through the design of a data extraction form;
    - **Data synthesis** with chosen qualitative and quantitative techniques.

3. The MLR **reporting** phase is a single stage phase:

    - Summarizing the extracted data from the selected literature and report findings by answering the research questions.

Chapter 3

3. Background

In this chapter, relevant background knowledge on Blockchain, GDPR, Electronic Health Records and Personal Health Records is presented.

3.1. Blockchain Technology

The concept of Blockchain was first introduced in [26] as the underlying technology behind Bitcoin, a peer-to-peer electronic cash system. Unlike traditional currencies, which are issued by central banks, Bitcoin has no central authority [27]. Bitcoin is the first cryptocurrency that allows to perform transactions in a secure manner without the need of a trusted third-party, while also solving the double-spending problem. Nevertheless, Bitcoin was just the first of many Blockchain applications [28].

In a nutshell, Blockchain is a synchronized, shared, distributed, append-only database (ledger), that relies on strong consensus algorithms, such as Proof of Work and Proof of Stake, to maintain the peer-to-peer network [27]. Rather than being an entirely new technology, Blockchain is a combination of multiple existing technologies, mainly asymmetric key encryption, hash functions, Merkle trees, and peer-to-peer networks.

The information in Blockchain is stored in blocks that are linked together to form a chain [27]. Blocks consist of two types of data, a block header that contains metadata about the block, and the block content that contains the block's information, for instance a list of the block's transactions. The block's header is composed of the hash root (hash digest of the block's data), the hash value of the previous block (except the genesis block), and a timestamp [27]. Since each block holds the hash value of the previous block, the blocks are cryptographically linked together after undergoing a validation process. As new blocks are added to the Blockchain, older blocks become more difficult to modify. This approach renders the Blockchain tamper-evident and tamper-resistant, lending to the key attribute of immutability [27,28].

As a distributed ledger technology, Blockchain is managed by a peer-to-peer network. In this way, the digital ledger is shared, updated, and replicated within the network, and any conflicts are resolved automatically using established rules [27,28].

Blockchain networks can be categorized based on their permission model. In Permissionless Blockchains, anyone can maintain the network by publishing blocks and participating in the consensus, as in the case of Permissioned Blockchains only particular users are allowed to do it [28]. There are four main types of Blockchain network architectures: Public, Private, Hybrid, and Consortium Blockchains. Public permissionless Blockchains are open for access to anyone and all users can publish and validate blocks without permission from any authority [28]. Private permissioned Blockchains are closed networks, usually owned by an entity or organisation, where only authorized users can participate in the network and perform operations over the distributed ledger. Hybrid Blockchains are a combination of Public and Private Blockchains that allow to control who can access specific information stored on chain and what information will be public. Finally, Consortium Blockchains, also known as Federated Blockchains, are similar to Hybrid Blockchains but instead of being managed by a single entity or organisation, they are managed by a group of organisations and individuals, typically referred to as a consortium [28].

3.2. General Data Protection Regulation

The General Data Protection Regulation (GDPR), which entered into force on 25 May 2018 [19,29], is a legal regulation containing a set of measures designed to enhance privacy and privacy awareness in the European Union (EU) [30,31]. The regulation is described in detail across 99 articles and applies to any entity or organization that processes personal data of EU citizens, regardless of where the data is processed [8]. By appointing higher requirements and obligations on entities who manage and process personal data, the GDPR aims to empower individuals with more control over their personal data [30,32–37].

According to Article 4 of the GDPR, “personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors”, i.e., personal data is any information that can, directly or indirectly, be associated with a natural person.

The GDPR clearly differentiates three roles and specifies their associated rights and obligations under the EU law [30]. Data Subject is an identified or identifiable natural person whose personal data refers to. Data Controller is defined as “the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data”. On the other hand, Data Processor is defined as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” (Article 4 of the GDPR).

The means by which personal data should be protected are defined in the GDPR on a set of core data processing principles: Lawfulness, Fairness, and Transparency. Data subjects should be aware of the

processing purposes and provided with proper notification and information regarding its scope; Purpose Limitation. Personal data should be used for specific and well-defined purposes; Data Minimization. Personal data should only be collected for processing purposes and redundant data should not be collected; Storage Limitation. Personal data should be stored no longer than necessary; Accuracy of data records; Integrity; and Confidentiality [11,30].

Furthermore, the GDPR lays out a variety of rights aiming at providing the Data Subjects with more control over their personal data [8,30], primarily the right to be informed (Article 13), right of access (Article 15), right to rectification (Article 16), right to erasure (Article 17), and right to data portability (Article 20).

3.3. Electronic Health Records

According to ISO/TR 14639, the electronic health record (EHR) is “information relevant to the wellness, health, and healthcare of an individual, in computer processable form and represented according to a standardized information model”. EHRs is a digital collection of patients’ medical data [38]. EHRs store a patient’s demographics, medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results [39]. EHRs are operated by healthcare organizations and data are entered by physicians. Patients cannot access or control their own medical records. Its purpose is to collect data from healthcare professionals and facilitate electronic collaboration and information sharing between healthcare organizations, whereas patients are merely passive actors [39].

EHRs enable the integration of data between healthcare providers, facilitate and increase access to patients’ data, reduce medical errors and their associated costs and losses, and consequently improve disease management quality of care [39]. However, the main limitation of EHR systems is related to interoperability [39].

3.4. Personal Health Records

Personal health records (PHRs) are a form of electronic health records (EHRs) [40]. Unlike EHRs, PHRs allow patients to manage and access their own medical data [38–42]. The fact that the patient is responsible for maintaining the data is seen as a key advantage over the EHR [39]. Also, PHRs allow to integrate data about a patient’s lifestyle and wellness, as well as data withdrawn from various sensors that monitor their health state [39]. In sum, PHRs’ provide a comprehensive overview of the patient’s medical history, containing data entered by the patient, lab results, as well as data from

devices such as wearables sensors or collected from a smartphone [38,39,42]. Benefits of PHR include patient empowerment leading to improved outcomes and reduced healthcare costs [40].

Chapter 4

4. Implementing GDPR-compliant Blockchain Solutions: A Systematic Literature Review

In this chapter, a Systematic Literature Review (SLR) is conducted to identify the benefits and challenges of using Blockchain technology to store personal data, and review the current state of the art for implementing GDPR-compliant Blockchain solutions.

4.1. Planning

This section corresponds to the first phase of the abovementioned SLR process. It begins by stating the underlying motivation behind this work, followed by the specification of the developed research questions that guided the review, and ending with the description of the review protocol.

4.1.1. Motivation and Related Work

Over the last few decades, we have been experiencing a digital revolution, which has resulted in the exponential growth of digital information, including personal data. As the amount of available information grows, the challenge of managing that same information is becoming increasingly difficult, sometimes exposing the information to a variety of privacy and security risks. Therefore, the need to collect, store, and process information in a way that assures its privacy and protection has become increasingly important, especially when dealing with personal information.

Blockchain is portrayed as a disruptive technology with the potential to revolutionize the way information is stored and disseminated, particularly sensitive information, such as personal data [6]. However, due to its rapid development, Blockchain technology is subject to different issues, mainly compliance with legal regulations [9]. The introduction of the General Data Protection Regulation (GDPR) brought some challenges to the designing and development of Blockchain solutions and changed the way personal data is perceived [12].

With the goal of summarizing existing evidence and identifying any gaps in the literature for advancing knowledge on the topic, a Systematic Literature Review (SLR) is performed where the main benefits and challenges of using Blockchain technology for storing personal data are identified and categorized, and a review of the existing techniques and solutions proposed in the literature to address those challenges is conducted.

Prior to undertaking the SLR, two other existing systematic reviews on the topic were identified and examined. This allowed us to acquire a deeper understanding on the subject, since systematic reviews are considered the highest level of evidence [23,24], and to identify any existing gaps in the literature that should be addressed in our work. [9] performs a systematic review of state-of-the-art privacy-preserving solutions and mechanisms in Blockchain, as well as the associated privacy challenges. However, it mainly focuses on the privacy-preserving technologies related with data security and only covers the compliance with legal regulations to a certain extent. On the other hand, [8] offers a very comprehensive work on the topic, covering the most crucial GDPR requirements and obligations and its implications on Blockchain. Additionally, it provides a framework that identifies the strategies and tactics necessary to design GDPR-compliant Blockchain solutions. Still, the article presents some constraints that may result in omitting important evidence on the subject. Unlike this work, it only focuses on permissionless Blockchains and does not consider domain-specific ones. Moreover, it only mentions Blockchain GDPR-related challenges and does not cover other existing issues concerning the implementation of Blockchain solutions. Nonetheless, both systematic reviews were extremely well conducted and provided a great deal of evidence on the topic, and so they were included in the SLR.

4.1.2. Research Questions

Based on the main purposes of this research, the following three research questions were formulated to guide the review:

- **RQ1.** What are the main benefits and challenges of using Blockchain technology for storing personal data?
- **RQ2.** What are the main challenges when implementing GDPR-compliant Blockchain technology?
- **RQ3.** What is the current state-of-the-art for implementing GDPR-compliant Blockchain solutions?
    - What concepts, methods, and techniques are proposed in the literature to address the challenges of implementing GDPR-compliant Blockchain solutions?
    - What set of good practices and guidelines should Blockchain developers and architects adopt in order to build GDPR-compliant Blockchain solutions?

4.1.3. Review Protocol

To address the research questions, a review protocol was delineated, specifying the methods used to undertake the review. The review protocol used in this research is illustrated in figure 4. The goal is to identify and map the studies which are relevant to the research topic and that may provide answers to the proposed research questions. With that in mind, a paper search was conducted in the third and fourth weeks of October 2021. The search string and the chosen research database to perform the search are listed below:

- Search string: (blockchain OR dlt) AND (gdpr OR "data privacy" OR "data protection") AND (concept* OR method* OR model OR framework)

- Research database: EBSCO

The EBSCO research database was selected due to its wide coverage, and the search expression presented above was used to search the database in the abstract field of the articles. At first, the keywords “blockchain” and “dlt” (distributed ledger technology) were combined with “gdpr”, "data privacy", and "data protection", which are directly derived from the scope of our research. However, to narrow the search and find the most relevant studies to the review, the keywords “concept*”, “method*”, “model”, and “framework” were included in the search string.

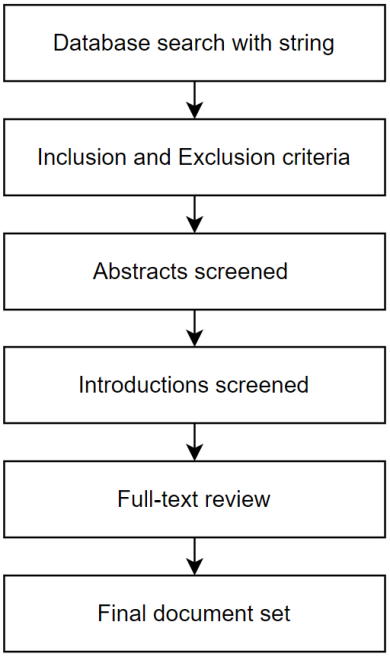

Figure 4 - Review protocol

After performing the database search with the search string, the first set of papers was obtained, and the inclusion and exclusion criteria was applied to refine the search results. The inclusion and exclusion criteria applied can be observed in table II. The selected studies must be academic journals or conference materials, which should assure a certain quality of the papers, written in the English language, with accessibility to the full text, and should be related to Blockchain and GDPR, data privacy, or data protection. Studies that failed to fulfil any of these requirements were discarded. No specific starting publication date was defined to constrain the database search, although it was expected that no paper prior to 2016 would be found, when the GDPR was originally published.

Table II - Inclusion and Exclusion criteria applied in the search

Inclusion criteria	**Exclusion criteria**
Written in English	Not written in English
Full text accessible	Full-text not accessible
Academic journals and conference materials	Not academic journals or conference materials
Mentions both Blockchain and GDPR	Does not mention Blockchain
Describes or implements a solution	Does not mention GDPR, data privacy, or data protection

Once the inclusion and exclusion criteria were applied, the abstracts, introductions, and full texts were screened in order to narrow down the results and obtain the final set of studies to conduct the review. In each of these stages, the inclusion and exclusion criteria were taken into consideration and the papers were classified as “Included”, “Excluded”, or “Maybe”, according to their relevance for the research. Papers classified as “Included” or “Maybe” proceeded to the next stage, whether papers marked as “Excluded” did not.

4.2. Conducting

This section corresponds to the second phase of the SLR process, in which it will be described how the review was conducted. It begins by describing the selection of studies procedure in detail, followed by detailing the data extraction process, and concludes with an analysis of the extracted data.

4.2.1. Selection of Studies

A complete summary of the search process performed in order to identify the most relevant studies for the review can be observed in figure 5.

The first step consisted of searching the EBSCO database with the search string. The search was constrained to look for the keywords in the abstract field and limited to academic journals and conference materials, in accordance with the defined inclusion and exclusion criteria. A total of 432 results were obtained at this stage. After removing the duplicates, the set was reduced to 285 results. The 285 abstracts were screened and, from those, 212 papers were excluded, 28 were classified as “Maybe”, and 45 were included. Next, the introductions of the remaining 73 papers were read. In the end, 37 papers were excluded, 22 were classified as “Maybe”, and 13 were included. The final stage involved reading the full text of 35 papers. In this stage, all papers were included and, consequently, were selected for performing the review.

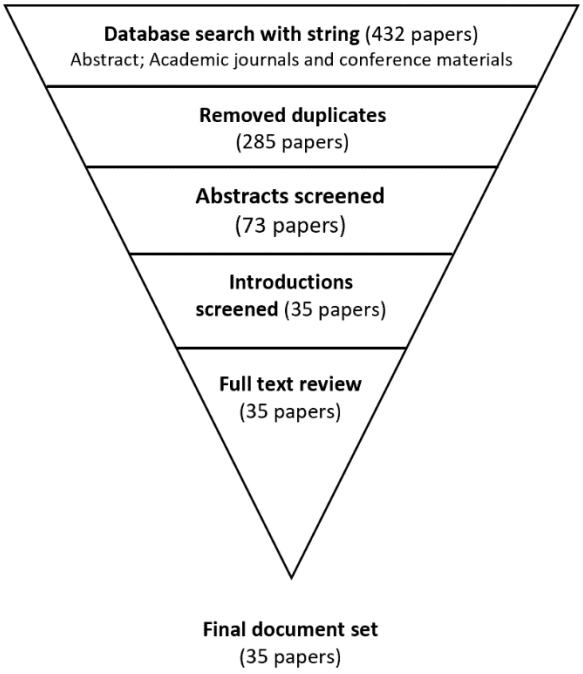

Figure 5 - Selection of studies process

4.2.2. Data Extraction

To facilitate the data extraction process, a form to collect all the required information concerning the research questions was designed following the guidelines from [23,24]. The form consists of the following items:

- Paper ID
- Author(s)
- Year of publication
- Title of paper
- Type of publication
- Publisher
- Journal
- Study design
- Domain
- Keywords
- Research question 1
- Research question 2
- Research question 3
- Additional findings
- Notes

4.2.3. Data Synthesis

In this section, an analysis of the data extracted from the 35 selected studies is presented. An overview of the number of publications over the years, type, and domains among the selected publications is provided.

