IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 14 February 2024, accepted 14 May 2024, date of publication 28 May 2024, date of current version 18 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3406724

TOPICAL REVIEW

Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions

NEMER ALBERTO ZAGUIR, GUILHERME HENRIQUE DE MAGALHÃES, AND MAURO DE MESQUITA SPINOLA

Department of Production Engineering, University of São Paulo, São Paulo 05508-010, Brazil

Corresponding author: Nemer Alberto Zaguir (nemer.zaguir@usp.br)

ABSTRACT Compliance with the General Data Protection Regulation (GDPR) or related laws by organizations could require organizational and technological changes. This topic has gained significant attention from management and scholars alike. Although the literature presents some reviews and research articles discussing challenges and enablers for GDPR compliance, they are often scattered and fragmented. One particular challenge is the implementation roadmap gap that arises when using ISO-based standards for compliance in isolation. On the other hand, as enablers for compliance, it raises the potential use of information governance (IG) and enterprise architecture management (EAM) disciplines. This research aims to provide a systematic literature review of the challenges and enablers for GDPR compliance and address this gap. The findings include a categorized list of challenges and enablers, a strategy for bridging the roadmap gap using IG and EAM, and the development of five propositions based on some challenges and enablers around this gap. Moreover, the study proposes a research agenda that includes conceptual work to build an IG-EAM framework, empirical research to verify those propositions, and developing new hypotheses stemming from the review's challenges and enablers. These contributions enhance the body of knowledge providing practical insights for organizations striving for GDPR compliance.

INDEX TERMS Challenges, enablers, enterprise architecture management, GDPR, general data protection regulation, information governance, privacy, systematic literature review.

I. INTRODUCTION

The evolution of the debate on the right of individuals to the legal protection of their private life originates in the late 19th century, motivated by the seminal article by Warren and Brandeis [1]. The authors suggest that the advent of new technologies, such as instant photographs and the popularization of newspapers, can invade family spaces and jeopardize the privacy of others. This work served as the basis for Article 12 of the Declaration of Human Rights [2], which explained the right to privacy and became a pillar of all future milestones until the creation of the GDPR [3].

With the increased technological resources for data collection and the significantly low price and potentially limitless cloud storage, organizations may store massive amounts of personally Identifiable Information (PII) and use this as a source of revenue [4], [5]. Companies that were born digital, such as Google, Netflix, Airbnb, Amazon, and Uber, with the use of Big Data and Artificial Intelligence (AI), can process a high volume of data, obtaining trends and insights to expand their scope with new products, markets and services and scale the business at a much higher speed than in traditional companies [4], [5], [6]. However, traditional companies have already adopted and pursued these characteristics by digitalizing their services and products, significantly raising PII relevance [6]. Organizations have inherent security challenges and risks in this context, making them vulnerable to privacy breaches [7]. In environments with Big Data, even anonymized PII can be re-identified, threatening the privacy of individuals [8]. This scenario, where technology enables and plays a crucial

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamed Elhoseny.

role in today's business transformations, raises the need to understand the challenges and enabling factors for GDPR compliance.

Many review articles have been published about the GDPR. Some articles, such as those by Teixeira, Silva, and Pereira [9] and [10], focus on the critical success factors for GDPR compliance implementation, also discussed by Fernandes et al. [125] for higher education institutions. Others, like those by Bernabe et al. [11] and Haque et al. [12], explore the relationship between GDPR and blockchain technology. Kounoudes and Kapitsaki [13], on the other hand, delve into the compliance issues related to data security that arise from the use of Internet of things (IoT)-based applications, and there are numerous other reviews on how GDPR affects various fields like medicine, social science, and engineering.

In addition to the comprehensive reviews, several articles indicate the gap in achieving compliance using ISO-based standards and suggest complementing them [33], [39]. Alternatively, some articles discuss the potential use of IG and EAM disciplines to enable GDPR compliance [41], [42], [43], [44], [45], [46]. Additionally, specific questions are addressed in other articles, such as legal matters, data protection, technology use, challenges related to consent and transparency in data subject (DS) rights, recording of processing activities, and data sharing. Therefore, this review aims to compile state-of-the-art literature regarding the challenges and enablers for implementing and maintaining compliance addressing the implementation roadmap gap with a fresh perspective and novel research questions.

After this introduction, the next topic provides the GDPR background, and the third outlines the applied Systematic Literature Review (SLR) method, featuring six research questions. The fourth topic shows the results, addressing five of the questions above. The fifth topic discusses these results, presenting five propositions and providing an answer to the sixth question by suggesting a research agenda. Lastly, the conclusion covers research limitations and highlights the contributions to management and the overall body of knowledge about challenges and enablers for GDPR compliance.

II. BACKGROUND

This topic shows the privacy timeline till the GPDR comes into effect, describes general aspects of GDPR structure and concepts used in this review, and illustrates some initial challenges of GDPR compliance from a review article.

A. PRIVACY TIMELINE

Fig. 1 shows the timeline with the main events around the privacy concepts and their dissemination. It starts with the seminal article from Warren and Brandeis [1] going through events sponsored by entities like the United Nations (UN) and the Council of Europe (CoE), which act as a guardian of human rights and the rule of law in Europe; the Organization for Economic Co-operation and Development (OECD); and the bicameral legislative branch of the European Union (EU)

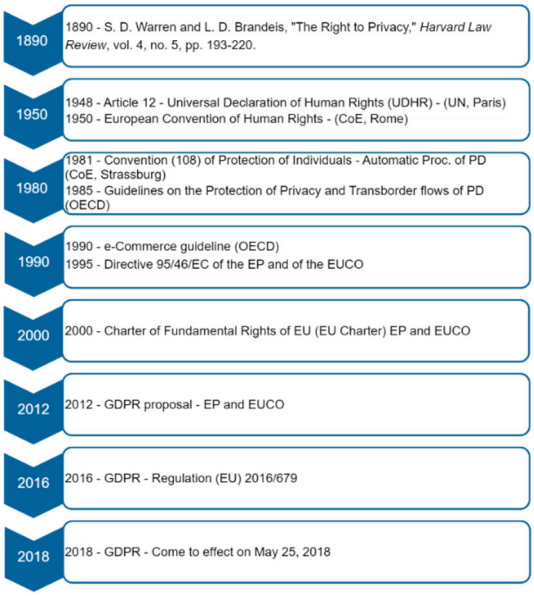

FIGURE 1. Timeline of privacy and data protection events.

formed by the European Parliament (EP), and the council of EU (EUCO), governed by the Treaty on the Functioning of the EU (TFEU) that contains the specific provisions about the Union institutions and policies.

Privacy protection in Europe has traditionally been strong for historical, cultural, political, and legal reasons, placing the GDPR in a leading position as the most comprehensive privacy regime [14]. Greenleaf [15] identified that by March 2023, 162 countries had data protection legislation, and 20 others had bills in progress, all firmly based on the GDPR. The author suggests that countries without such laws will develop them this decade, making these laws ubiquitous worldwide.

B. GDPR

GDRP is the regulation (EU) 2016/679 of the EP and of the EUCO of April 27, 2016, and came into effect on May 25, 2018. The GDPR is related to Article 8(1) of the Charter of Fundamental Rights of the EU and Article 16(1) of the TFEU, which provides that everyone has the right to the protection of PII concerning them. The principles and rules on the protection of natural persons concerning the processing of their data should, whatever their nationality or residence, respect their fundamental rights and freedoms, particularly their right to protect their data. This regulation aims to accomplish freedom, security, justice, an economic union, economic and social progress, strengthening and convergence of the economies within the internal market, and the well-being of natural persons. Although GDPR only protects EU citizens, it has a global impact on any organization targeting the European market or holding PII on EU residents [116]

To ensure compliance, organizations must adhere to the 11 chapters and 99 articles that make up the GDPR. The 173 recitals offer additional context to complement the articles

and are relied upon by the European Data Protection Board for interpretation. The Court of Justice of the EU reviews the recitals to determine the meaning and application of the GDPR.

Article 4 of the GDPR's first chapter, General Provisions, provides key concepts that could be helpful during this review, such as personal data (PD), processing, restriction of processing, profiling, pseudonymization, filing system, controller, processor, recipient, third party, consent, PD breach, genetic data, biometric data, data concerning health, and DS.

The second chapter outlines six principles related to the processing of PD. Article 6 explains the lawfulness of processing, and Article 7 details the conditions for consent. Articles 8 to 11 cover the requirements applicable to particular categories of PD. The third chapter, The Right of DS, groups articles 12 to 27 into five sections. The first section, ''Transparency and modalities,'' contains Article 12, which addresses the transparent information, communication, and modalities for exercising the rights of the DS. Article 13 provides information on the details that should be provided when collecting personal data from the DS.

C. INITIAL CHALLENGES TO GDPR COMPLIANCE

As supervisory authorities may impose sanctions whenever non-compliance is detected, organizations must review their processes and procedures to ensure they collect, hold, and process PD following the regulation [17]. Besides technological challenges regarding data protection, GDPR brings a lot of juridical and functional changes, along with the need to educate staff and change their mindset and culture to this new paradigm [18].