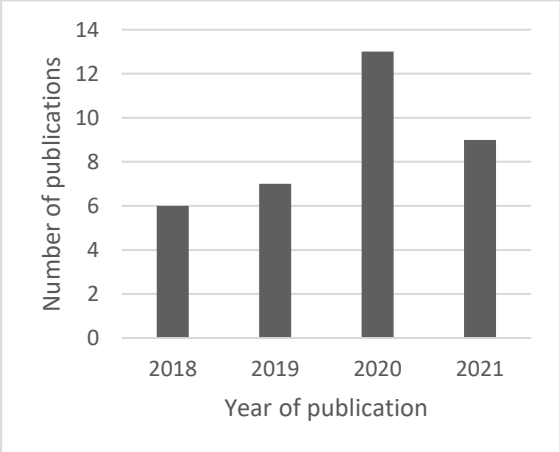

Figure 7 - Number of publications over the years

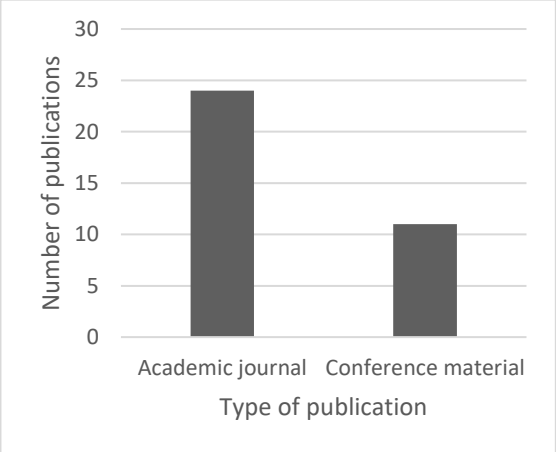

Figure 6 - Type of publications

Looking at figure 6, we can observe the number of publications over the years among the selected studies. As expected, no paper prior to 2016 was selected. In fact, the first publications from this set trace back to 2018, when the GDPR was implemented.

It is interesting to point out the continuous growth of the selected papers over the years, which shows an increasing interest in the research topic. The slightly lower number of papers in 2021 compared to the previous year can be justified due to the time the search was conducted. As previously mentioned, the database search occurred in October 2021, which renders 2021 an incomplete year.

Regarding the type of publication, we can notice that, from the final set of documents, 24 correspond to academic journals while the remaining 11 are conference materials, as shown in figure 7. Additionally, resorting to the information collected in the data extraction form, we perceived that the most common domains among the selected studies are healthcare and law, although the majority of the papers focus on general Blockchains rather than domain-specific ones.

4.3. Reporting

In this section of the SLR, all three research questions are addressed in light of the studies obtained using the review protocol.

4.3.1. RQ1 – What are the main benefits and challenges of using Blockchain technology for storing personal data?

Table III displays the different benefits of using Blockchain technology for storing personal data reported in the literature. The table includes a list of the benefits, the number of publications in which they have been mentioned, and their respective references.

The analysis revealed that the immutability of records stored on-chain is considered one of the main benefits of using Blockchain for storing personal data, being mentioned in 18 of the 35 reviewed papers. Immutability of records is indeed one of Blockchains' most herald features and several authors even consider it its core value proposition. It lies in the premise that, once validated by the nodes, all data stored in the Blockchain can no longer be modified or deleted [5]. This quality is achieved through the use of timestamps and cryptographic mechanisms. Each block in a Blockchain is timestamped and linked to the previous block through hashing techniques in order to form a chain of connected blocks. Since each block contains the hash value from the previous block's header, any attempt to tamper or forge data in a particular block in the chain will be evident, as the hash of its data will no longer match the hash value included in the next block, thus breaking the chain [6,8,13,30,31,43–47]. This

architecture, therefore, ensures that Blockchains are tamper-proof and tamper-evident, which is mentioned as a quality in 13 publications, lending to the key attribute of immutability.

Furthermore, these properties provide a set of other privacy-friendly qualities, such as accountability, verifiability, traceability, integrity, and data provenance [5,9,11,43,47]. According to [9], the integrity of the chain can be verified by computing all the hashes from the genesis block to the last block and compare them to the respective hash pointers. The chain is said to be altered if any hash pointer differs from the one computed. Also, the fact that the records are immutable, and the blocks are stored in a chronological order, makes the audits more feasible [47,48].

The distributed nature of Blockchain technology is another significant benefit, as mentioned in 9 papers. As a distributed ledger technology, Blockchain is managed by a peer-to-peer network, where all information stored on-chain is shared, updated, and replicated among network participants in near real time [6,8,9]. In this way, every participating node on the Blockchain has a duplicate copy of the ledger, trustable, and non-repudiable, that can be used to confirm the veracity of contained information [12]. The distributed nature of Blockchain, thus, promotes transparency of records and establishes trust among the nodes [10]. Additionally, it ensures fault tolerance, absence of single point of failure, and resistance to attacks [45], providing enhanced security and reliability of the system.

Besides being a distributed database, most Blockchains are also decentralized, meaning that the system does not need to rely on a trusted third-party for collection, storage, and processing of data [13,49,50]. By eliminating this need of a centralized authority to manage the data, the data subjects are presented with more control over their personal data [11].

Trust, which is considered by 11 papers as an advantage, is achieved through means of strong consensus algorithms, such as proof-of-work or proof-of-stake. These are used to ensure security through an agreement on the state of the Blockchain. The consensus algorithms are run by the network and can be verified by any node, shifting the trust from a traditional central authority to a distributed verification [9].

Two other important benefits of Blockchain technology are the security and authenticity of data, which are mentioned in 17 and 7 publications, respectively. The system relies on public-key cryptography to assure the security of records, which guarantees protection for the data entered in the chain [5,47]. Public-key cryptography is used to generate digital signatures, which prove the identity of peers that send data to the chain, ensuring the authenticity of data [5,11,13].

Another feature of Blockchain technology is anonymity, mentioned as a quality in 3 papers. [31] state that while everyone is allowed to participate in the network (assuming that the blockchain is permissionless) without having to link their accounts to their real identities, the account identifiers are visible to other users in the network, which renders the Blockchain pseudo-anonymous.

Table III - Benefits of using Blockchain technology for storing personal data

Benefit	Reference	Total
Immutability	[8,9,11–13,21,30,43,45,47,48,50–56]	18
No third-party	[5,6,8,9,11–13,30,31,45,48–51,53,56–58]	18
Security	[5,6,8,10,12,21,31,43,45,48,49,51,53,56–59]	17
Transparency	[6,9–11,21,30,31,43–45,47,56,59,60]	14
Tamper-proof/ resistant/evident	[6,8,11,13,30,31,43,44,46,52,54,56,61]	13
Decentralization	[6,8,9,11,13,30,45,47,50,53,54,56]	12
Traceability	[5,9,11,12,30,43,44,47,51,54,58,61]	12
Integrity	[5,6,8,11,44,47,48,50,52,59,62]	11
Trust	[6,9,10,12,21,44,45,48,55,56,61]	11
Data sharing	[6,10,13,21,51,53,55,58,59]	9
Distributed	[6,12,30,31,48,51,55,56,58]	9
Authenticity	[5,6,10,13,44,45,52,58]	8
Data availability	[12,21,45,48,50,57]	6
Reliability	[6,12,44,48,55,57]	6
Accountability	[9,11,44,54,59]	5
Privacy	[21,44,45,48,53]	5
Replication	[6,8,9,12,55]	5
Data provenance	[9,11,30,62]	4
Interoperability	[11,12,51,59]	4
Timestamping	[5,6,8,56]	4
Anonymity/Pseudo-anonymity	[30,31,58]	3
Reduced costs	[10,12,31]	3
Verifiability	[9–11]	3
Access control	[11,58]	2
Confidentiality	[6,50]	2
Data standardization	[21,59]	2

Although using Blockchain technology for storing personal data brings several advantages compared to other conventional methods of storing information, it also introduces some challenges. Table IV displays the various challenges of using Blockchain technology for storing personal data reported in the reviewed papers.

The analysis revealed that the prevailing challenge of using Blockchain technology for storing personal data is achieving regulatory compliance, in particular GDPR compliance, as mentioned in 19 of the 35 reviewed papers. In addition, several of the remaining identified challenges in the literature relate to

the GDPR in a direct or indirect way. The challenges related to regulatory compliance will be addressed in detail in *section 4.3.2*.

The next most cited is immutability/irreversibility, mentioned in 14 papers. Despite being considered key features of the Blockchain technology, the immutability and tamper-proofness present disadvantages for Blockchain, when it is used in areas where the modification or deletion of data is demanded [43].

Other important challenges mentioned in the literature comprise problems of scalability and storage of data. Blockchain systems tend to face problems when managing large data sets, mainly due to the limited size of blocks on a blockchain, making it difficult to store more complex data other than state of data, transaction history, registry entries, and hashes on a block [21,44].

Blockchains are also subject to security issues, such as transaction linkability [9]. Even though the data stored on the blockchain is encrypted using public-key cryptography, analysing transaction relationships, patterns, time and links is still possible [10].

Privacy issues are yet another reason of concern when storing personal data on Blockchain, as mentioned in 9 papers. According to [10], the availability of transaction information and data contents at all participating nodes introduces a risk of privacy breach of the user involved in a transaction. Additionally, since all transactions must be validated and processed by the majority of the nodes in the network, all the necessary information to perform this processing must be public, potentially in detriment of the confidentiality of the information [47]. Moreover, it is important to notice that Blockchain networks are not completely anonymous and, when a transaction is broadcasted to the verifying nodes, the IP address of the node gets prone to leakage [10].

Table IV - Challenges of using Blockchain technology for storing personal data

Challenge	**Reference**	**Total**
Regulatory compliance	[5,8,9,12,13,31,43–47,49,50,52–54,60,63,64]	19
Immutability/ Irreversibility	[5,9,10,31,43–45,47,52–54,60,63,64]	14
Privacy	[5,9,10,12,13,44,50,51,62]	9
Scalability	[9–11,21,44,47]	6
Security	[9–11,51]	4
Data storage	[21,44,63]	3
Transparency	[10,31,46]	3
Access control	[21,47]	2
Confidentiality	[47,62]	2
Tamper-proof	[31,43]	2
Transaction likability	[9,10]	2
Resource consumption	[52]	1

4.3.2. RQ2 – What are the main challenges when implementing GDPR-compliant Blockchain technology?

As stated in the previous section, the prevailing challenge of using Blockchain technology for storing personal data among the reviewed papers is achieving regulatory compliance, in particular GDPR compliance. Having said that, in this section, the challenges concerning GDPR compliance will be addressed in detail. Table V lists the most important challenges when implementing GDPR-compliant Blockchain technology reported in the literature.

The most cited challenge in the literature is the immutability of records in Blockchain versus the GDPR right to erasure (Article 17), also called “right to be forgotten”, which is mentioned in 18 of the 35 reviewed papers. This article states that the data subject may withdraw the consent on which the processing is based and has the right to obtain from the controller the erasure of his/her personal data without undue delay. Furthermore, the controllers are obligated to delete the personal data of data subjects when it is no longer necessary for the purposes it was collected or otherwise processed, or if it has been unlawfully processed. [11–13]. This requirement is in direct conflict with the immutability feature of Blockchain, which makes it difficult to modify or delete data entered in the Blockchain [5,8,31,44].

The right to rectification (Article 16 of the GDPR) presents another challenge for the implementation of GDPR-compliant Blockchain technology, as mentioned in 13 papers. The GDPR protects false or inaccurate personal data [5] and provides data subjects with the right to request for its rectification [12]. This requirement collides, again, with the immutable nature of records in Blockchain. [5] argue that it is possible to amend incorrect personal data by introducing a new block in the chain with the correct data, however, this procedure does not change the previous blocks, meaning that the incorrect information remains in the old blocks of the chain.

Due to the reasons aforementioned, Blockchain technology also clashes with the principles of purpose limitation, data minimization, and storage limitation [5,8,13].

Another issue revolving Blockchain’s compliance with the GDPR is the identification of the data controller and data processors as well as defining their responsibilities and obligations. The GDPR defines a data controller as any natural or legal person that “determines the purposes and means of the processing of personal data” [13,54]. Due to the decentralized architecture of Blockchain, it is difficult to ascertain who is responsible and, therefore, accountable for the storage and processing of information [5,9,31,49,54]. In fact, the more decentralized the Blockchain’s governance, the more challenging it is to determine who the data controller is [49]. Having said that, public Blockchains, in particular, create the greatest GDPR compliance challenges.

According to Article 4 of the GDPR,” personal data means any information relating to an identified or identifiable natural person” [11]. On the other hand, data that is rendered completely anonymous does not qualify as personal data, falling outside of the scope of the GDPR [13,49]. In the context of

Blockchain, the data stored is usually either encrypted or hashed which, under the EU law, cannot be considered anonymous data, thus qualifying as personal data for the purposes of the legal framework [8,9,13,49,54].

In terms of the Article 22 of the GDPR, which deals with automated individual decision-making and states that the data subject has the right "not to be subject to a decision based solely on automated processing", the challenge can be attributed to Blockchain applications, such as smart contracts, which run automatically and provide an entirely autonomous mode of operation [5,60].

The right to access to personal data is indicated as a challenge in 3 publications. According to Article 15 of the GDPR, the data subject can request a copy of all their personal data and inquire about the purpose of the collection and processing of their data [8]. This requirement can be difficult to satisfy since the decentralized architecture of the Blockchain, in the case of the public Blockchains, does not permit any data subject to enforce their rights, as there is no data controller to whom any privacy request can be sent [5,49]. Moreover, the data on the Blockchain is encrypted or hashed, so the controllers would not know which document's data is stored or processed on the Blockchain [8].

Other important aspects to be considered comprise the right to data portability (Article 20 of the GDPR), which states that the data subject has the right to receive its personal data in a structured, commonly used and machine-readable format [49], the confidentiality principle, since data are publicly available to every Blockchain participant [5,31], and the territorial scope, which raises compliance issues due to the transnational nature of Blockchain [8,13].

Table V – Challenges when implementing GDPR-compliant Blockchain technology

Challenge	**Reference**	**Total**
Erasure	[5,8,9,12,13,31,43–47,49,52–54,60,63,64]	18
Rectification	[5,8,9,12,13,43–45,47,49,53,63,64]	13
Identifying data controller/processors	[5,8,9,13,31,46,47,49,54,60]	10
Anonymization of personal data	[5,8,9,13,44,47,49,54,62]	9
Data minimization	[5,8,13,46,52]	5
Accountability	[5,49,63,64]	4
Confidentiality	[5,31,47,63]	4
Purpose limitation	[5,47,49,63]	4
Access to personal data	[8,13,49]	3
Territorial scope	[8,13,60]	3
Automated data processing	[5,60]	2
Defining	[9,49]	2

responsibilities/ obligations		
Data portability	[49]	1
Transparency of data collection and processing	[12]	1

4.3.3. RQ3 – What is the current state-of-the-art for implementing GDPR-compliant Blockchain solutions?

In this section, the current state-of-the-art for implementing GDPR-compliant Blockchain solutions will be assessed. Table VI outlines the different techniques suggested by the research community to address the aforementioned challenges of implementing GDPR-compliant Blockchain solutions.

To solve most of the identified challenges, the general consensus among the authors is to adopt a hybrid data storage method for Blockchain solutions, leveraging both on-chain and off-chain storage capabilities, where data classified as personal data is encrypted and stored off-chain. The personal data is linked to the distributed ledger through a hash pointer, which contains the information required to access the personal data in the separate database, such as the storage address [11,53,57,60]. In this way, it is possible to comply with GDPR requirements, such as the right to rectification (Article 16) and the right to erasure (Article 17), since the off-chain data can be modified, rectified, and deleted at any time [11,53,64], while still taking advantage of the property of data trustworthiness provided by the distributed ledger, as it is possible to verify the data integrity and provenance due to the hash value stored on-chain [45]. Moreover, storing personal data off-chain improves scalability, reduces storage requirements, and enhances privacy [21].

A different approach is carried out by [10,12,46,52,59,65], that opt to store personal data directly on the Blockchain.

Other solutions indicated in the literature to address challenges resulting from the immutable nature of records in the Blockchain are destroying the encryption key, mentioned in 7 papers, and the use of chameleon hash functions, mentioned in 3 papers. The former consists of destroying the private key by which the data has been encrypted, deeming it inaccessible [8,12,13,31]. This technique lies in the premise that the GDPR does not “specify what constitutes erasure” and states that “some encryption techniques, coupled with [private] key destruction” could potentially be considered erasure [49]. The latter involves the use of chameleon hash functions in order to make the Blockchain redactable. Chameleon hashes “allow determining hash collisions efficiently, given a secret trapdoor information” [31], which maintains the state of the Blockchain consistent after a modification is made [43]. This

technique, however, does not extend to public Blockchains since it requires a secret key holder, who can be a miner, a centralized authority, or several trusted authorities sharing the secret chameleon trapdoor key [31].

[43] proposes a method relying on the use of truncated hash values for modification of transactions. Upon request, the proposed method allows the modification of transactions by making truncated hash values of modified versions equal to the original hash values of the block.

Smart contracts, which consist of a self-executing script containing an agreement or set of rules governing the transactions, are deployed in the Blockchain for access control management [11] and to facilitate, verify, and enforce the consent of the data owners [47,64].

To facilitate the identification of the data controller and, consequently, the entity responsible and accountable for the rights delineated in the GDPR, [5] proposes the implementation of a centralized sidechain that would manage and exercise control over the Blockchain architecture, determining "the purposes and means of the processing of personal data", according to the GDPR.

To address the privacy concerns regarding Blockchain, privacy techniques, such as stealth addresses, ring signatures, zero-knowledge proof, and adding noise to data, have been suggested in [8,13,55]. [10] also proposes limiting the number of nodes that a transaction is broadcast to for verification, resulting in reduction of computation overhead of the network and improved scalability. Additionally, by changing the selected nodes for verification in each transaction, the possibility of network listening and deanonymization of users decreases.

It is important to notice that the majority of the solutions stated in the reviewed papers are built upon private/permissioned or consortium Blockchains, which facilitates the compliance with Article 5 of the GDPR.

Table VI – State-of-the-art for implementing GDPR-compliant Blockchain solutions

Solution	**Reference**	**Total**
Off-chain storage	[8,9,11,13,21,30,31,44,45,47,50–58,60–62,64,66,67]	25
Smart contract	[5,8,11,13,30,47,50,51,56,61,64,67]	12
Destroying the encryption key	[8,12,13,31,45,49,54]	7
Personal data on-chain	[10,12,46,48,52,59]	6
Chameleon hash	[8,13,31]	3
Centralized sidechain	[5]	1
Truncated hash	[43]	1

Besides the solutions and techniques previously mentioned, the literature provides a set of good practices and guidelines that Blockchain developers and architects should adopt in order to build GDPR-compliant Blockchain solutions.

The GDPR states in its principles and various Articles that the concepts of privacy-by-default and privacy-by-design, data minimization, transparency, pseudonymization, encryption and other privacy-enhancing tools should be applied when designing Blockchain solutions [8,11,13,31,47,63].

With this in mind, to be truly compliant with the GDPR, Blockchain developers and architects must, from the beginning, account for the GDPR's requirements and obligations [13,54]. The impact of data protection must be assessed, defining what information needs to be collected, stored, and processed [8,47].

Concerning the identification of the data controller, [49,68] state that the data controller should be designated prior to the implementation of the solution. A potential solution consists in creating a legal person to be considered the accountable entity [49].

The use of smart contracts involving personal data is encouraged by authors since it could be beneficial for ensuring protection for the data subject and the data controller's compliance with the GDPR informed consent requirements [5]. The smart contract should be implemented containing the terms and conditions for the collection, storage and processing of the data subject's personal information as well as its consent [47,64]. In addition, smart contracts can also be adopted for smart consent forms, which enable both data subject and data controller to keep track of data processing and related compliance in real-time. This would render the data subject with more control over their personal data and privacy [5].

4.4. Discussion and Implications

The SLR revealed that there is a growing interest in the use of Blockchain technology for personal data storing and processing purposes. Its distributed and immutable nature allows it to be applied to a wide variety of areas, including finance, healthcare, or to connected environments, such as the Internet of Things (IoT) ecosystem. Indeed, healthcare is one of the most addressed fields among the reviewed papers, where the application of Blockchain technology can enable transparent and fast access to personal healthcare data, promote data standardization, and enhance transfer and sharing of healthcare data [21].

Although Blockchain is regarded as a promising technology for areas that deal with sensitive information, its implementation raises a significant amount of challenges. The majority of reviewed papers identified the benefits and challenges of using Blockchain solutions for storing personal data, while others simply reported having developed and implemented a specific Blockchain solution.

On the one hand, a great deal of studies concludes that using Blockchain solutions for storing personal data has clear advantages compared to other conventional methods of storing information due to its privacy and security features. On the other hand, the use of Blockchain introduces some concerns, mainly compliance with legal regulations, privacy issues, and scalability limitations.

As privacy became a substantial public concern, it is crucial that privacy regulations, such as the GDPR, are considered when designing new applications. The GDPR, however, did not take emerging decentralized technologies into account during its development [8], which resulted in tension between Blockchain technology and the regulation [13]. The literature identifies the conflicts between Blockchain's immutable records and the GDPR's right to rectification (Article 16) and right to erasure (Article 17) as the most alarming concerns when developing Blockchain applications. Although deemed by many authors as its core value proposition, this immutability presents disadvantages for Blockchain technology when used in areas where the modification and deletion of data is demanded, and it is the reason several sectors are yet to completely embrace this new technology [43]. It is important to notice, however, that even though it is very difficult to amend blockchains, it is not impossible [13]. Other important challenges comprise the anonymization of personal data and the identification of the data controller and data processors. The latter is especially worrisome when dealing with public Blockchains [49].

The Blockchain technology, by design, cannot comply with legal regulations, such as the GDPR. However, this does not mean it cannot be compliant, it just implies the need to complement Blockchain with other technologies. The general consensus among the reviewed papers is to leverage off-chain storage capabilities in order to achieve compliance. In this solution, data classified as personal data is encrypted and stored off-chain, and is linked to the distributed ledger through a hash pointer. This solves several of the aforementioned challenges since the off-chain data can be modified or deleted at any time. Additionally, storing personal data off-chain improves scalability, reduces data storage requirements, and enhances privacy (Miyachi & Mackey, 2021). Other solutions include destroying the encryption key and the use of chameleon hash functions. The former lies in the premise that the GDPR does not "specify what constitutes erasure" since, technically, the data is not erased but rather deemed inaccessible, remaining stored in the Blockchain. The latter only works in private Blockchains and requires a trusted authority to hold the secret key, which defeats the purpose of blockchain to eliminate the need for third parties and centralized authority [8].

It is essential to mention that each of the presented solutions has its own limitations and should be chosen based on the specific use case. In fact, the compliance with GDPR will depend on the specific architecture that underlies a particular Blockchain application, each application must be evaluated independently, on a case-by-case basis.

Some studies proposed a set of good practices and guidelines for developers and architects to achieve GDPR compliance when building Blockchain solutions. An appropriate understanding of the GDPR principles and objectives is fundamental so that the Blockchain can be designed and tailored according to the GDPR requirements [31]. Furthermore, the principles of privacy-by-design and privacy-by-default, data minimization, transparency, pseudonymization, encryption and other privacy-enhancing tools should be applied when designing Blockchain applications. Smart contracts containing the users' consent should be implemented.

In short, Blockchain technology is an interesting alternative to traditional methods of storing information, however, the proper precautions should be taken and the foregoing challenges considered when implementing Blockchain applications.

4.4.1. Research Limitations

Identified limitations of this study include the fact that a single research database, EBSCO, was searched for eligible studies, even if considered a major aggregator, and the restriction to articles written in the English language, which may exclude significant studies in other languages. Furthermore, even though there was no restriction on the type and domain of Blockchains, this study focused mostly on generic Blockchain solutions for storing and processing personal data and did not analyse the different implications on each type and specific domains.

Chapter 5

5. Implications of the GDPR in Healthcare: A Systematic Literature Review

In this chapter, a Systematic Literature Review (SLR) is conducted with the goal of identifying the main benefits and challenges of compliance with the GDPR in the healthcare sector, as well as existing derogations from the regulation.

5.1. Planning

This section corresponds to the first phase of the abovementioned SLR process. It begins by stating the underlying motivation behind this work, followed by the specification of the developed research questions that guided the review, and ending with the description of the review protocol.

5.1.1. Motivation and Related Work

The General Data Protection Regulation (GDPR), which became enforceable on 25 May 2018 [19,29], seeks to harmonize data protection laws across the European Union (EU), to protect and empower all EU citizen's by defining several basic rights regarding control of and access to their personal data, and to reshape the way organisations approach the processing of data, especially personal data [20,69–72].

This harmonization that the GDPR intends to achieve affects all economic sectors, including healthcare [71,72]. However, despite being sector wide, the regulation impact on organisations is sector specific [69], meaning the obligations and requirements of organisations under the GDPR may differ according to the specific sector they find themselves in.

The healthcare sector traditionally processes large amounts of personal data. In the present technological era, huge amounts of personal data are generated due to the increasingly use of modern technologies, such as mobile health applications and wearable devices (e.g., smart watches).

Such kind of personal data represents a special category of personal data under the GDPR, the so-called "sensitive data" [14–19]. This type of personal data benefits from additional protection [15]. Hence, it is of the essence that healthcare organisations and other institutions that process or intend to process health data of individuals are aware of their obligations under the GDPR and the measures that they need to take to fulfil them.

To our knowledge, there is no systematic review on the impact and implications of the GDPR in the healthcare industry available. That being said, with the goal of achieving a deep understanding of the research topic, a Systematic Literature Review (SLR) is performed where the main benefits and challenges of compliance with the GDPR in the healthcare sector are identified and categorized. The knowledge gathered in this work will support the authors in the development of a GDPR-compliant healthcare Blockchain solution, focused on health tourism.

5.1.2. Research Questions

Based on the main purposes of this research, the following three research questions were formulated to guide the review:

- **RQ1.** What are the benefits of compliance with the GDPR in the healthcare sector?
- **RQ2.** What are the challenges of compliance with the GDPR in healthcare?
- **RQ3.** What exemptions from the GDPR exist in the healthcare sector?

5.1.3. Review Protocol

To address the research questions, a review protocol was delineated, specifying the methods used to undertake the review. The review protocol used in this research is illustrated in figure 8. The goal is to identify and map the studies which are relevant to the research topic and that may provide answers to the proposed research questions. With that in mind, a paper search was conducted in the second and third weeks of April 2022. The search string and the chosen research database to perform the search are listed below:

- Search string: (gdpr AND healthcare)
- Research database: EBSCO Discovery Service

The search engine EBSCO Discovery Service was selected due to its wide coverage. It includes the main sources, namely Scopus, Academic Search and Clarivate Analytics (itself containing Web of Science, Current Contents Connect, Derwent Innovations Index, MEDLINE e SciELO Citation Index, and other resources such as Citation Reports and Essential Science Indicators). The search expression presented above was used to search the database in the abstract field of the articles. At first, the keyword “gdpr” (General Data Protection Regulation) was combined with “health tourism” and "wellness", which are directly derived from the scope of our research. However, due to the lack of relevant studies found in preliminary test searches, we decided to broaden the search to the healthcare sector as a whole instead of focusing on the specific area of health tourism. That being said, the keyword “healthcare” was included in the search string and the keywords “health tourism” and "wellness" were removed since they did not provide any additional studies to the search.

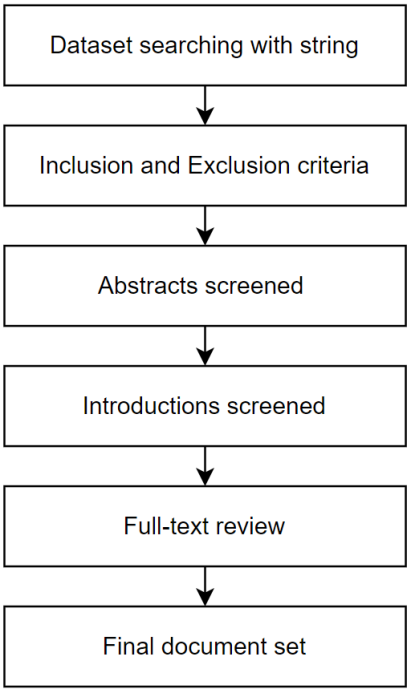

Figure 8 - Review protocol

After performing the database search with the search string, the first set of papers was obtained, and the inclusion and exclusion criteria was applied to refine the search results. The inclusion and exclusion criteria applied can be observed in table VII. The selected studies must be peer reviewed academic journals or conference materials, which should assure a certain quality of the papers, written in the English language, with accessibility to the full text, and should be related to healthcare and GDPR. Studies that failed to fulfil any of these requirements were discarded. No specific starting publication date was defined to constrain the database search, although it was expected that no paper prior to 2016, the year the GDPR was originally published, would be found.

Table VII - Inclusion and Exclusion criteria applied in the search

Inclusion criteria	**Exclusion criteria**
Written in English	Not written in English
Full text accessible	Full-text not accessible
Academic journals and conference materials	Not academic journals or conference materials
Peer reviewed	Not peer reviewed
Mentions both GDPR and healthcare	Does not mention GDPR or healthcare

Once the inclusion and exclusion criteria were applied, the abstracts, introductions, and full texts were screened in order to narrow down the results and obtain the final set of studies to conduct the review. In each of these stages, the inclusion and exclusion criteria were taken into consideration and the papers were classified as “Included”, “Excluded”, or “Maybe”, according to their relevance for the research. Papers classified as “Included” or “Maybe” proceeded to the next stage, whether papers marked as “Excluded” did not.