Teixeira, Silva, and Pereira [9] conclude that the barriers or challenges to adapting organizations to GDPR start with the regulation itself, as it is complex, extensive, and involves subjectivity. The compliance process is extensive, time-consuming, and requires substantial financial and human resources. The lack of privacy knowledge and expertise, the technology necessary, and practical guides or standard procedures are also barriers to reaching compliance. They found that the most challenging requirements to comply with GDPR are the right to erasure, recording processing activities, implementing data protection by design and default, and designating a Data Protection Officer (DPO).

Based on the results from the initial review, these authors identified and prioritized challenges to GDPR compliance and enablers, seeking consensus of a group opinion by surveying a panel of 21 DPOs from organizations in Portugal through the Delphi method [10].

Table 1 lists the challenges of GDPR implementation based on Teixeira, Silva, and Pereira [9]. Each line in Table 1 is identified with ''Cn,'' where ''n'' represents a sequential number in the table. Additional challenges from this review are listed accordingly, and the third column of the table features a classification system developed by the authors. Other reviews discuss challenges to GDPR compliance and enablers from different points of view and objectives. Additionally, many other articles discuss particular aspects of GDPR compliance, enforcing the purpose of this review.

TABLE 1. Challenges of GDPR implementation.

GDPR implementation challenges	Authors	Classifications
C1. GDPR does not provide specific guidelines regarding technologies that should be used to comply with its requirements.	[17]	Lack of technology Lack of guidelines
C2. GDPR does not provide specific guidelines to implement it and involves subjectivity.	[7]	GDPR subjectivity Lack of guidelines
C3. GDPR compliance may be expensive and time consuming as it requires substantial financial and human resources.	[17], [19]	GDPR extension Lack of budget
C4. GDPR compliancy increase administrative work.	[20]	Increase work
C5. Designating an inside DPO is also a challenge as it is difficult to recruit and retain people with these skills.	[17], [21]	Lack of human resources
C6. The lack of privacy knowledge and expertise inside organizations may also require extra budget to recruit privacy experts and increase business costs.	[22]	Lack of budget Lack of human resources
C7. Requires changes and technology to leads with complexity process to comply with the right to erasure, with the recording of processing activities and with data protection by design and by default.	[23]	GDPR complexity Lack of technology to comply with some GDPR requirements
C8. The GDPR may lead some organizations to reduce their product offering to European citizens to step away from the regulation.	[24]	Reduce product offering
C9. Owing to all the regulatory restrictions of GDPR, compliance may also decrease organization's performance.	[25]	Reduce organization´s performance

III. METHOD

This study employs a Systematic Literature Review (SLR) methodology. According to Webster and Watson [26], a well-executed literature review serves as a factual foundation for knowledge advancement, promotes theoretical development, enables the analysis and synthesis of high-quality literature, provides insight into existing research and its interrelationships, supports future research, and determines whether a research contribution adds value to the subject's knowledge base.

Levy and Ellis [27] outline a systematic review process that follows the input-processing-output model, utilizing the effective review model proposed by Webster and Watson [26]. Each phase of the process has sequential steps and guidelines to ensure traceable, replicable, and reliable outcomes. Meanwhile, Kitchenham and Charters [28] recommend three phases for conducting an SLR: planning, execution, and summary. They also provide detailed procedures for constructing an SLR protocol during the planning phase.

In Topic A, we present a roadmap for the planning phase to develop the protocol, as demonstrated in Topic B. To conduct this SLR, we use the StArt tool, which is a proven and

TABLE 2. Phase I roadmap.

Roadmap for SLR protocol definition
1) Define the objective and research questions.
2) Choose academic databases and publication sources.
3) Generate search strategy: keywords and search key.
4) Studies identification, selection, and extraction.
5) Guidelines for bibliometric studies.
6) Strategy to perform the content analysis.
7) Compile the SLR protocol.

efficient tool that supports the entire SLR process [29]. This tool streamlines the selection of eligible studies by assigning scores to articles, taking into account the frequency of search term occurrences in the title, abstract, and keywords. The StArt tool is open source and available at http://lapes.dc.ufscar.br/tools/start_tool.

The study's methodological limitations include potential bias in the selection of studies that influences the number of articles in the final sample, gaps in the databases used that do not cover all relevant publications on the topic, dependence on automated tools, and the researchers; subjective interpretation.

A. PHASE I – SLR PLANNING

During this phase, a set of activities is carried out to identify qualified publications and determine methods to prevent incomplete or inadequate samples [27]. Once the academic databases have been selected, three search techniques are recommended, as outlined by Webster and Watson [26]: conducting keyword-based searches for papers in the chosen databases; conducting backward searches in the previous literature using the reference lists of found works, and conducting forward searches in the literature for works that cite the outcomes found. Wohlin [30] referred to this sampling technique as ''snowballing'' and presented evidence of its successful application in replicating a published study, underscoring the reliability of this approach. A roadmap for this phase is presented in Table 2.

B. PHASE I – SLR PROTOCOL

This topic follows the route proposed in Table 2 resulting in the research protocol. This protocol is also available in the form of an electronic file generated by StArt that provides other reports about this SLR. The first, second and third steps were carried out and documented in this section. The results of the execution of further steps are documented in the results section.

1) DEFINE THE OBJECTIVE AND RESEARCH QUESTIONS

The objective of this SLR is to compile state-of-the-art literature regarding the challenges and enablers for implementing and maintaining compliance. This objective was broken-down in six research questions:

RQ1 - How have GDPR implementation discussion progressed in the literature? What are the most prominent journals, articles and authors that debate the theme?

RQ2 - What are the subject areas that are relevant to GDPR compliance?

RQ3 - Which references or models have been applied to reach the GDPR compliance? Is there any gap?

RQ4 - What are the challenges and enablers for GDPR compliance?

RQ5 - What are the technologies and their characteristics that can generate negative impacts on compliance with GDRP? And what are the ones that promote positive impacts?

RQ6 - What gaps exist in current research about challenges and enabler of GDPR compliance that future research can investigate?

2) CHOOSE ACADEMIC DATABASES AND PUBLICATION SOURCES

The indexed databases chosen were the Web of Science Core Collection™ (WoS), and Scopus® from Elsevier BV. They have search tools for different publications and provide data about their references and the works cited. These databases calculate and offer essential indicators for evaluating publications, such as JCR (Journal Citation Report) and SJR (SCImago Journal Rank) [31].

3) GENERATE SEARCH STRATEGY: KEYWORDS AND SEARCH KEY

This step aims to define the terms to compose the search key. Selected documents must contain these terms in the title, abstract, or keywords. After simulations and debates with some RSL experts, the search key was defined to obtain only journal articles in English or Portuguese about GDPR or LGPD *(Lei Geral de Proteção de Dados)* the brazilian data protection law, regarding implementation, deployment, adoption, and compliance. Therefore, the following search key was used in both databases:

- (GDPR OR LGPD) AND (impl* OR deploy* OR ado* OR complia* OR conform*) Article or Review Article restricted to English or Portuguese languages from 2014 till Dec. 31, 2023.
- The symbol ''*'' in the sentence allows you to obtain similar terms in English and Portuguese, such as adoption or ''*adoção*'', implementation or ''*implementação*'', and conformance or ''*conformidade*.''

The inclusion of the LGPD had the exploratory purpose of adding other legislation in addition to the GPDR and because it is the domain of the authors.

4) STUDIES IDENTIFICATION, SELECTION AND EXTRACTION

The purpose of this process is to choose relevant studies for content analysis. Fig. 2 shows the four-step process. The symbols on the right column represent the database icons (WoS and Scopus), automated activity (gear), manual activity (saw), a filter for the initial stages of selection (larger filter), filtering through the complete reading (smaller filter), and analysis for extraction (microscope).

The first step initiates using the native tools of the WoS and Scopus databases (1.1) to obtain a set of article metadata that includes title, abstract, keywords, references, and others to be uploaded to StARt (1.2).

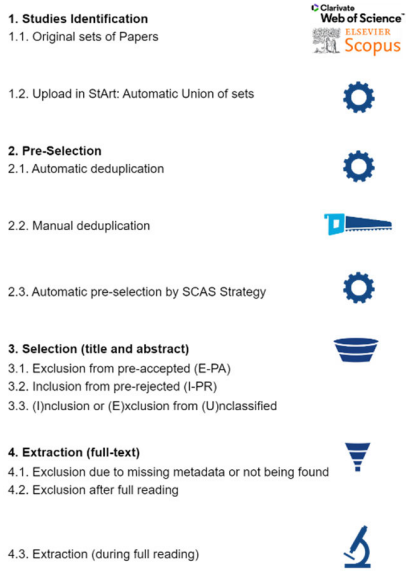

FIGURE 2. From original sets of papers to extraction.