5.2. Conducting

This section corresponds to the second phase of the SLR process, in which it will be described how the review was conducted. It begins by describing the selection of studies procedure in detail, followed by detailing the data extraction process, and concludes with an analysis of the extracted data.

5.2.1. Selection of Studies

A complete summary of the search process performed in order to identify the most relevant studies for the review can be observed in figure 9.

The first step consisted of searching the EBSCO database with the search string in all fields of all documents. No aggregators were used in the process. The search engine returned a total of 589 hits. To narrow down the results, a second search was conducted using the same search string but constrained to look for the keywords in the abstract field. A total of 317 studies were obtained at this stage. Next, the inclusion and exclusion criteria were applied, limiting the search to peer reviewed academic journals and conference materials written in the English language, which produced a total of 216 results. After removing the duplicates, the set was reduced to 125 candidate studies. The 125 abstracts were then screened using the web-tool Rayyan and, from those, 76 papers were excluded, 28 were classified as “Maybe”, and 21 were included. Of the 76 papers that were excluded, 71 were considered out of scope, 3 were not written in the English language, 1 the full text was not available

and 1 was neither an academic journal nor conference material. Following, the introductions of the remaining 49 papers were read. In the end, 19 papers were deemed out of scope and excluded, 18 were classified as “Maybe”, and 12 were included. The final stage involved reading the full text of 30 papers. In this final stage, 25 papers were included and, consequently, selected for performing the review while 5 were excluded, 3 for being out of scope, 1 due to study design and 1 for poor overall quality of the paper.

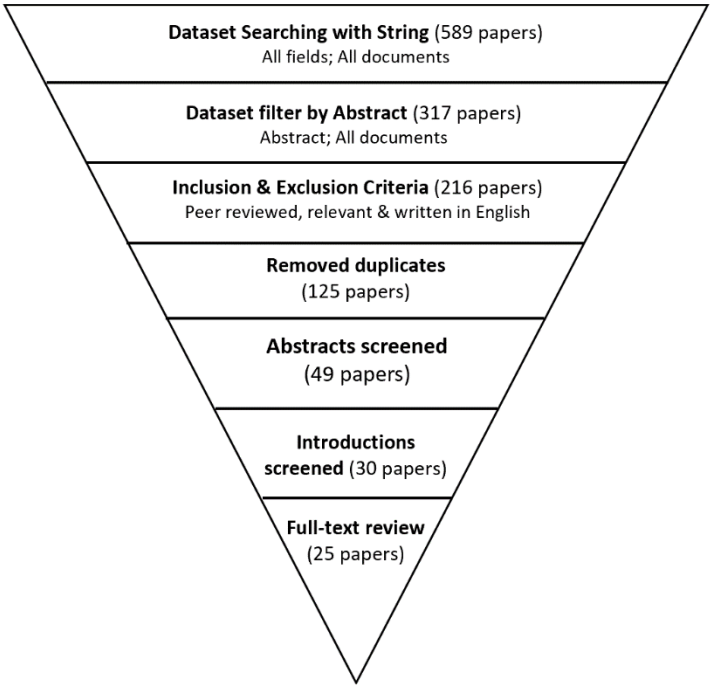

Figure 9 - Selection of studies process

5.2.2. Data Extraction

To facilitate the data extraction process, a form to collect all the required information concerning the research questions was designed following the guidelines from [23,24]. The form consists of the following items:

- ID
- Author(s)
- Year of publication
- Title of paper
- Type of publication
- Publisher
- Journal name
- Keywords
- Research question 1

- Research question 2
- Research question 3
- Additional findings
- Notes

5.2.3. Data Synthesis

In this section, an analysis of the data extracted from the 25 selected studies is presented. An overview of the number of publications over the years and type among the selected studies is provided.

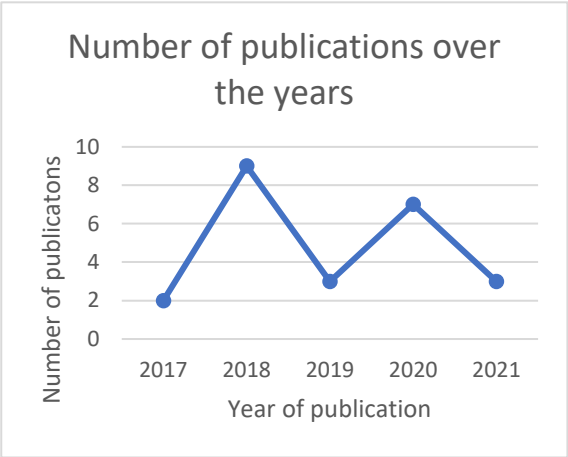

Figure 10 - Number of publications over the years

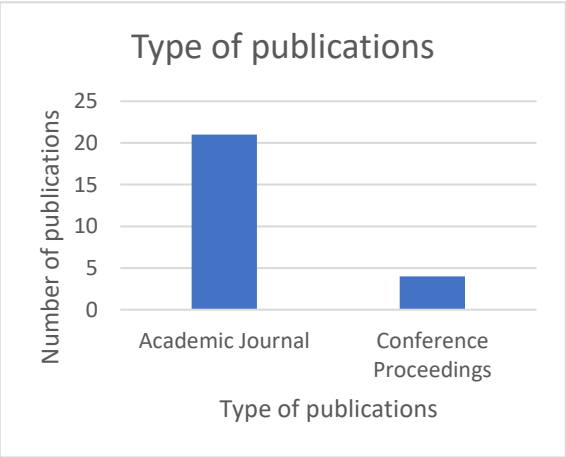

Figure 11 - Type of publications

Looking at figure 10, we can observe the number of publications over the years among the selected studies. As expected, no paper prior to 2016 was selected. In fact, the first publications from this set trace back to 2017, one year after the GDPR was originally published.

It is possible to point out that there has been a slightly decrease in the number of papers published over the years, with 2018 and 2020 being the years with the most contributions for this research. With the GDPR being officially enforceable to all EU member states and other organisations that process personal information of individuals inside the EEA (European Economic Area) from 25th of May 2018, it is only natural that 2018 is the year with the most publications regarding the research topic.

Another thing to notice is that the search provided no papers after 2021. This may be justified due to the time the search was conducted. As previously mentioned, the database search occurred in April 2022, which renders 2022 an incomplete year.

Regarding the type of publication, we can notice that, from the final set of documents, 21 correspond to academic journals while the remaining 4 are conference materials, as shown in figure 11.

5.3. Reporting

At this stage of the SLR, all three research questions are addressed in light of the studies obtained using the review protocol.

5.3.1. RQ1 – What are the benefits of compliance with the GDPR in the healthcare sector?

In this section, the SLR provides an answer to the first research question, by revealing a list of the benefits of complying with the GDPR in the healthcare sector found in the literature. As such, the list displayed in Table VIII is based on the literature review of the 25 publications. The table includes a list of the benefits, the number of publications in which they have been mentioned, and their respective references.

Table VIII - Benefits of compliance with the GDPR in the healthcare sector

Benefit	**Reference**	**Total**
Data subjects' control of personal data	[15,17,18,20,69,73–77]	10
Trust	[14,16,18,29,72,74,76,78,79]	9
Standardization of data protection laws in EU	[20,74]	2

The analysis revealed that the increased control that the data subjects possess over their personal health data is considered the main benefit of compliance with the GDPR in the healthcare sector, being mentioned in 10 of the 25 reviewed papers. By laying down a variety of legal rights as well as imposing a series of requirements on data controllers and processors over the processing of data, the GDPR is able to empower the data subjects with more control over their personal data [15,17,20,73,76].

The GDPR grants data subjects the legal right to specifically agree to (or refuse) having their data processed in any of the ways statutorily defined as "processing" [75,77]. This reliance on consent gives data subjects significantly more scope to control the processing of their personal data [69]. Individuals also have the legal right to be fully informed (Article 13 of the GDPR) about each and every intended use of their data by data controllers and processors, as well as the right to refuse such use [73,77]. They have the right to be informed about the security measures that are put in place to protect their personal data and transparently see how their personal data is processed, by whom and to what purposes [73]. Besides the right to be informed, GDPR enhances individuals' rights to access (Article

15), amend (Article 16) and even erase (Article 17) their personal data. Furthermore, since health data is regarded as “sensitive data”, which is a special category of personal data under the GDPR, it benefits from additional protection from the regulation [15]. The GDPR establishes stricter requirements for data controllers and processors that process and storage this type of personal data.

The GDPR is not only beneficial for the data subjects but also for the organisations as it provides individuals the confidence to share their personal data with the organisations [29]. This is particularly important for organisations focused on healthcare research and quality-of-care. Trust is then perceived as another advantage of compliance with the GDPR in the healthcare sector, as mentioned in 9 of the 25 reviewed papers.

Data subjects’ control over their personal data is directly associated with the level of trust they have in the organisations that handle that same data. As such, the enhanced control that the GDPR provides to the individuals over their personal data improves the public's confidence in how their information will be accessed and used by organisations [18,76]. Patients and stakeholders that would otherwise be reluctant to share their personal data, due to cases of previous misuse of patients' data, will now be more inclined to do it [78,79].

GDPR’s provisions that ensure the privacy and protection of individuals’ personal data are also a key element in building trust in healthcare organisations, particularly the ones that promote transparency and accountability [16,18,74]. The GDPR requires relevant bodies to demonstrate their compliance with the principles outlined by the regulation, which greatly affects the public’s confidence in the organisation [74]. Other requirements, such as conducting a Data Protection Impact Assessment (DPIA) also enhance the trust among data subjects and stakeholders as it results in the minimization of privacy, security and reputation risks [72].

The standardization of data protection laws within the European Union (EU) promoted by the new set of regulations introduced in the GDPR is yet another benefit, as stated by [20,74]. Prior to the introduction of the GDPR, the overall governing law on data protection EU was the Data Protection Directive. As a directive, EU member states were required to enact their own laws based on the principals outlined by the directive [74]. Ultimately, this led to legal variances which resulted in different degrees of enforcement, legal uncertainty and administrative costs, affecting both the trust and confidence of individuals as well as organisations’ ability to operate [74]. Unlike a directive, a regulation is directly binding and applicable on all EU member states [77], therefore, the new set of rules introduced by the GDPR resolves previous issues by standardizing data protection regulations, improving the sharing of data and boosting economic development throughout the EU [20,74].

5.3.2. RQ2 – What are the challenges of compliance with the GDPR in healthcare?

In this section, the SLR provides an answer to the second research question. Table IX outlines the challenges of compliance with the GDPR in the healthcare sector reported in the reviewed papers.

Table IX - Challenges of compliance with the GDPR in the healthcare sector

Challenge/Requirement	Reference	Total
(Explicit) consent	[14,15,17–20,29,69,73,75–83]	18
Satisfaction of data subjects' rights	[14,15,18–20,69,73–76,80,84,85]	13
Data Protection Impact Assessment (DPIA)	[15,18,71,72,74–76,80,81,84,85]	11
Application of technical and organisational safeguards	[14–16,19,20,29,69,76,77,80]	10
Data breach notification	[15,18,20,73,74,76,79,85]	8
Data transfer between EU member states	[15,16,20,70,74,77,79]	7
Appointment of a Data Protection Officer (DPO)	[18,20,74,76,79,85]	6
Legal basis for the processing of personal data	[18,29,69,70,77,84]	6
Record of Processing Activities (ROPA)	[71,74,76,85]	4

The most cited challenge in the literature concerning compliance with the GDPR in the healthcare sector relates to consent, being mentioned in 18 of the 25 reviewed papers. The GDPR raised the bar by laying down more rigorous requirements for obtaining individuals' consent [73,81]. The consent must be obtained from the data subjects prior to the processing or communication of their personal data [15,20], unless derogations exist [20], and "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her. […] Silence, pre-ticked boxes or inactivity should not therefore constitute consent" (Recital 32 of the GDPR) [69,77]. The consent needs to be demonstrable and should be presented in a way that clearly distinguishes it from other matters, in an understandable and easily accessible form, using a clear and simple language [17,69]. Additionally, the consent may be withdrawn at any time as long as it does not affect the lawfulness of the

processing before the withdrawal and it should be as easy as giving consent [69,81]. As processing of health data concerns a special category of personal data, if consent is the legal ground relied on for setting aside the prohibition on processing, that consent will need to be “explicit consent” [69], meaning that the data subject must give an express statement of consent, such as by a written statement [83].

The satisfaction of data subjects’ rights is described as another challenge of compliance with the GDPR in the healthcare sector, mentioned in 13 publications. Data controllers must implement appropriate measures in order to adhere to the data protection rules and requirements laid out by the GDPR [15]. Thus, providing the data subjects with several fundamental rights and freedoms that give them more control over their personal data [76]. Data subjects have the right to be informed if their data are being processed, how, where, and for what purpose (Article 13 of the GDPR) [14,19,73]. This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language [14,19,73]. The controller must also provide access for the data subjects to their personal medical records (Article 15 of the GDPR) as well as a digital copy of personal data free of charge and in a structured, commonly used and machine-readable format (Article 20 of the GDPR) [20]. Other data subjects’ rights, such as right to rectification (Article 16) and right to erasure (Article 17) must also be assured by the data controller.

The GDPR introduced two specific duties that impact healthcare, namely the Record of Processing Activities (ROPA) and, for each high-risk processing, the Data Protection Impact Assessment (DPIA) [71]. These are mentioned in 4 and 11 reviewed papers, respectively. The ROPA includes a minimum dataset of information that defines each processing made by the controller or the processor, which are the two entities involved in the protection of personal data [71]. In other words, The GDPR requires data controllers and processors to maintain records of their processing activities (Article 30 of the GDPR) [74,76,85]. In the case of the DPIA, this must be performed if the processing poses high risks to the rights and the freedom of individuals [71,72]. The DPIA should assess the risks of the data processing and describe how these risks will be averted [81]. The healthcare domain involves a large scale processing of sensitive data, resulting in high risks to the rights and freedoms of their subjects. Therefore, it should be assumed that a DPIA is always necessary [71,72].

The appointment of a Data Protection Officer (DPO) is a requirement for large institutions or institutions which process certain types or volumes of data [20], which is the case of healthcare institutions. The duties of the DPO include: informing and advising the organization and its employees about their obligations to comply with the GDPR; monitoring and managing compliance with the GDPR; and be the first point of contact for supervisory authorities and for individuals whose data is processed [74]. As such, the GDPR recommends that the DPIA should be performed together with the DPO (van Veen, 2018).

Another significant challenge constitutes what happens in the event of a data breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data trans-mitted, stored or otherwise processed [18,20], as mentioned in 8 papers. Unless it poses no risk to the rights and freedoms of individuals, data breaches must be reported to supervisory

authorities and individuals affected by the breach within 72h (Article 33 of the GDPR) of the detection [18,20,73,74,76]. Preventive technical solutions need to be implemented in order to avoid a data breach and individuals have the right to know what safeguards are in place [15]. Organisations may be fined if preventive measures are not implemented and for non-compliance with the breach notification requirements [15,74]. Penalties can amount to as much as €20m or 4% of the company's global annual turnover, whichever is greater [74,76,85].

The topic of health data transfer between EU member states is also a widely discussed challenge in the literature, mentioned in 7 publications. Despite the GDPR intentions to foster data sharing within the EU through consistent level of personal data protection and the elimination of obstacles to data flows (Recital 10 of the GDPR) [70], the room that it creates for further regulation at the national level results in conflicts and limitations regarding transfer of personal data [70,74]. Concerning the sharing of data outside the EU, the GDPR implemented stricter rules [79]. Data can cross EU internal borders if the planned processing complies with the general requirements of the GDPR, namely the conditions detailed in chapter V of the GDPR [70,74]. The laws of non-EU countries must not undermine existing data subjects' rights and appropriate safeguards must be put in place [77,79]. Ultimately, the European Commission decides if the destination of the data ensures an adequate level of protection [74,77].

In order to lawfully process personal data under the GDPR, which is considered by 6 papers as a challenge, data controllers and processors are required to invoke a legal basis pursuant to Article 6(1) [29,69,70]. In the case of health data, a legal ground that justifies the processing of this special data must also be invoked pursuant to Article 9(2) of the GDPR [70]. The latter will be addressed in further detail in *section 5.3.3*. Table X enumerates the relevant legal basis for the processing of personal data mentioned in the reviewed papers and provides a brief description of each one.

Table X - Legal basis for the processing of personal data

Article	Description
6 (1)(a)	The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
6 (1)(b)	Processing is necessary for the performance of a contract to which the data subject is party.
6 (1)(c)	Processing is necessary for compliance with a legal obligation to which the controller is subject.
6 (1)(d)	Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
6 (1)(e)	Processing is necessary for the performance of a task carried out in the public interest.
6 (1)(f)	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

Lastly, the regulation requires that the controller implements appropriate technical and organisational measures for protecting the rights and freedoms of the data subject, in particular to respect the principle of data minimization [69]. It is also essential to take appropriate safeguards if the data has to be transferred outside a non-EU member state, whose level of data protection is considered to be adequate [15], or in the case that the controller is solely using automated processing [77].

5.3.3. RQ3 – What exemptions from the GDPR exist in the healthcare sector?

As mentioned earlier, the GDPR describes some specific derogations for data concerning health, aiming at protecting the rights of individuals and the confidentiality of their personal health data, whilst preserving the benefits of processing data [20]. Table XI presents the requirements and obligations of the GDPR reported in the literature for which specific derogations exist in the healthcare sector. These exemptions will be addressed in detail in this section.

Table XI - Exemptions from the regulation on health data

Exemption (from the)	**Reference**	**Total**
Prohibition of the processing of health data	[14,17–20,29,69,70,73,76,77,79–84]	17
Data subjects' rights	[17,20,69,70,75,79,81]	7
Purpose limitation principle	[69,70,80,81]	4
Storage limitation principle	[69,81]	2

In principle, the processing of special categories of personal data, which includes data concerning health, is strictly prohibited under the GDPR [14,17,19,69,77,81]. Article 9(1) of the GDPR clearly states that the "processing of personal data revealing racial or ethnic origin, […] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited". However, the regulation lays down some exemptions to this prohibition, as mentioned in 17 of the 25 reviewed studies.

In addition to the established legal basis for processing personal data pursuant to Article 6(1) of the GDPR, a legal ground that justifies the processing of special categories of personal data pursuant to Article 9(2) GDPR must then be invoked in order to lawfully process health data for healthcare purposes [19,69,70,81]. Of the 10 exemptions to the prohibition of processing of health data laid down by the regulation, the literature focuses on 6 that are particularly relevant for the processing of health

data and that might be invoked in the context of health services and research. Table XII lists the relevant exemptions mentioned in the reviewed papers and provides a brief description of each one.

Table XII – Relevant exemptions for the processing of health data

Article	Description
9 (2)(a)	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
9 (2)(c)	Processing is necessary to protect the vital interests of the data subject.
9 (2)(g)	Processing is necessary for reasons of substantial public interest.
9 (2)(h)	Processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
9 (2)(i)	Processing is necessary for reasons of public interest in the area of public health.
9 (2)(j)	Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

It is important to point out that, of the abovementioned derogations, the explicit consent (Article 9 (2)(a)), if not excluded by member state law, and the protection of the vital interests of the data subjects (Article 9 (2)(c)) are the only legal grounds based on which special categories of personal data can be processed without member states' further regulation [70]. Under the remaining derogations, the processing of data concerning health is based on specific member state law which must be "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject" [17,70,77,81]. Organisational and technical safeguards outlined in Article 89 (1) include anonymisation, pseudonymisation and encryption [20]. Moreover, Article 9 (2)(h) is also subject to professional secrecy, according to Article 9 (3) [81].

The limitation of data subjects' rights is another significant derogation from the GDPR affecting the healthcare sector, as stated in 7 papers. According to Article 89 (2) of the GDPR, the data subjects' rights of access, rectification, restriction and to object can be limited by member state law in the interest of data processing for scientific research under the conditions and safeguards defined in Article 89 (1) of the GDPR in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes [69,70,75,81]. In the same conditions as previous rights, the obligation of transparency when data have not been obtained directly from the data subject and the right to be forgotten do not apply [81]. Furthermore, the right to be forgotten and the right to object are also not applicable for reasons of public interest in the area of public health [81]. It should be noted that the ability to

derogate from the protection of these rights is not available when relying on consent as the legal basis for processing personal data [69].

Finally, the GDPR specifies directly applicable exemptions from the purpose and storage limitation principles, as mentioned in 4 and 2 publications, respectively. According to Article 5 (1)(b) of the GDPR, further processing of personal data for reasons of public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), be compatible with the purpose for which they were originally collected and will not require a new legal basis as the original suffices [69,70,81]. This, however, does not mean that those who did not have access to the personal data can now have [81]. Also, in case of transfer of the personal data to another legal entity to perform research, the new controller will require its own legal basis for processing [81]. Similarly, the storage limitation principle is also limited in the context of scientific research [69]. The regulation states that personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) and subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject (Article 5 (1)(e)) [69,81].

5.4. Discussion and Implications

The papers reviewed in the SLR emphasised the importance of being compliant with GDPR, especially in an industry such as healthcare which deals with extremely sensitive personal data of patients. The lack of compliance may result in unnecessary risks to the rights and freedoms of individuals as well as organisations which may suffer from financial penalties for failing to comply with the regulations [20].

Even though it is mandatory for all EU member states, some papers acknowledged the benefits of being compliant with the GDPR in the healthcare industry. The literature identified the improved control of data subjects over their personal health data as one of the main benefits of compliance. By defining a variety of legal rights and imposing several requirements on data controllers and processors, the GDPR enables the data subjects to manage their personal health data however they see fit [15,17,20,73,76], except in specific cases such as in cases of public interest. This enhanced control leads to yet another benefit as it is one of the factors that positively influence the level of confidence data subjects have in the organisations that handle their personal data [18,76]. Trust is key as it is what motivates individuals to share their personal data with the organisations. The standardization of data protection laws within the EU is also recognised as an advantage. However, it is important to note that, even though it is an improvement over the previous regulation, the manoeuvrability that the GDPR provides for further legislation at the national level, particularly in relation to exemptions, leads to some legal variances hindering the sharing of data [70].

Most articles focused on the challenges regarding compliance with the GDPR on healthcare as well as the requirements and obligations imposed on data controllers and processors. The literature considers achieving patients' consent one of the most disturbing concerns as the GDPR's stricter requirements add significant complexity to the use of patients' data [79]. The regulation, however, acknowledges the difficulty of obtaining specific and granular consent, particularly for scientific research, and so it recognises to some extent 'broad consent' (Recital 33). It is often not possible to fully identify the purpose of personal data processing at the time of data collection. Therefore, data subjects should be allowed to give their consent to only certain areas [69,81]. Moreover, it is vital to understand that the notion of "consent" is different under the GDPR as opposed to the ones traditionally sought in clinical or scientific research. The standard notion of consent seeks a subject's free and voluntary expression of his or her willingness to participate in a particular clinical or scientific research, setting aside the duty of confidence. On the other hand, GDPR seeks consent for the processing of personal data. This implies a requirement for distinct formal processing for both types of consent [82]. [86] states that organisations may rely on consent to set aside the duty of confidence but rely on a different legal ground under the GDPR, namely the public interest and the research condition.

Several studies have also addressed the specific derogations for data concerning health laid out by the GDPR. The GDPR recognises the importance of science and innovation and is designed to facilitate the free flow of information. To that end, it defines several exemptions for processing of special categories of personal data, such as health data [83], which is prohibited under the GDPR. These can be observed in *section 5.3.3*. While explicit consent is considered the most common legal ground for processing, it is important to stress out that is not a mandatory requirement to comply with the GDPR [83].

This SLR has brought important contributions to both academia and industry on the effects of the GDPR on healthcare. At a time where huge amounts of personal health data are being generated daily due to the increasingly use of modern technologies, researchers, practitioners, healthcare organisations and other institutions that process or intend to process health data of individuals may resort to our study to gain awareness and to better understand their obligations under the GDPR and the procedures that they need to take to accomplish them. The quality of the evidence included in the review is considered to be high since the vast majority of the reviewed papers were published in top-tier scientific journals.

5.4.1. Research Limitations

Identified limitations of this study include the fact that a single research database, EBSCO Discovery Service, was searched for eligible studies, even if considered a major aggregator, and the restriction to articles written in the English language, which may have excluded significant studies in other languages. Furthermore, only "white" literature (academic journals and conference materials) was reviewed, leaving out possibly interesting "grey" literature, such as technical reports from the industry

side. Finally, this study focused solely on the GDPR's provisions, which are quite general and lack the specifics needed for routine implementation, leaving room for member states to modify certain aspects of the GDPR in their own data protection laws, especially in economic sectors that require more detailed provisions, such as healthcare [16].

Chapter 6

6. Blockchain for Health Tourism: A Multivocal Literature Review

In this chapter, a Multivocal Literature Review (MLR) is conducted to summarize the existing evidence on both the state-of-the-art and practice on the use of blockchain solutions for health tourism.

6.1. Planning

This section corresponds to the first phase of the abovementioned MLR process. It begins by stating the underlying motivation behind this work, followed by the specification of the developed research question that guided the review, and ending with the description of the review protocol.

6.1.1. Motivation and Related Work

As previously mentioned, there are some entrenched challenges within the health tourism industry, such as privacy and transparency concerns, lack of access to centralized medical records, fraudulent practices, opportunistic behaviour of intermediaries, foreign currency risks, and contractual/legal issues, that require addressing [87]. Blockchain technology is perceived as a viable solution for these problems, however, the current literature on blockchain use in health tourism is largely limited and fragmented which hinders its large-scale acceptability and implementation [87].

With the goal of achieving a deep understanding of the research topic, a Multivocal Literature Review (MLR) is performed where the current state-of-the-art in the use of Blockchain for health tourism is assessed. By performing a MLR instead of other forms of review, the authors expect that the GL collected complements gaps of the formal literature and provides “current” perspectives from the industry side. Additionally, the authors feel that if GL were not included important perspectives on the topic could be lost. The knowledge gathered in this work will support the authors in the development of a GDPR-compliant healthcare Blockchain solution, focused on health tourism.

Prior to undertaking the MLR, seven other existing systematic reviews on the topic were identified and examined [3,40,88–92]. This allowed us to acquire a deeper understanding on the subject, since systematic reviews are considered the highest level of evidence [23,24], and to identify any existing gaps in the literature that should be addressed in our work. However, only [87] explicitly mentions Blockchain in the context of health tourism while the remaining reviews focus on PHR blockchain solutions for healthcare in general. [87] developed a blockchain framework for medical tourism providing a systematic overview of the various blockchain applications and their benefits for health tourism. Nonetheless, it does not cover existing solutions nor the current stage of development of blockchain solutions for health tourism practice.

6.1.2. Research Question

Based on the main purposes of this research, the following research question was formulated to guide the review:

- **RQ.** What is the current state-of-the-art in the use of Blockchain for health tourism?

6.1.3. Review Protocol

To address the research question, a review protocol was delineated, specifying the methods used to undertake the review. The review protocol used in this research is illustrated in figure 12. The goal is to identify and map the studies which are relevant to the research topic and that may provide answers to the proposed research question. With that in mind, a search was conducted in the first week of October 2022. The search string and the chosen research database to perform the search are listed below:

- Search string: (blockchain OR dlt) AND ("medical tourism" OR "global healthcare" OR wellness OR wellbeing OR well-being OR "personal health records")

- Research databases: EBSCO Discovery Service, Google

The search engine EBSCO Discovery Service was selected due to its wide coverage. It includes the main sources, namely Scopus, Academic Search and Clarivate Analytics (itself containing Web of Science, Current Contents Connect, Derwent Innovations Index, MEDLINE e SciELO Citation Index, and other resources such as Citation Reports and Essential Science Indicators). Although EBSCO Discovery Service also includes some grey literature, we decided to use Google as our primary engine

to search and collect grey literature. This raised an issue since, unlike in the formal literature, there is not a clear stopping condition for the search process of GL. That being said, considering that our evidence is mostly qualitative, we identified theoretical saturation as the best stopping criteria for our GL search. As such, when we reach a point of theoretical saturation, i.e., no new concepts emerge from the search results, the search will be stopped. More specifically, when no relevant study emerges from a Google page, the search will be stopped.

The search expression presented above was used in the EBSCO Discovery Service database to search in the abstract field of the articles and in Google as a regular web search. At first, the keywords “blockchain” and “dlt” (Distributed Ledger Technology) were combined with “health tourism”, which are directly derived from the scope of our research. However, due to the lack of relevant studies found in preliminary test searches, we decided to add related search terms to the string in order to increase the number of hits. That being said, the keywords "medical tourism", "global healthcare", “wellness”, “wellbeing” and “well-being” were included in the search string. Furthermore, the keyword "personal health records" was also included due to being a potential solution for the practice of health tourism, when integrated alongside with blockchain technology. In the end, the keyword “health tourism” was removed since it did not provide any additional studies to the search.

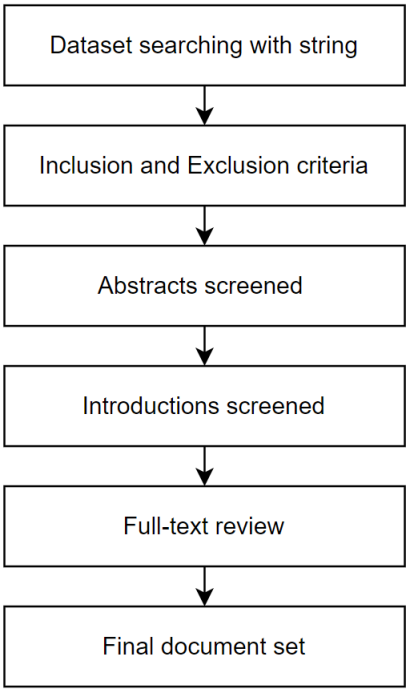

Figure 12 - Review protocol

After performing the database search with the search string, the first set of studies was obtained, and the inclusion and exclusion criteria was applied to refine the search results. The inclusion and exclusion criteria applied can be observed in table XIII. The selected studies must be written in the English language, but not restricted to academic papers, with accessibility to the full text, and should be related to blockchain and health tourism. Studies that failed to fulfil any of these requirements were

discarded. No specific starting publication date was defined to constrain the database search, although it was required that the literature had a clearly stated date as well as identified authors. These last criteria were particularly important for the quality assessment of the grey literature. As GL is more diverse and less controlled than formal literature, the selection criteria should be more fine-grained and take criteria considering the source type and specific quality assessment criteria [1].