In the second step, StArt automatically combines the data and removes some duplicate articles (2.1). However, it is necessary to manually remove the remaining ones (2.2). Additionally, StArt offers a semi-automatic ''snowball'' process that analyzes articles from previous literature. Whereas the tool does not automatically find articles from subsequent literature, it is possible to manually include them in this process. StArt facilitates a semi-automatic pre-selection of studies based on inclusion and exclusion criteria using the SCAS (Score Citation Automatic Selection) strategy (2.3).

Fabbri et al. [29] described the SCAS strategy to automate the initial selection in SLR based on two characteristics calculated for each study: the score and the number of citations. When combined, studies are classified into four quadrants. The first quadrant includes studies with high scores and at least one citation. The second quadrant comprises studies that have high scores but no citations. The third quadrant contains studies that have low scores and at least one citation. Finally, the fourth quadrant includes studies with low scores and no citations. The score is calculated based on keywords that are defined in the protocol. These keywords are found in the title, abstract, or keywords available in the union of sets. The score is essential as it provides the ranking of studies according to their supposed relevance to the context of the SLR. This pre-selection step with StArt improves the quality and drastically optimizes the time to perform this entire process.

During the third step, the authors review the results of the previous one, excluding articles that were pre-selected by StArt in quadrant 1 (3.1). They also include articles that were rejected in quadrant 4 (3.2). They may also contain or exclude articles that were unclassified by StArt in quadrant 3 or 4 (3.3).

In the fourth step, the full text of selected articles should be obtained for extraction. This step applied the quality criteria for content analysis. In some cases, the article may not have enough metadata, or it may not be accessible by the authors and should be rejected (4.1). During the entire reading, the article should also be rejected if it is not relevant to the context of the research (4.2). If the article is appropriate for research purposes, a new register in the extraction form should be documented accordingly (4.3).

Fig. 3 illustrates the results execution of these processes. From the initial sample from WoS and Scopus, 83 works were extracted to provide the bibliometric studies and content analysis.

It should be noted that the number of articles in WoS and Scopus regarding LGPD was about 2% in both situations. The extracted sample has only two articles about LGPD [77] and [79], and no one in Portuguese.

5) GUIDELINES FOR BIBLIOMETRIC STUDIES

Bibliometric studies aim to answer the RQ1 by providing information on the number of publications and citations over a specific period of time, as well as the ranking of publications and the most notable authors.

6) STRATEGY TO PERFORM THE CONTENT ANALYSIS

The extraction process uses a form based on an Excel table generated by StArt, which is then supplemented with other fields. This form records essential information from the text content, making it easier to conduct a comparative analysis, discover patterns, and synthesize data in order to answer the further RQ. Any blank fields that are not automatically populated are completed during the full reading. Some of the form columns are article title, authors, journal, year, StArt Score, StArt quadrant, reading a priority, research method, research question, implementation framework, technology discussed, the impact of the technology, consents, transparency, challenge, enabler, contribution, research gaps, and future research indication.

7) COMPILE THE SLR PROTOCOL

StArt provided automatic reports that helped build the research protocol above. This protocol allows this SLR replication and was used to provide the results in the next section.

IV. RESULTS

This topic aims to answer the research questions from RQ1 to RQ5. Section A describes the answer to RQ1 about bibliometric study using the fifth step from the protocol. Further sections describe the answers to the RQ2 to RQ5, considering the content analysis strategy described in the sixth step of the protocol. The RQ6 is answered in the discussion of results topic.

A. RQ1 - HOW HAVE GDPR IMPLEMENTATION DISCUSSION PROGRESSED IN THE LITERATURE? WHAT ARE THE MOST PROMINENT JOURNALS, ARTICLES AND AUTHORS THAT DEBATE THE THEME?

Fig. 4 exhibits the times cited and publications from the original 744 documents from WoS executed on Dec. 31, 2023. The 991 publications from Scopus have a similar profile.

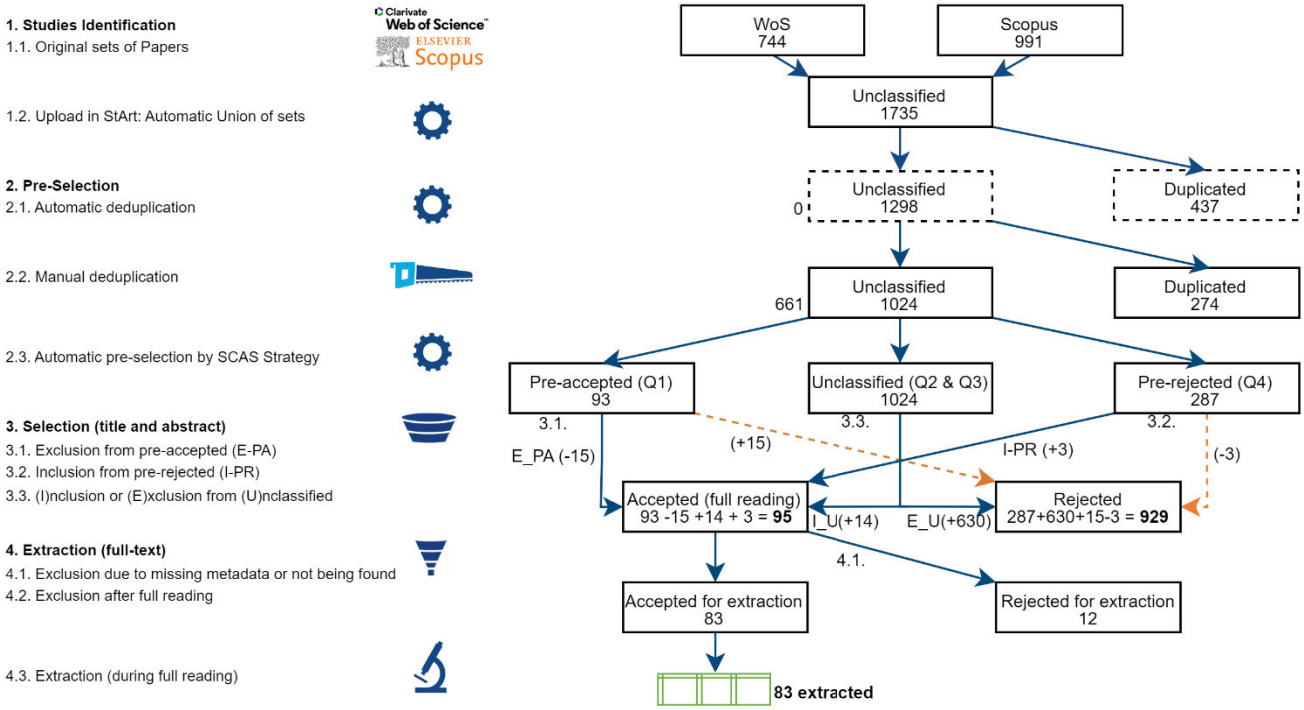

FIGURE 3. Studies identification, selection, and extraction.

This graph indicates a rise in articles from 2017 to 2020, with a stabilization afterward. However, the increase in citations since 2017 suggests sustained academic interest in the theme, answering how the GDPR implementation discussion progressed in the literature.

Tables 3 and 4 were constructed based on the sample that contains the 83 extracted articles listed in the spreadsheet available in Appendix and information from WoS e Scopus databases about these articles.

Table 3 provides insights into the leading journals that discuss the theme, highlighting the Computer Law and Security Review (CLSR) and IEEE Access. The sample of 83 articles was published in 59 periodicals, suggesting a broad academic interest in this theme.

The citation columns for WoS and Scopus show the total number of citations received by all articles published by each journal. The rankings are sorted by Scopus citation figure. To sort by WoS citation, remove positions 4 and 5, and swap 8 and 9.

Table 4 shows the top 10 most cited articles sorted by descending order by Scopus, highlighting some review articles and articles published in the period of 2018 till 2021, and the authors of each paper.

After reviewing the original WoS and Scopus samples, we observed the authors who published the most on the topic, with up to six articles, namely Alepis, E., Malgieri, G., Patsakis, C., Politou, E. All of them have earned a spot in the top 10 of the selected sample, indicating a remarkable correlation between these data sets and a noteworthy work by them.

B. RQ2 - WHAT ARE THE SUBJECT AREAS THAT ARE RELEVANT TO GDPR COMPLIANCE?

According to protocol step six, content analysis strategies can aid in comparative analysis and pattern discovery. This was executed on 83 articles using an extraction spreadsheet to group the subjects covered.

A classification of subjects was proposed, divided into five categories, with each article being associated with multiple categories. The GOV category covers IG compliance, EAM, ISO-based standards for GDPR compliance, implementation roadmaps, and general challenges and enablers in compliance projects.

The DSR-C and DSR-T categories are related to data subject rights involving consent and transparency, highlighting challenges and enablers in the DS-controller relationship.

The MISC category includes articles on compliance with regulations in various countries, the GDPR's relationship with innovation, and the Data Protection Impact Assessment (DPIA), among others.