Table XIII - Inclusion and Exclusion criteria applied in the search

Inclusion criteria	**Exclusion criteria**
Written in English	Not written in English
Full text accessible	Full text not accessible
Mentions both Blockchain and health tourism	Unidentified author
Describes or implements a solution	No publication date
	Does not mention Blockchain
	Does not mention health tourism (or related)

Once the inclusion and exclusion criteria were applied, the abstracts, introductions, and full texts were screened in order to narrow down the results and obtain the final set of studies to conduct the review. In each of these stages, the inclusion and exclusion criteria were taken into consideration and the papers were classified as “Included”, “Excluded”, or “Maybe”, according to their relevance for the research. Papers classified as “Included” or “Maybe” proceeded to the next stage, whether papers marked as “Excluded” did not.

6.2. Conducting

This section corresponds to the second phase of the MLR process, in which it will be described how the review was conducted. It begins by describing the selection of studies procedure in detail, followed by detailing the data extraction process, and concludes with an analysis of the extracted data.

6.2.1. Selection of Studies

A complete summary of the search process performed in order to identify the most relevant studies for the review can be observed in the diagram in figure 13 with a visual representation of the applied MLR selection process. This reflects all the selection work done through the methodical process of the MLR.

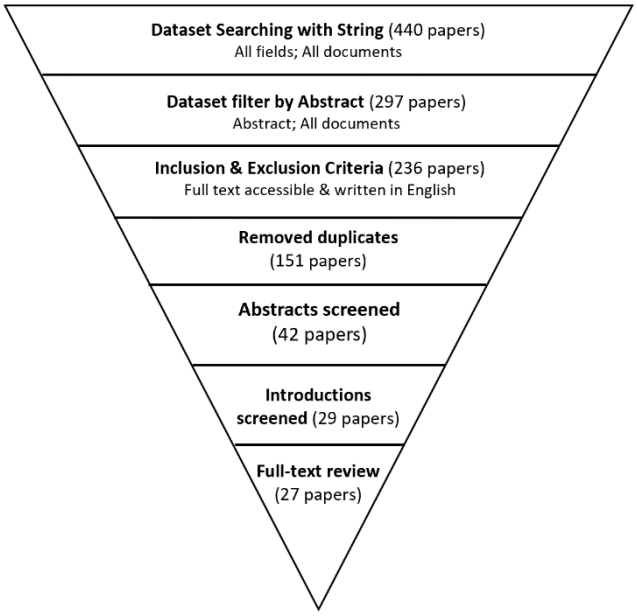

Figure 13 - Selection of studies process

The first step consisted of searching the EBSCO database with the search string in all fields of all documents. No aggregators were used in the process. The search engine returned a total of 434 hits. To narrow down the results, a second search was conducted using the same search string but constrained to look for the keywords in the abstract field. A total of 291 studies were obtained at this stage. Next, the inclusion and exclusion criteria were applied, limiting the search to full-text documents written in the English language, but not restricted to academic papers, which produced a total of 230 results. After removing the duplicates, the set was reduced to 145 candidate studies. The 125 abstracts were then screened using the web-tool Rayyan and, from those, 109 papers were excluded, 19 were classified as “Maybe”, and 17 were included. Of the 109 papers that were excluded, 108 were excluded due to being out of scope and 2 due to study design. Following, the introductions of the remaining 36 papers were read. In the end, 13 papers were deemed out of scope and excluded, 6 were classified as “Maybe”, and 17 were included. The final stage involved reading the full text of 23 papers. In this final stage, 22 papers were included and, consequently, selected for performing the review while 1 were excluded for being out of scope.

For the Google search, the first steps do not apply, thus the results stay the same in those steps, and the inclusion and exclusion criteria are applied from the start. The search returned a total of 6 relevant studies. In the cases belonging to GL there is no abstract, therefore all text was skimmed, making it possible to better assert an inclusion or exclusion of that publication.

In the end, 27 publications were considered relevant and remained for full-text document.

6.2.2. Data Extraction

To facilitate the data extraction process, a form to collect all the required information concerning the research questions was designed following the guidelines from [23,24]. The form consists of the following items:

- ID
- Author(s)
- Year of publication
- Title
- Type of publication
- Publisher
- Journal name
- URL
- Keywords
- Research question
- Blockchain use
- Type of system
- Type of contribution
- Additional findings
- Notes

6.2.3. Data Synthesis

In this section, an analysis of the data extracted from the 27 selected studies is presented. An overview of the number of publications over the years and type among the selected studies is provided.

Looking at figure 14, we can observe the number of publications over the years among the selected studies. The first publications from this set trace back to 2019, which shows the novice of the research topic. From then on, the number of publications was evenly distributed through the years showing a continued interest in the topic. Another thing to notice is that 2022 is an incomplete year since the database search occurred in October 2022. This could lead to a slight increase in the number of articles in that year showing an intensified interest in the topic.

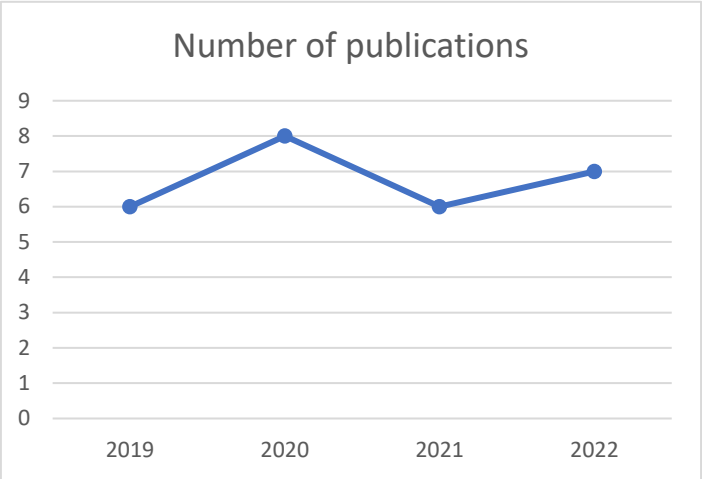

Figure 14 - Number of publications over the years

Regarding the type of publication, we can notice in figure 15 that, from the final set of documents, 19 correspond to academic journal papers, 5 are conference proceedings, 1 is a thesis, 1 is a webpage and 1 is a magazine article. It is interesting to notice that even though a MLR was conducted, most of the included studies are considered formal literature.

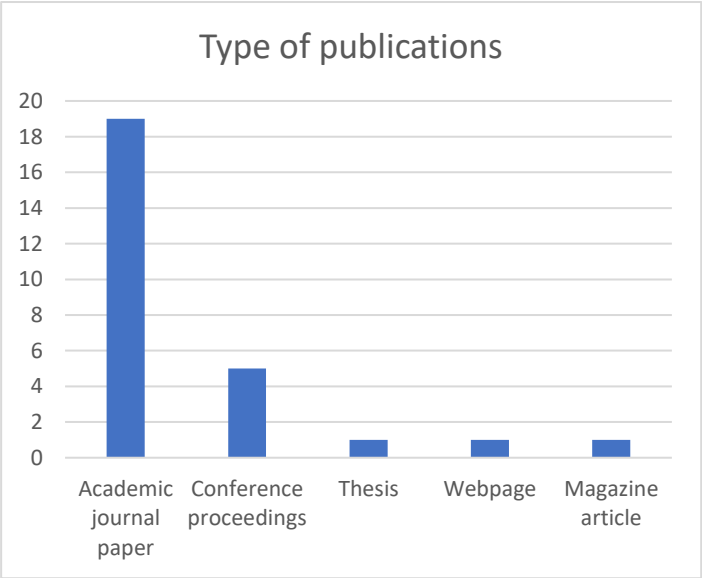

Figure 15 - Type of publications

6.3. Reporting

At this stage of the MLR, all three research questions are addressed in light of the studies obtained using the review protocol.

6.3.1. RQ – *What is the current state-of-the-art in the use of Blockchain for health tourism?*

6.3.1.1. Blockchain use in health tourism

As aforementioned, there are some entrenched challenges within the different phases of the health tourism value chain and blockchain is seen as a technology capable of breaking several of those barriers [7]. Out of the many applications and benefits mentioned in the literature, the most cited include: disintermediation, interoperability, trust and transparency.

With the growth of the health tourism market, many travel agencies have become health tourism intermediaries, playing an intermediary role between health tourists and health service providers [2,4]. In the pre-procedure phase, health tourists heavily rely on these intermediaries to organize the trip due to their lack of technical knowledge and their inability to assess the quality, suitability, and benefits of a health tourism destination [2–4]. Often such intermediaries engage in opportunistic behaviour, including fraudulent activity, which can be detrimental to patient health and well-being [3]. The peer-to-peer nature of the blockchain network enables potential health tourists to engage in direct, interactive communication with the healthcare service provider [1–4], eliminating the need for intermediaries. This disintermediation also eliminates data theft, identity theft, and credit card theft that can occur when patients share sensitive medical history and financial information with travel agents and other intermediaries [3].

Blockchain technology enables effective and fast sharing of health data among health tourists, foreign health service providers, local health services, and other stakeholders [4]. This is particularly important for health tourism since healthcare providers require access to past health records of patients so they can make better decisions during treatment [3]. By employing a patient-centric model of information handling, patients have access to their own tamper-free health data which they can manage and share with providers [3,7]. In addition, healthcare providers can also share data concerning a medical tourist to maintain the continuum of care [4]. Moreover, the interoperable environment of blockchain allows patients, especially those requiring extensive follow-up care or experiencing complications after returning home, to switch to a local healthcare provider [3].

The use of blockchain technology can also enhance trust and transparency allowing prospective health tourists to make reasonable and well-informed decisions [2]. In the pre-procedure phase, health tourists often rely on online search information, reviews and ratings [3]. Unfortunately, the inability to distinguish between real and fake reviews and ratings is a significant problem [3]. By using blockchain-enabled systems, health tourists receive detailed, authentic, and verified information about health tourism institutions [2]. Due to the immutability of the blockchain, ratings published on the blockchain cannot be deleted and updates are only possible with a traceable history. In addition, blockchain will

enable verification of the qualifications and entitlements of healthcare providers by linking them to certification bodies [2,3].

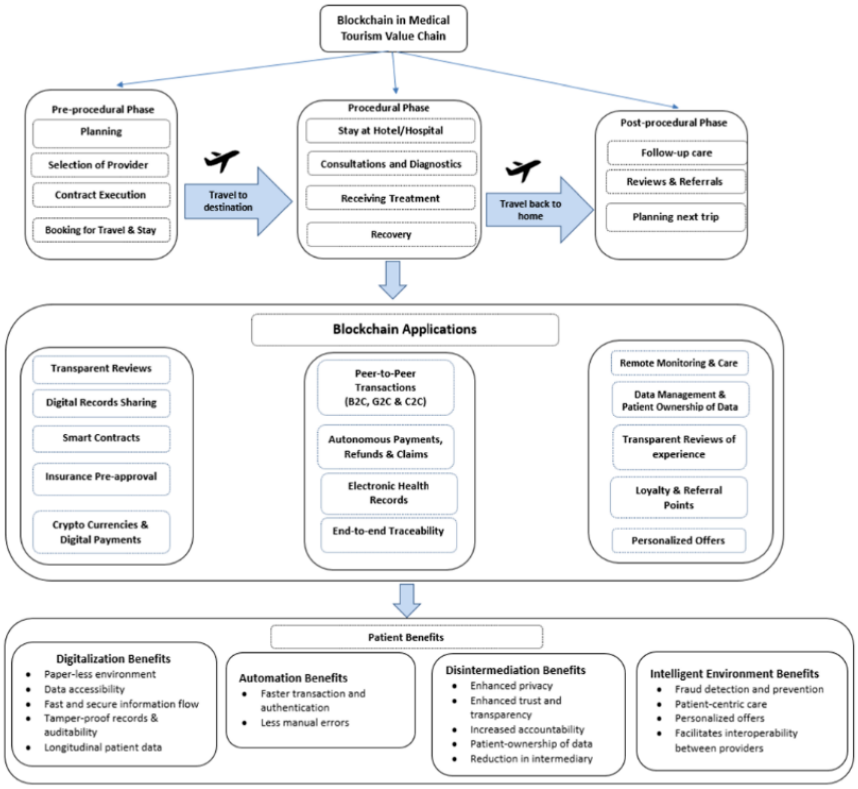

Figure 16 - Blockchain framework for health tourism [3]

[87] developed a very interesting and comprehensive blockchain framework for health tourism, which is displayed in figure 16, capturing the various blockchain applications and their respective benefits to patients and travellers across the health tourism value chain. The framework depicts the different stages comprising each of the three stages of the health tourism value chain, the blockchain applications that can be implemented in each phase as well as the corresponding benefits for the patients. The findings in this framework are useful for practitioners and policy makers who intend to take advantage of this technology. Furthermore, researchers can adapt and apply the framework in their own context.

6.3.1.2. Types of contributions of the analysed studies

Table XIV breaks down the types of contributions found in the literature. The table includes a list of the different types of contributions, the number of publications in which they have been mentioned, and their respective references.

Table XIV - Types of contributions of analysed studies

Type of contribution	Reference	Total
Raising awareness about Blockchain use in health tourism	[1–4,7,88,89,91,93–95]	11
Implementation of a Blockchain system	[38,39,41,88,91,96–98]	8
Literature review on Blockchain in health tourism	[3,40,88–92]	7
Description of a system idea not implemented yet	[42,99–104]	7
Examples of Blockchain use in health tourism	[2–4,95]	4
Discussion of Blockchain challenges in Health tourism	[3,4,92]	3
Proof of Concept of a Blockchain system	[39,103,104]	3

Most studies are still focused on raising awareness about the opportunities for using Blockchain in health tourism and its immense potential to address the industry's inherent challenges and inefficiencies. Nonetheless, some have already implemented a blockchain system or at least discussed ideas for systems that could be implemented. It is important to note, however, that not all systems found in the literature were developed specifically for the practice of health tourism but the authors believe them to be a viable solution. Some studies contribute with literature reviews, which allowed us to acquire a deeper understanding on the subject by assessing the existing solutions and the current stage of development of blockchain solutions for health tourism practice. Lastly, a few provide examples of blockchain use and potential applications and their benefits while about the same number discusses the existing challenges and limitations of the use of the technology in health tourism.