The technology category was divided into seven subcategories, six of which relate to specific technologies such as Blockchain (BC), Internet of Things (IoT), and Artificial Intelligence (AI) as a threat or enabler for compliance. The seventh subcategory (T_O) is for papers discussing other technologies. Big data technologies could be part of the discussion in all subcategories and are also included in the T_O category. Table 5 displays the categories and the number of documents (Doc) found in the 83 extracted sets of articles.

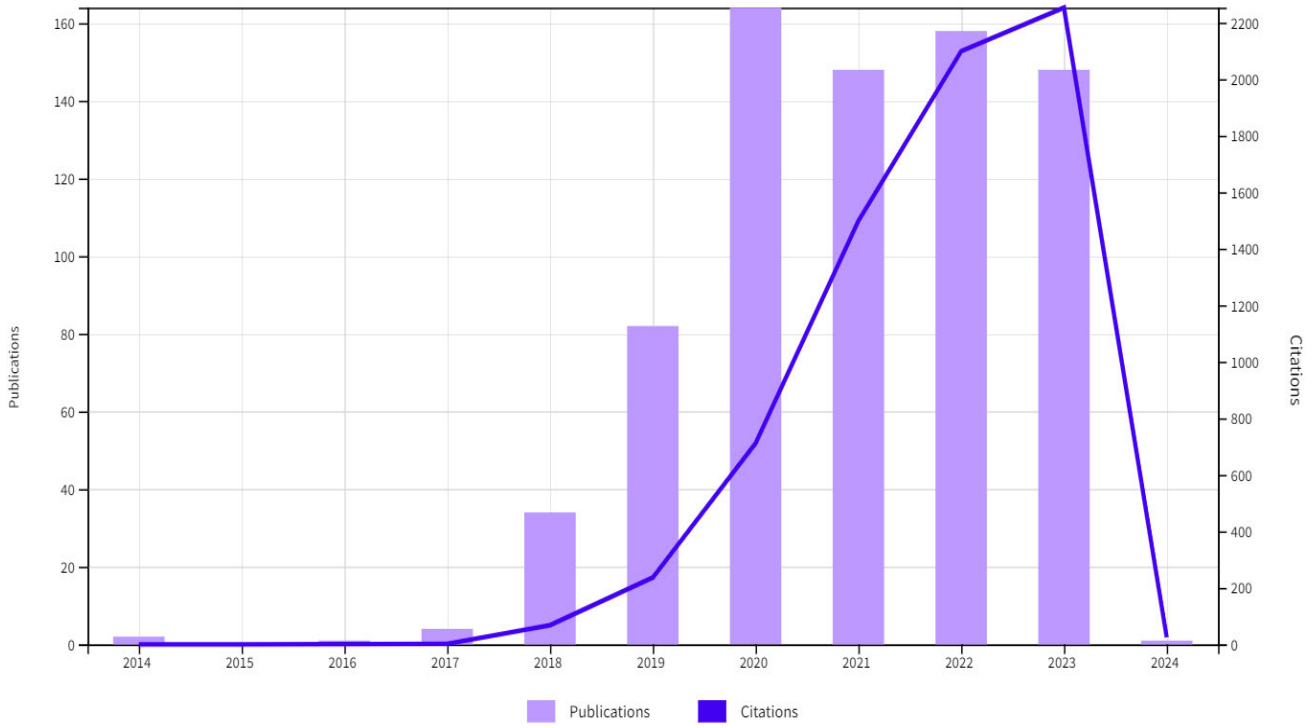

FIGURE 4. Publications and time cited over time.

TABLE 3. Top 10 publishers.

ID	Publisher	Number of Articles	WoS Citation	Scopus Citation
1	COMPUTER LAW AND SECURITY REVIEW (CLSR)	10	483	647
2	IEEE ACCESS	6	255	392
3	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (IEEE TIFS)	1	131	168
4	JOURNAL OF CYBERSECURITY (JC)	1	0	155
5	ECANCERMEDICALSCIENCE	1	0	114
6	JOURNAL OF GLOBAL INFORMATION TECHNOLOGY MANAGEMENT (JGITM)	1	72	88
7	INTERNATIONAL DATA PRIVACY LAW (IDPL)	2	59	64
8	COMPUTER STANDARDS & INTERFACES (CSI)	1	42	64
9	APPLIED SCIENCES SWITZERLAND (ASS)	1	34	51
10	DIGITAL POLICY, REGULATION AND GOVERNANCE (DPRG)	2	29	49

C. RQ3 - WHICH REFERENCES OR MODELS HAVE BEEN APPLIED TO REACH THE GDPR COMPLIANCE? IS THERE ANY GAP?

The papers that could help answer these questions were classified in the GOV category.

Multiple studies have explored how to plan and implement actions for GDPR compliance using ISO-based standards as an implementation roadmap. However, all of them have revealed that these approaches are insufficient to provide a comprehensive guide to compliance. This gap, referred to as the *implementation roadmap gap*, is a significant limitation of ISO-based standards. Other studies suggest that the IG discipline can be a useful reference to address this gap, with a focus on the use of EAM to manage the informational assets under the IG.

Diamantopoulou et al. [34] recommend actions to comply with GDPR for organizations already certified according to ISO 27001:2013 standard for the information security management system (ISMS). The ISO27701:2019 complements ISO27001 with specific requirements for a privacy management system. Anwar and Gill [35] present the common requirements and gaps for compliance with GDPR and ISO 27701, which cannot meet specific legislation issues such as DS rights and PD collection. Lachaud [33] demonstrates that compliance with this standard is insufficient for compliance with the GPDR. Bartolini et al. [36] studied the correlation between GDPR requirements and ISO/IEC 27018/1014, a standard for public cloud computing providers about PII. Gobeo et al. [37] propose an assessment of information assets based on value and risk level to achieve homogeneous data management. The authors evaluate the structure of COBIT 5 (Control Objectives for Information and Related Technologies) with the ISO 27001 standard and conclude that, based on such references, companies can manage PI in line with

TABLE 4. Top 10 most cited articles, including authors.

ID	Title	Authors	Publisher	Year	WoS Citation	Scopus Citation
1	Privacy-Preserving Solutions for Blockchain: Review and Challenges	Bernal Bernabe, J. and Canovas, J. L. and Hernandez-Ramos, J. L. and Torres Moreno, R. and Skarmeta, A.	IEEE ACCESS	2019	138	221
2	EU General Data Protection Regulation: Changes and implications for personal data collecting companies	Tikkinen-Piri, C. and Rohunen, A. and Markkula, J.	CLSR	2018	137	190
3	GDPR-Compliant Personal Data Management: A Blockchain-Based Solution	Truong, N.B. and Sun, K., and Lee, G.M. and Guo, Y.	IEEE TIFS	2020	131	168
4	Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions	POLITOU, Eugenia; ALEPIS, Efthimios; PATSAKIS, Constantinos.	JC	2018	0	155
5	The Internet of Things ecosystem: The blockchain and data protection issues	Wachter, S.	CLSR	2018	94	139
6	The right to data portability in the GDPR: Towards user-centric interoperability of digital services	De Hert, P. and Papakonstantinou, V. and Malgieri, G. and Beslay, L. and Sanchez, I.	CLSR	2018	94	126
7	The impact of the EU general data protection regulation on scientific research	Chassang, G.	ECANC ERMEDI CALSCI ENCE	2017	0	114
8	Smart City IoT Platform Respecting GDPR Privacy and Security Aspects	Badii, Claudio and Bellini, Pierfrancesco and Difino, Angelo and Nesi, Paolo.	IEEE ACCESS	2020	62	91
9	The Impact of GDPR on Global Technology Development	Li, H. and Yu, L. and He, W.	JGITM	2019	72	88
10	Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0	Larrucea, Xabier and Moffie, Micha and Asaf, Sigal and Santamaria, Izaskun.	CSI	2020	42	64

regulatory requirements by inserting specific requirements. Dharni et al. [38] combine the COBIT 2019 framework for IT governance and management with the insertion of a focus area that adopts cybersecurity benchmarks such as NIST and ENISA for PD protection and point out that there are still actions left for compliance with GDPR.

Lachaud [33] emphasizes that works that use standards for compliance with the GDPR make use of the risk management discipline since, to meet a certain requirement, it is possible to adopt organizational or technical measures subject to non-compliance due to vulnerabilities inherent to the environment in which they are adopted. The works indicate a path to compliance and resolve a portion of the requirements, but do not present a complete solution. The author emphasizes that to comply with GDPR, a mix of two approaches must be used. The risk-based approach, as presented in the works mentioned above, and the law-based approach. The author defines the legal approach as establishing a ''non-negotiable'' right of the DS to have their PD protected, aiming to guarantee the legality and transparency of data processing. The GDPR grants, for example, DS the right to access and rectify their data, but the EU legislator has not proposed a risk-based approach in this area because it considers that the level of access and rectification should not vary across countries regarding the risks incurred. Similarly, Yeung and Bygrave [39] examine the tension between the compliance approach based on risk management and the approach to the primary objective of legislation to safeguard fundamental rights, pointing to them as distinct sources of the legislation's requirements in their nature. They suggest that despite the complexity and uncertainty surrounding the requirements, the scheme is an innovative hybrid with a significant degree of built-in ''future-proofing'' that should help make it more resilient to being overcome by organizational and technological measures.

On the other hand, Assis [40] discusses the concept of IG as an approach to the governance of informational assets in organizations. It highlights IG as a business-oriented discipline, compliance with standards, secrecy, external threats, data and information management, challenges regarding access governance, and use and storage of data, which are also apply to the PII context. According to a survey carried out by the (CGOC) Compliance, Governance, and Oversight Council [41], compliance with the GDPR has become one of the main issues in IG today.

Burmeister et al. [45] suggest that the implementation of the GDPR sparked global IG efforts, with companies required to address the information artifacts more intensively through their EAM systems. EAM can be described as a means to plan, coordinate, and guide the continuous digital transformation in organizations, encouraging the use of a common language to support decision-making [43]. Lajara and Maçada [44] suggest that EAM can provide a basis for IG when it captures the representation of information and its processes through EA (enterprise architecture) artifacts that could use different techniques and levels of abstraction.

Burmeister et al. [45] argue that EAM can be key to implementing GDPR as an important domain of IG and ensuring transparency in information integration across the organization. The authors identified a multitude of benefits

TABLE 5. Categories discussed in articles.

Category	Description	Doc
GOV	IG, EAM, ISO-based roadmaps, generic challenges, and enablers for compliance	25
DSR_C	DS Rights – Consents	25
DSR_T	DS Rights – Transparency	14
MISC	Miscellaneous – Regulations in Countries, Innovation, DPIA, others	8
TEC	Technologies and related impact for compliance (challenges or enablers)	43
T_BC_C	Blockchain – challenges	7
T_BC_E	Blockchain – enablers	11
T_IoT_C	IoT – challenges	9
T_IoT_E	IoT – enablers	2
T_AI_C	AI – challenges	5
T_AI_E	AI - enablers	3
T_O	Others	6

for using EAM for GDPR implementation, or equivalently, GDPR enablers for using EAM, based on interviews with 29 enterprise architects in German organizations. They listed these enablers in Table 6 ranked by the frequency that means the importance of each one for GDPR compliance in the view of those experts.

The tables below include identifiers for enablers, challenges, and benefits. Enablers are identified as ''En,'' challenges as ''Cn'' (which have already appeared in Table 1), and benefits as ''Bn,'' where ''n'' is a sequential number.

Based on these enablers the authors derived seven design principles that must improve IG for compliance.

The first and the most frequent factor from Table 6 shows congruency with the results of Huth et al. [46]. These authors emphasize the importance of RoPA and detail a list of attributes that must be maintained by organizations as a result of the principle of responsibility in legislation. This principle requires, under certain conditions, the demonstration of records of activities on PD to supervisory authorities, in accordance with art. 30 GDPR [47], in particular under data leakage situations.

Becker et al. [48] exemplify EAM as an IG instrument for GDPR compliance under scientific research in biomedical areas context, which have a special interest in RoPA because of sensitive PD and laws in certain countries.

The aforementioned topic indicates that adherence to IG discipline and EAM practices could facilitate GDRP compliance. Hence, exploring the viability of utilizing these disciplines to address the implementation roadmap gap for complete GDPR compliance when using solely an ISO-based standard would be a valuable endeavor. Such an investigation could help identify ways to bridge this gap effectively.

Further sections, from D to G, will answer RQ4, which asks about the challenges and enablers for GDPR compliance. Section D describes the challenges and enablers for the GOV category, section E for the DSR-C category, section F for the DSR-T category, and section G for the MISC category. The remaining sections will answer RQ5, which pertains to the challenges and enablers for the technology category.

D. RQ4 - CHALLENGES AND ENABLER FOR THE GOV CATEGORY

Table 7 shows specific challenges and enablers regarding GDPR compliance after the content analysis considering articles in the GOV category.

To summarize, the main challenges discussed are related to ensuring the rights of individuals whose data is being used, especially the right to be forgotten, which involves removing PD from digital environments. This can be a complex task, as noted by Poritskiy et al. [49], Zaeem and Barber [50], Georgiopoulou et al. [51], Politou et al. [8], Tikkinen-Piri et al. [17]. It is important to note that this challenge is significant and has also been identified in the DSR-C and DSR-T categories. Challenges C9, C10 and C11 are algo part of DSR-T category discussion, but they still appear in GOV category.

Regarding GDPR enablers, rather than focusing solely on issues that the EAM can handle as exposed in Table 7, it is important to highlight the enablers associated with more strategic components of the IG, like E11, E12, E13, and E14.

A model of GI components is presented in E12 by Tallon et al. [54]. It includes relational practices like community communication, user involvement, and idea exchanges—in this case, on data privacy—and structural practices like supervision mechanisms, policy definition, and role and responsibility definition. The relational practices also are discussed under a leadership and communication skills point of view to turn viable decentralized focal points to improve to better data protection management, as stated the E11 based on [53].

The significance of alignment and harmony between business areas and governance leaders cannot be underestimated, as emphasized by Vojvodic and Hitz [55], which we have labeled as E13. To attain this alignment, they suggest creating a versatile team that is spearheaded by proactive leaders with a genuine dedication to improving and promoting privacy practices. This methodology bears resemblance to E11 [53] and can also be viewed as a type of relational practice in the realm of IG [54], in accordance with E12.

A COBIT 2019 adaption for data privacy by Dharni [38] represents the enabler E14. ISACA [56] created the COBIT 2019 with 40 objectives categorized into the domains of governance and management. These objectives are associated with practices formed by policies and procedures, information flow, organizational structure, services, infrastructure, applications, culture and ethics, and processes. Dharni [38] combines the use of COBIT 2019 with a cybersecurity area focus indicating the NIST or ENISA references to cover the PD data protection. Therefore, E14 are related to the view of the strategic aspect of IG for data privacy.

Poritskiy et al. [49], along with others, have discussed the advantages of GDPR compliance. Raising awareness among data protection stakeholders about these benefits can be a significant motivation for holding privacy practices accountable

TABLE 6. GDPR enablers by the of EAM adapted from Burmeister et al. [45].

GDPR enablers using EAM	Freq.
E1. Creation of the Record of Process Activity for PD (RoPA) using existing EA artifacts.	79%
E2. EA artifacts are central sources for obtaining data by data stewards.	63%
E3. Documentation of business-related privacy aspects in a more sustainable way.	54%
E4. Support for compliance with DS´s rights.	50%
E5. Promotes common terminology for the organization.	42%
E6. Simplifies privacy impact surveys and analyses when evaluating new technologies.	29%
E7. Enables independent reporting by the data controller using EA tools.	25%
E8. Improved data leakage impact survey/analysis.	17%
E9. Supports the implementation of the "privacy by design" concept.	17%

and achieving compliance. Table 8 provides a summary of the discussed benefits.

E. RQ4 - CHALLENGES AND ENABLER FOR DS RIGHT - CONSENT CATEGORY (DSR-C)

The issues and challenges regarding the DS rights, such as the right to revoke consent, and the right to be forgotten, among others, are also debated in a more specific way for sectors such as means of payments under the environment under use and technologies such as big data analytics and AI that promote facilities for the re-identification of PD without individual consent [8], for scientific research sectors in the health area that face the processing of sensitive data [57], [58], [59], biometric data [60], from children [61], for organizations in the Telecommunications sector that deal with a high volume of PD from consumers [62] among others.

To ensure compliance with GDPR, the Resource-Based View (RBV) literature was consulted in addition to EAM and IG disciplines. Labadie and Lagner [123] apply RBV as a framework for GDPR, highlighting the importance of allocating specific resources for compliant operations. Through expert observations of 22 companies and four GDPR compliance projects, the authors establish a capabilities model. They identify three critical groups of capabilities and resources that are essential for successful implementation: infrastructure, data management, and external communication management.

In contrast to these challenges, there are works that discuss the systemic approach to consent management as a tool to enable compliance with legislation and circumvent it.

Sim et al. [63] propose a model to explain the technical requirements for a system to meet the rights of DS in relation to access to their data. They discuss the essential importance of consent management with transparent processing allowing traceability of data, including modifications to consents.

Robol et al. [64] states that modeling frameworks have been suggested to aid in the examination of requirements in intricate socio-technical systems. They propose a modeling language and formal framework for analyzing privacy-consent requirements, based on the social principle of consent. This research project with the Trentino health-care provider in the medical domain provides valuable insights into the analysis of privacy.

Similarly, Robol et al. [65] and Peyrone and Wichadakul [66] propose formal models for managing subscriptions updated with technical improvements. The first authors propose that organizations can improve their data protection policies with a consent regime that supports both normal or non-retroactive granting, retroactive granting, and revocation for these two situations, in line with legislation.