6.3.1.3. Types of systems proposed in analysed studies

Table XV outlines the different types of systems proposed in the literature. The table includes a list of the different types of systems, the number of publications in which they have been mentioned, and their respective references.

Table XV - Type of systems proposed in analysed studies

Type of system	Reference	Total
PHR	[38–41,88,90,91,96–98,100,103,104]	13
EHR	[42,89,92,99,101,102]	6
N/A	[1,4,94,95]	4
Health tourism system	[2,3,7]	3
Global healthcare system	[93]	1

Our analysis revealed that the prevailing type of system proposed in the literature is PHR which are owned by the patients and store health data from heterogeneous sources, such as the patients' medical records (e.g., EHR systems), different healthcare providers (laboratories, pharmacies), as well as various sensors from wearable devices (fitness trackers, smartphones, wearable sensors). EHR systems are proposed by 6 of the 27 analysed studies where only patients possess the private key to the medical records and hence can share it with desired healthcare providers. Some studies propose systems faced for the specific case of health tourism while 1 study focuses on a decentralised global healthcare system. In the case of 4 studies, no specific type of system was discerned.

6.3.1.4. Review of blockchain systems in analysed studies

As discussed above, using blockchain in health tourism has huge potential to address several of the current health tourism challenges. It can provide a novel approach to data ownership and permission-based access across the health tourism value chain. Blockchain technology in health tourism enables a shift from traditional interoperability to patient-centric interoperability, allowing patients to become the owners of their health records and to decide who has access to their data. Table XVI shows a review of some of the healthcare blockchain systems found in the literature and that the authors believe can be applied to the health tourism industry.

Table XVI - Review of blockchain systems

Name	Type of system	Description
OmniPHR [96]	PHR	Distributed system for storing patient health data. Allows a unified view of health records, which are distributed in several health organizations. It stores different patient datasets into different blocks on the chain.
[41]	PHR	Blockchain-applied PHR application that uses an on-chain, off-chain system to manage patients' consent

		data in blockchain.
OSHealthRec [88]	PHR	Blockchain-secured PHR which manages the authorization and access rights via a blockchain and stores the data off-chain. Healthcare professionals can only access the PHR with permission of the patient.
[100]	PHR	Blockchain-based secure PHR data storage sharing framework that leverages the benefits of IPFS that ensures privacy with patient full control over his data and enhancing scalability.
PatientDataChain [39]	PHR	Permission-based decentralized healthcare data sharing system which unifies all the data related to a patient's health records in a wallet, owned by the patient. The patient gives healthcare providers access to their data for a limited period of time.
MedAccess [102]	EHR	Decentralized platform which stores large scalable encrypted EHR on an effective off-chain solution and the identifiers on the blockchain.

6.4. Discussion and Implications

The MLR revealed that there is a growing interest in recent years on the use of Blockchain technology to address and solve several of the challenges and inefficiencies inherent to the health tourism industry [2,3,7]. Nevertheless, blockchain technology is under constant development and its implementation in health tourism is still at an early stage, which reflects on the current literature being largely limited and fragmented [3]. The majority of the analysed studies that specifically address health tourism mostly focuses on raising awareness about the opportunities and applications for using blockchain in health tourism.

As mentioned in the literature, the use of blockchain allows for disintermediation, interoperability, trust and transparency. However, the technology has limitations that must be considered when applied in the health tourism sector.

One of the main limitations is related to data storage and management. The data integrity feature of the blockchain results in immutability, so any data that is entered into the blockchain cannot be deleted or changed. However, because health data is protected by privacy laws, it must be deleted if requested by a health tourist. In addition, although blockchain can perfectly be used as a database to record health data, it is not suitable for storing large volumes of data or high-speed data due to

redundancy from many processing nodes holding a full copy of all data. To get around this limitation, only a hash or other metadata can be stored on the blockchain, while the key data is stored off-chain.

Another limitation of blockchain usage is the lack of standardization of blockchain architectures. This can hinder the establishment of relationships between healthcare providers implementing blockchain due to difficulties in integrating different architectures.

The most frequent implementations found in the literature consisted of distributed PHR systems leveraging both on-chain and off-chain capabilities where patients manage their own health records and decide who has access to their data. Though, it important to note that many of these solutions were not specifically designed for health tourism.

This MLR has brought important contributions to both academia and industry on the current state-of-the-art in the use of Blockchain for health tourism. At a time where huge amounts of personal health data are being generated and global healthcare is becoming more of a reality, researchers, practitioners, healthcare organisations and other institutions may resort to our study to gain awareness and to better understand the impact and relevance of the use of blockchain for health tourism practice.

6.4.1. Research Limitations

Identified limitations of this study include the fact that only English-written studies were considered for the review, which may exclude significant studies in other languages. Also, the fact that the current literature on blockchain in health tourism is largely limited and fragmented. More thorough qualitative research and empirical data are critical to better understand the potential of blockchain technology in the health tourism industry.

Chapter 7

7. Conclusion

Based on the knowledge gathered from the literature reviews, we developed a blockchain-based framework for healthcare data management that follows the GDPR, focused on the specific case of health tourism practice.

To ascertain the feasibility of using Blockchain technology to store personal data while being compliant with the GDPR, a Systematic Literature Review (SLR) was carried out to identify the benefits and challenges of using Blockchain technology to store personal data, and review the current state-of-the-art for implementing GDPR-compliant Blockchain solutions. The search produced a total of 432 candidate studies, including duplicates, from which 35 were deemed relevant to the SLR and read in full.

To assess the impact of the General Data Protection Regulation (GDPR) in the healthcare, a Systematic Literature Review (SLR) was carried out to identify the main benefits and challenges of compliance with the GDPR in the healthcare sector, as well as existing derogations from the regulation. The search produced a total of 589 candidate studies, including duplicates, from which 25 were deemed relevant to the SLR and read in full.

To investigate the current developments and perspectives on the use of Blockchain for the practice of health tourism, a Multivocal Literature Review (MLR) was carried out to identify and review existing evidence on both the state-of-the-art and practice on the use of blockchain solutions for health tourism. The search produced a total of 440 candidate studies, including duplicates, from which 27 were deemed relevant to the MLR and read in full.

Blockchain technology constitutes an exciting new alternative to traditional methods of storing and sharing information. Its distributed and immutable nature enables it to be applied to a wide variety of areas, including healthcare. It can address and solve many of the challenges and inefficiencies inherent to the health tourism industry [2,3,7]. Even so, the technology possesses certain limitations and its implementation raises a significant amount of challenges that must be considered when applied in the health tourism sector, mostly concerning compliance with legal regulations.

In a time where Blockchain is at an early stage of development and the practical implications of the GDPR on the technology are yet to be fully understood, researchers and practitioners may resort to

our framework to gain awareness of the existing tensions and to better understand the impact and relevance of the GDPR on the development of Blockchain applications for health tourism.

7.1. Future Work

Future research is needed to study in detail the implications of the GDPR on the different types and specific domains of Blockchains. The regulation leaves room to modify certain aspects of the GDPR in specific EU member states data protection laws, so it is necessary to assess the implications of the GDPR on healthcare in specific EU member states, as well as the implications within the different areas of practice that comprise the healthcare sector.

Although the literature identifies off-chain storage as the best approach for achieving compliance, the solution is not unanimous among all the reviewed papers, hence, a generic solution for storing personal data on Blockchain is also indispensable.

Existing and upcoming Blockchain applications should be developed with conscious awareness of the tensions and challenges mentioned in this study and focus on the commonalities between Blockchain technology and the GDPR since, in the end, both are attempting to achieve the same objectives: enhance privacy and security, and increase the users' control over their personal data.

There is a need for clarification regarding some of the principles and requirements of the GDPR, for instance the meaning of "erasure", and the introduction of new and up-to-date regulations that take emerging decentralized technologies into consideration, which will most likely guide the development of the technology and increase its adoption.

Since blockchain technology is under constant development and its full impact on health tourism practice is yet to be fully understood further research on the topic is also needed. Additionally, it is of essence to consider the implication of data protection regulations, such as GDPR, in the implementation of blockchain systems in the health tourism industry.

With the knowledge gathered from this study, it would be interesting to develop a GDPR-compliant blockchain architecture for health tourism.

Bibliography

[1] Parekh J, Jaffer A, Bhanushali U, Shukla S. Disintermediation in medical tourism through blockchain technology: an analysis using value-focused thinking approach. Information Technology and Tourism 2021; 23:69–96. https://doi.org/10.1007/s40558-020-00180-4.

[2] Rejeb A, Keogh JG, Treiblmaier H. The Impact of Blockchain on Medical Tourism. WeB2019 Workshop on E-Business 2019.

[3] Balasubramanian S, Ajayan S, Paris CM. Leveraging Blockchain in Medical Tourism Value Chain. Information and Communication Technologies in Tourism 2022 2022:78–83. https://doi.org/10.1007/978-3-030-94751-4_8.

[4] Tyan I, Guevara-Plaza A, Yagüe MI. The benefits of blockchain technology for medical tourism. Sustainability (Switzerland) 2021;13. https://doi.org/10.3390/su132212448.

[5] Riva GM. What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights. Frontiers in Blockchain 2020;3. https://doi.org/10.3389/fbloc.2020.00036.

[6] Liu L, Xu B. Research on Information Security Technology Based on Blockchain 2018.

[7] Stephano R-M. Blockchain Technology: A Total Game-Changer in Medical Tourism. Medical Tourism Magazine 2019.

[8] Al-Abdullah M, Alsmadi I, AlAbdullah R, Farkas B. Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. Digital Policy, Regulation and Governance 2020;22:389–411. https://doi.org/10.1108/DPRG-04-2020-0050.

[9] Bernal Bernabe J, Canovas JL, Hernandez-Ramos JL, Torres Moreno R, Skarmeta A. Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access 2019; 7:164908–40. https://doi.org/10.1109/ACCESS.2019.2950872.

[10] Junejo AZ, Hashmani MA, Alabdulatif AA. Blockchain Privacy Preservation by Limiting Verifying Nodes' during Transaction Broadcasting. 3rd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2021, Institute of Electrical and Electronics Engineers Inc.; 2021. https://doi.org/10.1109/ICECCE52056.2021.9514212.

[11] Vasylkovskyi V, Guerreiro S, Sequeira JS. BlockRobot: Increasing Privacy in Human Robot Interaction by Using Blockchain. Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020, Institute of Electrical and Electronics Engineers Inc.; 2020, p. 106–15. https://doi.org/10.1109/Blockchain50366.2020.00021.

[12] Campanile L, Iacono M, Marulli F, Mastroianni M. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. Inf Process Manag 2021;58. https://doi.org/10.1016/j.ipm.2021.102511.

[13] Finck M. Blockchains and Data Protection in the European Union. European Data Protection Law Review 2018; 4:17–35. https://doi.org/10.21552/edpl/2018/1/6.

[14] Wierda E, Eindhoven DC, Schalij MJ, Borleffs CJW, Amoroso G, van Veghel D, et al. Privacy of patient data in quality-of-care registries in cardiology and cardiothoracic surgery: The impact of the new general data protection regulation EU-law. Eur Heart J Qual Care Clin Outcomes 2018;4:239–45. https://doi.org/10.1093/ehjqcco/qcy034.

[15] Mustafa U, Philip N. A Novel Privacy Framework for Secure M-health Applications: The Case of the GDPR, 2019.

[16] Mocydlarz-Adamcewicz M. Effective communication between hospital staff and patients in compliance with personal data protection regulations. Reports of Practical Oncology and Radiotherapy 2021; 26:833–8. https://doi.org/10.5603/RPOR.a2021.0138.

[17] Jekova V. EU REQUIREMENTS FOR PROTECTION OF PERSONAL DATA OF PATIENTS IN HEALTH ESTABLISHMENTS. KNOWLEDGE-International Journal 2021;46.

[18] Astrup J. GDPR - THE TRANSFER OF DATA POWER 2018.

[19] Mulder T. Health Apps, their Privacy Policies and the GDPR 2019.

[20] European Society of Radiology (ESR). The new EU General Data Protection Regulation: what the radiologist should know. Insights Imaging 2017; 8:295–9. https://doi.org/10.1007/s13244-017-0552-7.

[21] Miyachi K, Mackey TK. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf Process Manag 2021;58. https://doi.org/10.1016/j.ipm.2021.102535.

[22] Webster J, Watson RT. ANALYZING THE PAST TO PREPARE FOR THE FUTURE: WRITING A LITERATURE REVIEW. vol. 26. 2002.

[23] Kitchenham B. Procedures for Performing Systematic Reviews. 2004.

[24] Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering. 2007.

[25] Garousi V, Felderer M, Mäntylä M v. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Inf Softw Technol 2019; 106:101–21. https://doi.org/10.1016/j.infsof.2018.09.006.

[26] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System 2008.

[27] Gupta M. Blockchain IBM Limited Edition. 2017.

[28] Yaga D, Mell P, Roby N, Scarfone K. Blockchain Technology Overview 2018. https://doi.org/10.6028/NIST.IR.8202.

[29] Shah SM, Khan RA. Secondary use of electronic health record: Opportunities and challenges. IEEE Access 2020; 8:136947–65. https://doi.org/10.1109/ACCESS.2020.3011099.

[30] Truong NB, Sun K, Lee GM, Guo Y. GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. IEEE Transactions on Information Forensics and Security 2020;15:1746–61. https://doi.org/10.1109/TIFS.2019.2948287.

[31] Tatar U, Gokce Y, Nussbaum B. Law versus technology: Blockchain, GDPR, and tough tradeoffs. Computer Law and Security Review 2020;38. https://doi.org/10.1016/j.clsr.2020.105454.

[32] Shu IN, Jahankhani H. The Impact of the new European General Data Protection Regulation (GDPR) on the Information Governance Toolkit in Health and Social Care with Special Reference to Primary Care in England. Proceedings - 2017 Cybersecurity and Cyberforensics Conference, CCC 2017, vol. 2018- September, Institute of Electrical and Electronics Engineers Inc.; 2017, p. 31–7. https://doi.org/10.1109/CCC.2017.16.

[33] Sousa M, Ferreira D, Santos-Pereira C, Bacelar G, Frade S, Pestana O, et al. OpenEHR based systems and the general data protection regulation (GDPR). Stud Health Technol Inform, vol. 247, IOS Press BV; 2018, p. 91–5. https://doi.org/10.3233/978-1-61499-852-5-91.

[34] van Veen E ben. Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. Eur J Cancer 2018; 104:70–80. https://doi.org/10.1016/j.ejca.2018.09.032.

[35] Mustafa U, Philip N. A Novel Privacy Framework for Secure M-health Applications: The Case of the GDPR. n.d.

[36] Georgiou D, Lambrinoudakis C. Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (Gdpr). Information (Switzerland) 2020; 11:1–19. https://doi.org/10.3390/info11120586.

[37] Jekova V. EU REQUIREMENTS FOR PROTECTION OF PERSONAL DATA OF PATIENTS IN HEALTH ESTABLISHMENTS. vol. 46. n.d.

[38] Madine MM, Battah AA, Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y, et al. Blockchain for Giving Patients Control over Their Medical Records. IEEE Access 2020; 8:193102–15. https://doi.org/10.1109/ACCESS.2020.3032553.

[39] Cernian A, Tiganoaia B, Sacala IS, Pavel A, Iftemi A. Patientdatachain: A blockchain-based approach to integrate personal health records. Sensors (Switzerland) 2020; 20:1–24. https://doi.org/10.3390/s20226538.

[40] Fang HSA, Tan TH, Tan YFC, Tan CJM. Blockchain personal health records: Systematic review. J Med Internet Res 2021;23. https://doi.org/10.2196/25094.

[41] Kim JW, Kim SJ, Cha WC, Kim T. A Blockchain-Applied Personal Health Record Application: Development and User Experience. Applied Sciences (Switzerland) 2022;12. https://doi.org/10.3390/app12041847.

[42] Salonikias S, Khair M, Mastoras T, Mavridis I. Blockchain-Based Access Control in a Globalized Healthcare Provisioning Ecosystem. Electronics (Switzerland) 2022;11. https://doi.org/10.3390/electronics11172652.

[43] Lee NY, Yang J, Onik MMH, Kim CS. Modifiable Public Blockchains Using Truncated Hashing and Sidechains. IEEE Access 2019; 7:173571–82. https://doi.org/10.1109/ACCESS.2019.2956628.

[44] Delgado-Von-eitzen C, Anido-Rifón L, Fernández-Iglesias MJ. Application of blockchain in education: GDPR-compliant and scalable certification and verification of academic information. Applied Sciences (Switzerland) 2021;11. https://doi.org/10.3390/app11104537.

[45] Rotondi D, Saltarella M, Giordano G, Pellecchia F. Distributed ledger technology and European Union General Data Protection Regulation compliance in a flexible working context. Internet Technology Letters 2019;2: e127. https://doi.org/10.1002/itl2.127.

[46] Millard C. Blockchain and law: Incompatible codes? Computer Law and Security Review 2018; 34:843–6. https://doi.org/10.1016/j.clsr.2018.06.006.

[47] Molina F, Betarte G, Luna C. Design principles for constructing GDPR-compliant blockchain solutions. Proceedings - 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain, WETSEB 2021, Institute of Electrical and Electronics Engineers Inc.; 2021, p. 1–8. https://doi.org/10.1109/WETSEB52558.2021.00008.

[48] Nuansanong J, Kiattisin S. The electronic medical record exchange using a Blockchain technology. Songklanakarin J Sci Technol 2021; 43:335–43.

[49] Teperdjian R. THE PUZZLE OF SQUARING BLOCKCHAIN WITH THE GENERAL DATA PROTECTION REGULATION 2020;60.

[50] Mahindrakar A, Joshi KP. Automating GDPR Compliance using Policy Integrated Blockchain. 2020.

[51] Wang Z, Luo N, Zhou P. GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare. J Parallel Distrib Comput 2020; 142:1–12. https://doi.org/10.1016/j.jpdc.2020.03.004.

[52] Mamo N, Martin GM, Desira M, Ellul B, Ebejer JP. Dwarna: a blockchain solution for dynamic consent in biobanking. European Journal of Human Genetics 2019; 28:609–26. https://doi.org/10.1038/s41431-019-0560-9.

[53] Subramanian HC, Cousins KC, Bouayad L, Sheth A, Conway D, Salcedo E, et al. Blockchain regulations and decentralized applications: Panel report from amcis 2018. Communications of the Association for Information Systems 2020; 47:189–206. https://doi.org/10.17705/1CAIS.04709.

[54] Munier L, Kemball-Cook A. Blockchain and the General Data Protection Regulation: Reconciling protection and innovation. vol. 11. 2019.

[55] Konkin A, Zapechnikov S. Techniques for Private Transactions in Corporate Blockchain Networks. Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021, Institute of Electrical and Electronics Engineers Inc.; 2021, p. 2356–60. https://doi.org/10.1109/ElConRus51938.2021.9396228.

[56] Qian J, Wu W, Yu Q, Ruiz-Garcia L, Xiang Y, Jiang L, et al. Filling the trust gap of food safety in food trade between the EU and China: An interconnected conceptual traceability framework based on blockchain. Food Energy Secur 2020;9. https://doi.org/10.1002/fes3.249.

[57] Yang X, Li T, Pei X, Wen L, Wang C. Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology. IEEE Access 2020; 8:45468–76. https://doi.org/10.1109/ACCESS.2020.2976894.

[58] Zheng X, Mukkamala RR, Vatrapu R, Ordieres-Mere J. Blockchain-based personal health data sharing system using cloud storage. 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, Healthcom 2018, Institute of Electrical and Electronics Engineers Inc.; 2018. https://doi.org/10.1109/HealthCom.2018.8531125.

[59] Al-Karaki JN, Gawanmeh A, Ayache M, Mashaleh A. DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain, IEEE; 2019.

[60] Herian R. Blockchain, GDPR, and fantasies of data sovereignty. Law Innov Technol 2020; 12:156–74. https://doi.org/10.1080/17579961.2020.1727094.

[61] Zhang JS, Xu G, Chen XB, Ahmad H, Liu X, Liu W. Towards privacy-preserving cloud storage: A blockchain approach. Computers, Materials and Continua 2021;69:2903–16. https://doi.org/10.32604/cmc.2021.017227.

[62] Alboaie S, Ursache NC, Alboaie L. Self-sovereign applications: Return control of data back to people. Procedia Comput Sci, vol. 176, Elsevier B.V.; 2020, p. 1531–9. https://doi.org/10.1016/j.procs.2020.09.164.

[63] Zemler F, Westner M. Blockchain and GDPR Application Scenarios and Compliance Requirements 2019.

[64] Al-Zaben N, Mehedi Hassan Onik M, Yang J, Lee N-Y, Kim C-S. General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management, 2018.

[65] Nuansanong J, Kiattisin S. The electronic medical record exchange using a Blockchain technology. vol. 43. n.d.

[66] Wang S, Zhang Y, Zhang Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access 2018; 6:38437–50. https://doi.org/10.1109/ACCESS.2018.2851611.

[67] Satamraju KP, Malarkodi B. A decentralized framework for device authentication and data security in the next generation internet of medical things. Comput Commun 2021; 180:146–60. https://doi.org/10.1016/j.comcom.2021.09.012.

[68] Vasylkovskyi V, Guerreiro S, Sequeira JS. Designing and Validating a Blockchain-based Architecture to Enforce Privacy in Human Robot Interaction, 2021.

[69] Chico V. The impact of the general data protection regulation on health research. Br Med Bull 2018; 128:109–18. https://doi.org/10.1093/bmb/ldy038.

[70] Molnár-Gábor F, Sellner J, Pagil S, Slokenberga S, Tzortzatou-Nanopoulou O, Nyström K. 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 2021. https://doi.org/10.1016/j.semcancer.2021.12.001.

[71] Todde M, Beltrame M, Marceglia S, Spagno C. Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. Inform Med Unlocked 2020;19. https://doi.org/10.1016/j.imu.2020.100361.

[72] Georgiou D, Lambrinoudakis C. Data protection impact assessment (DPIA) for cloud-based health organizations. Future Internet 2021; 13:1–12. https://doi.org/10.3390/fi13030066.

[73] Muchagata J, Ferreira A. Translating GDPR into the mHealth Practice, 2018.

[74] Flaumenhaft Y, Ben-Assuli O. Personal health records, global policy and regulation review. Health Policy (New York) 2018; 122:815–26. https://doi.org/10.1016/j.healthpol.2018.05.002.

[75] Demotes-Mainard J, Cornu C, Guérin A, Bertoye PH, Boidin R, Bureau S, et al. How the new European data protection regulation affects clinical research and recommendations? Therapie 2019;74:17–29. https://doi.org/10.1016/j.therap.2018.11.008.

[76] Georgiou D, Lambrinoudakis C. Compatibility of a security policy for a cloud-based healthcare system with the eu general data protection regulation (Gdpr). Information (Switzerland) 2020; 11:1–19. https://doi.org/10.3390/info11120586.

[77] Mendelson D. The European Union General Data Protection Regulation (EU 2016679) and the Australian My Health Record Scheme - A Comparative Study of Consent to Data Processing Provisions 2018:23–38.

[78] Agbo CC, Mahmoud QH. Design and Implementation of a Blockchain-Based E-Health Consent Management Framework. Conf Proc IEEE Int Conf Syst Man Cybern, vol. 2020- October, Institute of Electrical and Electronics Engineers Inc.; 2020, p. 812–7. https://doi.org/10.1109/SMC42975.2020.9283203.

[79] Crowhurst N, Bergin M, Wells J. Implications for nursing and healthcare research of the general data protection regulation and retrospective reviews of patients' data 2019.

[80] Comandè G, Schneider G. Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of "Health Data." Eur J Health Law 2018; 25:284–307. https://doi.org/10.1163/15718093-12520368.

[81] van Veen E ben. Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. Eur J Cancer 2018; 104:70–80. https://doi.org/10.1016/j.ejca.2018.09.032.

[82] Rajam N. Policy strategies for personalising medicine "in the data moment." Health Policy Technol 2020; 9:379–83. https://doi.org/10.1016/j.hlpt.2020.07.003.

[83] Kirwan M, Mee B, Clarke N, Tanaka A, Manaloto L, Halpin E, et al. What GDPR and the Health Research Regulations (HRRs) mean for Ireland: "explicit consent"—a legal analysis. Irish Journal of Medical Sciences 2020. https://doi.org/10.1007/s11845-020-02331-2/Published.

[84] Nurgalieva L, O'Callaghan D, Doherty G. Security and Privacy of mHealth Applications: A Scoping Review. IEEE Access 2020; 8:104247–68. https://doi.org/10.1109/ACCESS.2020.2999934.

[85] Shu IN, Jahankhani H. The Impact of the new European General Data Protection Regulation (GDPR) on the Information Governance Toolkit in Health and Social Care with Special Reference to Primary Care in England. Proceedings - 2017 Cybersecurity and Cyberforensics Conference, CCC 2017, vol. 2018- September, Institute of Electrical and Electronics Engineers Inc.; 2017, p. 31–7. https://doi.org/10.1109/CCC.2017.16.

[86] Chico V. The impact of the general data protection regulation on health research. Br Med Bull 2018; 128:109–18. https://doi.org/10.1093/bmb/ldy038.

[87] Balasubramanian S, Ajayan S, Paris CM. Leveraging Blockchain in Medical Tourism Value Chain. Information and Communication Technologies in Tourism 2022, Springer International Publishing; 2022, p. 78–83. https://doi.org/10.1007/978-3-030-94751-4_8.

[88] Meier P, Beinke JH, Fitte C, Schulte to Brinke J, Teuteberg F. Generating design knowledge for blockchain-based access control to personal health records. Information Systems and E-Business Management 2021;19:13–41. https://doi.org/10.1007/s10257-020-00476-2.

[89] Alam S, Reegu FA, Mohd S, Hakami Z, Reegu KK. Towards Trustworthiness of Electronic Health Record system using Blockchain. Ann Rom Soc Cell Biol 2021; 25:2425–34.

[90] Tandon A, Dhir A, Islam N, Mäntymäki M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Comput Ind 2020;122. https://doi.org/10.1016/j.compind.2020.103290.

[91] Leeming G, Cunningham J, Ainsworth J. A Ledger of Me: Personalizing Healthcare Using Blockchain Technology. Front Med (Lausanne) 2019;6. https://doi.org/10.3389/fmed.2019.00171.

[92] Zubaydi HD, Chong YW, Ko K, Hanshi SM, Karuppayah S. A review on the role of blockchain technology in the healthcare domain. Electronics (Switzerland) 2019;8. https://doi.org/10.3390/electronics8060679.

[93] Goel P. Is blockchain the solution for failing global healthcare? World Economic Forum 2022. https://www.weforum.org/agenda/2022/09/blockchain-solution-for-failing-global-healthcare/.

[94] Gretzel U, Stankov U. ICTs and well-being: challenges and opportunities for tourism. Information Technology and Tourism 2021;23. https://doi.org/10.1007/s40558-021-00198-2.

[95] Shen Y, Bai G. Research on Application of Blockchain in Internationalization of China's Medical Tourism Industry*. Proceedings - 2020 International Signal Processing, Communications and Engineering Management Conference, ISPCEM 2020, Institute of Electrical and Electronics Engineers Inc.; 2020, p. 63–7. https://doi.org/10.1109/ISPCEM52197.2020.00018.

[96] Roehrs A. OmniPHR: A Blockchain based Interoperable Architecture for Personal Health Records. 2019.

[97] Wang S, Zhang D, Zhang Y. Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable. IEEE Access 2019; 7:102887–901. https://doi.org/10.1109/ACCESS.2019.2931531.

[98] Lee YL, Lee HA, Hsu CY, Kung HH, Chiu HW. SEMRES - A Triple Security Protected Blockchain Based Medical Record Exchange Structure. Comput Methods Programs Biomed 2022;215. https://doi.org/10.1016/j.cmpb.2021.106595.

[99] Mahalingam R, Ahmad Ahanger W. New technologies - BlockChain as a Service (BCaaS) for healthcare. Journal of Emergency Medicine, Trauma and Acute Care, vol. 2020, Hamad bin Khalifa University Press (HBKU Press); 2020. https://doi.org/10.5339/jemtac.2020.qhc.15.

[100] Ghani A, Zinedine A, el Mohajir M. A blockchain-based secure PHR data storage and sharing framework. Colloquium in Information Science and Technology, CIST, vol. 2020- June, Institute

of Electrical and Electronics Engineers Inc.; 2020, p. 162–6. https://doi.org/10.1109/CiSt49399.2021.9357318.

[101] Subasinghe M, Magalage D, Amadoru N, Amarathunga L, Bhanupriya N, Wijekoon JL. Effectiveness of artificial intelligence, decentralized and distributed systems for prediction and secure channelling for Medical Tourism. 11th Annual IEEE Information Technology, Electronics and Mobile Communication Conference, IEMCON 2020, Institute of Electrical and Electronics Engineers Inc.; 2020, p. 314–9. https://doi.org/10.1109/IEMCON51383.2020.9284898.

[102] Misbhauddin M, Alabdulatheam A, Aloufi M, Al-Hajji H, Alghuwainem A. MedAccess: A Scalable Architecture for Blockchain-based Health Record Management. 2020 2nd International Conference on Computer and Information Sciences, ICCIS 2020, Institute of Electrical and Electronics Engineers Inc.; 2020. https://doi.org/10.1109/ICCIS49240.2020.9257720.

[103] Zhang L, Zhang T, Wu Q, Mu Y, Rezaeibagha F. Secure Decentralized Attribute-Based Sharing of Personal Health Records with Blockchain. IEEE Internet Things J 2022; 9:12482–96. https://doi.org/10.1109/JIOT.2021.3137240.

[104] Wang Y, Zhang A, Zhang P, Qu Y, Yu S. Security-Aware and Privacy-Preserving Personal Health Record Sharing Using Consortium Blockchain. IEEE Internet Things J 2022; 9:12014–28. https://doi.org/10.1109/JIOT.2021.3132780.