Peyrone and Wichadakul [66] have proposed software engineering models to represent the basic functionalities of consent management. These models consist of four state machines and a class diagram of the object-oriented analysis technique that formalizes the structure of data and activities. Each machine represents the possible states regarding Data Protection (DP) and consents, and the transitions between these states. The models synthesize the behavior of functionalities such as basic processing on DPs considering the legal bases, revocation of consent or deletion of PD as requested, obtaining DP as requested to comply with the right to portability [115], confirmation, and recording of acceptance of consent. These models can be understood as Enterprise Architecture (EA) artifacts. Several works on consent management aligned with scientific research in the health area are based on industry standards, which are more rigorous than explicit requirements in GDPR.

TABLE 7. Challenges and enabler from GOV category.

Challenges (C) and Enablers (E)	Authors
C10. Data Portability.	[49], [115]
C11. Right to be forgotten or to remove PD.	[49], [50], [51], [8], [17]
C12. Right of access and rectification of PD by DS.	[49], [50], [51]
C13. Perform compliance audits across environments, including geographic transfers.	[49], [51]
C14. Increased Information Security budget.	[49]
C15. Subcontractor management and shared responsibility.	[49]
C16. Increased technical complexity.	[49]
C17. Limiting the growth of the use of emerging technologies.	[49]
C18. Transparency about PD leakage.	[50], [51]
C19. Transparency about PD processing.	[50],
C20. Transparency about the physical storage locations of DP and geographic movements (IaaS)*.	[51]
E10. Existence of an Information Security Management System (ISMS) complied with ISO 27001.	[52]
E11. Data protection management with decentralized focal points.	[53]
E12. IG practices in place (structural and relational).	[54]
E13. Alignment between governance leaders and business areas through the formation of a multifunctional unit under the management of proactive leaders.	[55]
E14. COBIT2019 as a framework for data privacy compliance.	[59]

Sutter et al. [67] discuss the use of electronic informed consent (eIC), which enables the interactive transmission of research information to its participants, influencing the obtaining of consent in a dynamic way. They emphasize that in the EU, there is a distinction between eIC for participation in clinical research and eIC for treating participants' PD. EU countries are divided into three groups regarding eIC regulation: those that accept and regulate the use of eIC, those that accept the use of eIC without explicitly regulating it, and countries that do not accept the use of eIC. As a result, the regulation of eIC through laws and guidelines shows a wide variety among Member States, whereas in the United States, it is harmonized through a federal code. Despite the lack of uniformity across the EU, Rau et al. [68] confirm that at the time of publication of their research, there were no commercial systems for managing consents to meet specific requirements for scientific research with patient health data. They specified a generic consent management system (gICS), to enable the implementation of specific rules for each type of research and type of communication desired with patients in a configurable way. The authors describe the characteristics of the technical architecture of gICS as an open-source tool, part of the MOSAIC project.

In empirical research, Wang et al. [69] analyzed the use of a mobile app with PD and health data of people with diabetes in Australasia. The application makes use of eIC and allows participants to view and modify their consent decisions based on iterative research, enabling the legal collection of the greatest amount of data for scientific research. Table 9 summarizes the challenges and enablers for the SR-C category discussed.

F. RQ4 - CHALLENGES AND ENABLERS FOR THE DS RIGHT – TRANSPARENCY CATEGORY (DSR-T)

Effective communication and management of DS rights must adhere to transparency requirements between DS and controllers to ensure legal compliance. Within the SR_T category review, seven works delve into the topic of consent, building upon the previous topic, while two works are examined alongside an article in the GOV category. Additionally, other works explore specific aspects, providing valuable insights into the current state-of-the-art literature in this field.

Coleti et al. [70] argue for the need for mechanisms to improve the presentation of information about PD, providing greater transparency in communication between controllers and DS. The authors propose the TR-MODEL with guidelines for a metadata profile management application that aims to standardize the minimum information necessary for DP transparency and a guide on how to present it. An application that uses the model was empirically tested with users evaluating transparency considering dimensions of the HCI (Human-Computer Interaction) approach, obtaining satisfactory results.

Brkan [71] discusses automated decision-making from a legal perspective, aiming to understand the guarantee of transparency in a criminal matter context. Although legislation imposes limitations on automated decisions that apparently can encourage the protection of individuals, they argue that they potentially inhibit AI applications that could contribute in this context. They debate the GDPR requirements for transparency about such decisions by providing the holder with "meaningful information about the logic involved" (Art. 13, Art. 14, and Art. 15), going beyond semantic questions about the "right to explanation.".

TABLE 8. Benefits of GDPR compliance.

Benefits
B1. Better understanding of the law.
B2. Confidence to maintain compliance.
B3. Improvement in the decision-making involving PII.
B4. Accuracy about privacy risks.
B5. Increased security in the marketing of products and services involving PII.
B6. Increase in the quality of documentation involving PII.
B7. Minimizing PII Collection.
B8. Improvements in data management.
B9. Creating competitive advantages.
B10. The motivation to share PD, which facilitates internal and external communication.

Pins et al. [72] analyzed results from 422 requests from DS in 139 organizations. They formulated the first empirically based body of knowledge on requirements and design for the right of access, considering transparency.

Veale et al. [73] criticize the application of Data Privacy by Design principles to the construction of PET-type tools. They show that some strategies of this principle focused on confidentiality used by data controllers present risks of allowing the identification of PD while at the same time limiting the ability to comply with the rights of access, deletion, and objection. Based on these criticisms, they suggest ways to implement data-centric principles to ensure more transparency in the relationship with DS through parallel systems.

Table 10 summarizes these factors. Note that some transparent challenges are also presented in GOV category. We do not repeat them in this table again.

G. RQ4 - CHALLENGES AND ENABLERS FOR MISCELLANEOUS CATEGORY (MISC)

The articles under the MISC discuss the GDPR compliance considering particular characteristics in EU member countries, the generic impact of GDPR on innovations, questions regarding the risk management approach to compliance, and articles that address legal and ethical issues around legislation.

Doe [74] shows a general discussion on the implementation of GDPR in the EU. Cordeiro et al. [75] for Portugal, Mitrou [76] for Greece, Faifr and Januska [77] for the Czech Republic and Canedo et al. [78] discuss the implementation of the LGPD in Brazil.

GDPR can introduce barriers to innovations or elements that drive them [79], [80], [81].

Some studies focus on the risk management approach of the GDPR, such as the development and use of the DPIA

(Data Protection Impact Assessment) [82], [83], [84], [85], [86], [87], [88] and on vulnerabilities and threats in international transfers via electronic payment wallets [89].

There are some works that deal with the effects of GDPR on organizations in general, with a focus on organizational structure [90]. Other works expand the discussion on legal concepts [91], and there are also those that focus on ethics and data privacy considerations during times of crisis, such as the COVID-19 pandemic [92].

The challenges and enablers in this category are highly context-dependent and cannot be generalized or synthesized like other categories.

The next sections, from H to L, provide detailed answers to RQ5, which is about the technologies and their characteristics that can have negative impacts on compliance with GDPR, as well as the ones that promote positive impacts.

H. RQ5 - CHALLENGES AND ENABLERS FOR TECHNOLOGY (T) CATEGORY

This topic brings generic considerations about the challenges and enables regarding technology category.

Discussions about technologies are crucial in current systems, such as health systems, smart cities, and data privacy tools. These systems are made up of physical and software components, humans, and the social environment. Hence, it is essential to consider organizational structures and the social environment's iterations in privacy issues [93].

There are some articles that discuss "big data" and "analytics." However, a separate subcategory for this topic was not created because it is generally justified by the high volume of data that these technologies use, along with IoT and AI technologies. Some specific articles on big data and analytics have been included in the "others" subcategory.

The next four sections, I,J,K,and L describe the challenges and enablers discussed in the seven technology subcategories, about blockchain (T-BC-C, T_BC-E), IoT (T-IoT-C, T-IoT-E), AI (T-AI-C, T-AI, E), and others (T-O) respectively.

I. RQ5 - CHALLENGES AND ENABLER FROM BLOCKCHAIN (T-BC-C AND T-BC-E) SUBCATEGORIES

Blockchain technology is built on a distributed and synchronized database for recording transactions known as "blocks," which are linked together through encryption to form a "ledger." This ledger is duplicated across multiple nodes in a computer network. New transaction blocks are added to each ledger only after being validated by cryptographic algorithms on each of the validator nodes. This process aims to ensure transparency, trust, and accountability [94].

Haque et al. [12] discuss in an RSL the challenges for GDPR compliance when personal data is transacted in an environment with blockchain technology. They propose workarounds that consider paths using the legislation itself and characteristics of the technology. There are two intrinsic challenges to this technology, already described by the European Parliamentary Research Service department:

TABLE 9. Challenges and enabler from SR-C category.

Challenges (C) and Enablers (E)	Authors
C21. Right to delete PD (the same as C11 from table 8, but from other authors).	[57], [58], [59], [60], [61], [62]
C22. Right to revoke consent.	[8], [17], [50]
C23. Avoid the identification of anonymized. PII in big data environments without consent.	[8]
E13. Tools for managing consents and use of electronic Informed consent systems (eIC).	[63], [64], [65], [66], [67], [68], [69]

i) Responsibility of controllers or processors: GDPR requires at least one data controller. The controller manages data collection and consents, and must be accessible to data subjects. With blockchain technology, each node owner of the validator network must be introduced as an actor, requiring greater complexity in terms of guaranteeing the principle of responsibility. ii) Non-modifiable and non-deleted data: GDPR recommends minimizing data, stating the purpose of limited use, and modifying and deleting data when necessary. The use of blockchain technology presents challenges to GDPR compliance because data stored in a blockchain is non-modifiable and non-removable. As new transactions occur, the data continually grows, and the information contained in ledger blocks cannot be altered or removed. To address these challenges, the authors identify six groups of articles of law and propose measures or workarounds that leverage blockchain technology as an enabler for compliance. The first two groups of challenges pertain to issues previously mentioned, while the other four are as follows: i) Challenges related to consent management can be resolved through the use of smart contracts, which allow the creation of rules with trackable executions. ii) Processing principles benefit from the inherent transparency and traceability of blockchain technology. iii) Territorial scope challenges, which involve the transparency required for data movements between countries, can be addressed by using a private blockchain network managed by the operator or controller. iv) Protection and "privacy by design" requirements can be met by the zero-knowledge proof (ZKP) feature of blockchain, which allows validation of a block or ledger transaction without making the transaction content available, ensuring anonymity. Other authors also present challenges for compliance with blockchain technology and its enablers in a similar way.

Cornelius [95] shows how blockchain records can meet the principles of transparency and responsibility, considering NFTs (non-fungible token) applications, which are unique cryptographic records linked to a good or object of value and contribute to the discussion about public and private blockchain. They highlight the challenges for compliance with the principle of responsibility in the public network.

From the side of challenges, Hofman et al. [119] also points out compliance obstacles, especially guaranteeing DS rights regarding deleting records under the Blockchain. Kapsis [122] discusses these and other challenges for the fintech (Financial Technology) sector, including the conversational

TABLE 10. Challenges and enabler from SR-T category.

Challenges (C) and Enablers (E) SR-T	Authors
C24. Ensuring transparency in automated decisions.	[71]
C25. Inhibition of AI tools to support transparency when making automated decisions, restricted by legislation.	[71]
C26. Mitigate risks of using the Data Protection by Design approach for the development of C4.	[73]
C27. PET tools with limit access and deletion capabilities.	[73]
C29. Precarious mechanisms for presenting information between controller and DS.	[70]
E14. Metadata profile management application that aims to standardize the minimum information necessary for DP transparency (HCI approach).	[70]
E15. Requirements and design on the right of access considering transparency.	[72]

stance of the European Commission that imposes barriers to blockchain characteristics to be fully adopted for the sector, inhibiting the acquisition of competitive advantages to EU member countries.

On the other hand, Freund et al. [121] analyze the privacy principles and data treatment in Blockchain, guided by the phases of the Data Life Cycle. It presents an approach for organizations to adapt to the legislation and provides data treatment options for the phases that present gaps. Moreover, Erbguth [124] proposes five ways for GDPR compliance using this technology.

Barnabe et al. [11], in an RSL, present the state of the art in privacy-preserving technologies with blockchain technology. They indicate techniques to get around them that apply the self-sovereign identity paradigm, SSI (Self-Sovereign Identity), which can be adopted by IDM (Identity Management System) to replace centralized models. This paradigm aims to empower users with the confidence of decentralized validation of their identity anonymously, made possible by techniques such as ZKP in digital transactions. Under this model, DPs are no longer available in third-party services, providers, or transactions, with interaction with users also being anonymized. The authors describe privacy problems in public networks due to the availability of the ledger and analyze the public keys of users involved in the transaction, indicating the potential for undue discoveries to be made by inferring information that should be confidential. They discuss workaround alternatives using the technology itself, synthesizing results from previous literature and open challenges such as those related to the management of cryptographic keys in recoveries, problems of resistance to cryptographic privacy for quantum computing, and other problems.

Alsayed Kassem et al. [117] also discuss IDM with blockchain for GDPR compliance, Campanile et al. [118] discuss DP systems of records.

Truong et al. [114] question the centralized management model for PD by controllers. They highlight that under this model, the prerogatives of the law are derived from explaining the rights of DS, leaving the exercise of such rights as a challenge for them and dependence on their skills. The authors propose a model for managing decentralized mechanisms for PD processing, enhancing transparency and governance using blockchain. The model includes a high-level architecture, design and functionality guidelines, and detailed algorithms for GDPR compliance.

J. RQ5 - CHALLENGES AND ENABLER FROM IOT (T-IOT-C AND T-IOT-E) SUBCATEGORY

Articles about IoT use the basic concept of IoT as a growing network of identified, internet-enabled objects or devices that communicate with each other. However, an IoT environment can potentially increase the risk of access to PII stored on network objects.

Wachter [96] highlight that identification and access control technologies are essential infrastructure for linking data between a user's devices with unique identities and providing integrated, linked services. However, profiling methods based on linked records can reveal unexpected details about users' identities and private lives, which can conflict with privacy rights. This can also lead data controllers to act in their economic interests or act in a discriminatory manner. Therefore, the authors propose that a balance must be struck between the identification and access control necessary for the IoT to function and the rights of DS to privacy. In summary, they discuss four challenges for compliance under IoT: profiling, inference, and discrimination; context-sensitive identity control and sharing; consent and uncertainty; and honesty, trust, and transparency.

Works by Badii et al. [97], Larrucea et al. [98], and Asghar et al. [99] discuss the challenges of GDPR compliance in IoT environments in smart cities, healthcare industry, and supporting electronic surveillance systems, respectively.

On the other hand, some works aim to demonstrate enablers for compliance under IoT technology (T-IoT-E). For example, Kounoudes and Kapitsaki [13] presented a conceptual framework for GDPR compliance under an IoT environment that encourages DS to have greater power over their PII.

Fabiano et al. [100], Sun et al. [101], and Rantos et al. [102] discuss the IoT environment and indicate blockchain as a suggestion for compliance solutions. Rantos et al. [102] propose a blockchain-based platform for consent management in the IoT ecosystem. Sanchez et al. [103] propose the management of privacy preferences in IoT environments using an approach that exploits Semantic Web (SW) technology. This approach intends to allow users to negotiate permissions to share data with third parties via connected devices.

K. RQ5 - CHALLENGES AND ENABLER FROM AI (T-AI-C AND T-AI-E) SUBCATEGORY

Kramcsák [104] argues that adequate data governance is a challenge for AI systems that want to obtain benefits from associated technologies. The accuracy and effectiveness of AI models depend on the availability of genuine, relevant, and representative training data, often in large volumes.

AI systems tested and validated using low-quality data or inadequate volume can produce inaccurate, erroneous, distorted, or harmful results that can affect individual rights and freedoms.

Kingston [105] proposes four areas of GDPR compliance where technologies such as machine learning or rules-based technologies can be relevant. These areas include following compliance checklists and codes of conduct, supporting risk assessments, complying with new regulations related to technologies that perform automatic profile identification, and complying with new standards regarding the recognition and reporting of security breaches. For example, Amaral et al. [106] describe systems for automating policy-based compliance checking, and Lore et al. [107] explain how to automate data protection actions for compliance in public records workflow systems in Italy.

In a more conceptual discussion, Butterworth [108] debates the role of impartiality and equity in the interpretation of the GDPR when using AI by organizations. Wulf and Seijof [109] conducted an online survey with 835 DS and 100 organizations to empirically validate the quality and effectiveness of communications about automatic AI processing required by GDPR. The survey showed that the communications required by the GDPR do not meet the expectations and needs of DS. The explanations prepared by the guidance of the GDPR generic formulations differ widely, are often vague, incomplete, and lack transparency.

In summary, AI technologies are data-intensive, which is the biggest challenge for compliance. AI as an enabler allows for the development of PET-type tools, as classified in Kingston [105].

L. RQ5 - CHALLENGES AND ENABLER FROM OTHER TECHNOLOGY (T-O) SUBCATEGORY

Solid is a software project that was initiated in 2016 and is led by Tim Bernes-Lee, the creator of the World Wide Web. The aim of Solid is to create a secure and decentralized platform for the exchange of public and private data. Pandit [32] highlighted the growing interest in Solid's radical approach, which gives data owners sovereignty over their data and moves away from control by controllers, blocks, and lack of privacy. Solid includes an IDM, access control, and communication called ''Pods'', all of which are controlled by the data owners. By having management control over their own data, owners can modify it and decide on sharing or revoking access requested by other individuals, organizations, or applications. Data stored in Pods uses standard, open, and interoperable protocols, and formats, enabling secure communication between owners and requesters or between owners and websites and systems relevant to the data stored in Pods.

Emerging technologies such as Big Data, quantum computing, and 5G technology can significantly impact compliance challenges and present opportunities to be used to their advantage.

Politou et al. [110] argue that one of the biggest threats to data privacy is the risk of re-identification of unidentifiable data using Big Data and Analysis techniques. To mitigate these risks, data science employs various methods and techniques based on principles already adopted by data protection legislation, such as Data Protection by Design (DPbD) principle.

Malina et al. [111] discuss the IoT environment under quantum computing, which poses more complex challenges to compliance, such as computational ease for breaking data encryption and reducing potential PET to remedy the increase in these risks.

Rizou [112] emphasize the risks of IoT enhanced by 5G technology, which allows a much greater number of devices on the network and increases connectivity facilities, making it more complex to meet the rights of holders due to the increase in the number of actors involved in a network of greater dispersion about connected objects.

Peukert et al. [120] found that websites reduced interactions with web technology providers after GDPR. Less popular sites were affected and market concentration increased for large providers such as Google.

The upper frame of Fig. 5 in the following topic illustrates the answers to the five research questions described as results in this topic.

V. DISCUSSION OF RESULTS AND RESEARCH AGENDA

This topic focuses on answering the research question RQ6 ''What gaps exist in current research about challenges and enablers of GDPR compliance that future research can investigate?''

Section A provides a research suggestion for the development of a model to cover the GDPR implementation gap. This suggestion is based on the answer to RQ3 in the results section.

Session B develops five propositions based on challenges and enablers discussed in RQ4. These propositions could provide valuable insights to future empirical research.

Session C aims to expand the scope of findings in other contexts. It suggests constructing hypotheses and possible variables that may be established in quantitative research based on the statements from the suggested propositions, indicated by C1 in Fig.5, and from the remaining challenges and enablers from the review, indicated by C2.

The bottom frame of Fig. 5 illustrates the research agenda described in session D and its connection with the discussion of results from previous sessions.

A. IG FOR PD MODEL TO COMPLEMENT ISO-BASED ROADMAPS

In response to RQ3, the results indicate that the existence of IG discipline and EAM practices could facilitate GDPR compliance, and further investigation into the potential use of these disciplines is recommended. The use of ISO-based and other frameworks alone may result in incomplete compliance due to gaps in requirements such as DS rights, records of

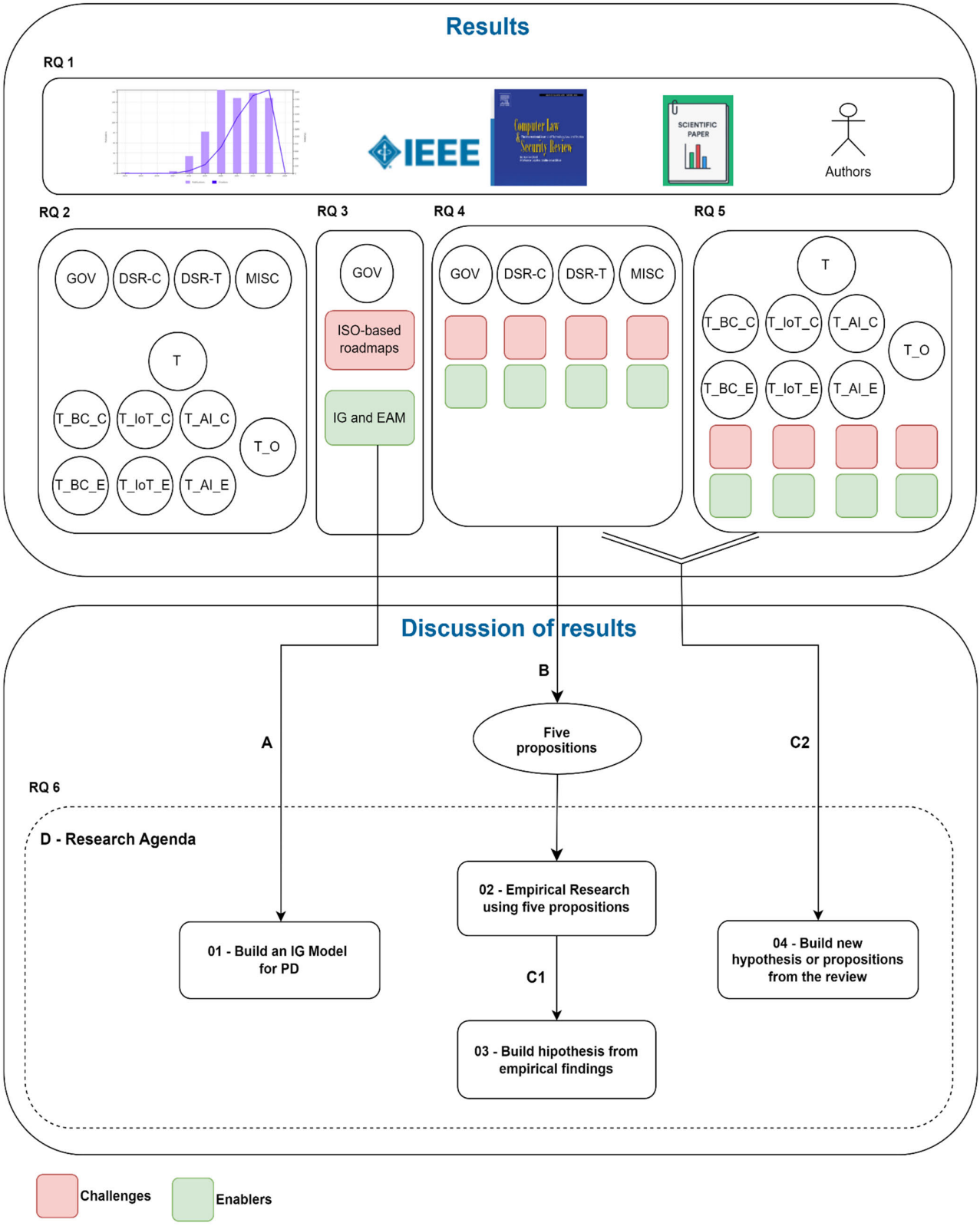

FIGURE 5. Overview of results and connections with its discussion.

process activity, data sharing management, and PD collection, called ''compliance implementation gap.''

On the other hand, Burmeister et al. [45] identify specific enablers of EAM for compliance, including the creation of a

TABLE 11. Propositions and links to challenges and enablers.

Proposition	Challenge / Enabler / Benefits
P1) Investment	C3. GDPR compliance may be expensive and time consuming as it requires substantial financial and human resources.
P2) DS rights	C11 Right to be forgotten or to remove PD. C21. Right to delete PD (the same as C11 from table 8).
P2) DS rights	C12. Right of access and rectification of PD by DS.
P2) DS rights	C22. Right to revoke consent.
P3) Record of Processing Activities	E1. Creation of the Record of Process Activity for PD (RoPA) using existing EA artifacts.
P3) Record of Processing Activities	E2. EA artifacts are central sources for obtaining data by data stewards.
P3) Record of Processing Activities	E3. Documentation of business-related privacy aspects in a more sustainable way.
P4) PII sharing	B10. The motivation to share PD, which facilitates internal and external communication.
P4) PII Sharing	C13. Perform compliance audits across environments, including geographic transfers.
P5) Data collection – Indirect data collection and anonymized data	C23. Avoid the identification of anonymized. PII in big data environments without consent.

Record of Process Activity for PD (RoPA) using existing EA artifacts, the centralization of data sourcing through EA artifacts, the documentation of business-related privacy aspects in a sustainable manner, and support for compliance with DS rights.

Thus, taking into account the match between the framework gap and enablers of EAM usage, it would be valuable for future research to propose an information governance (IG) model on PD that outlines the requirements using EAM. This model can be made up of two types of elements. The first one would illustrate the processes and information flows between external entities and functions within the scope. The second element would represent the structure of information and rules based on the GDPR. These conceptual artifacts would emphasize their relationships and characteristics, enabling organizations to better understand and capture their privacy practices within the defined scope. This tool would be useful for both researchers and privacy or data protection professionals.

According to the results presented in Section C, answering RQ3, it is recommended that the IG focus on strategic aspects of the business rather than solely on EAM problem-solving. To achieve this, the IG for PD model may consider adding a third element that takes into account a mix of the enablers discussed. E12 covers recommended structural and relational practices from the Tallon et al. [54] model, whereas E13 highlights the importance of a multifunctional unit led by a proactive leader who prioritizes privacy practices, as found by Vojvodic and Hitz [55]. E14 describes how to use COBIT 2019 for data privacy [56].

With this strategic component, the IG should act as a lens to capture IG practices at various levels, including organizational structure, leadership, roles and responsibilities, communications, and other privacy program facets.

B. FIVE PROPOSITIONS TO BE INVESTIGATED IN FUTURES EMPIRICAL RESEARCH

The literature offers valuable insights into the obstacles and opportunities surrounding data protection and privacy practices. By leveraging this knowledge, researchers can develop propositions to test these factors in empirical studies. It is crucial to take into account specific contexts to gain a deeper understanding of these practices. Through the use of propositions, researchers can anticipate future scenarios whereas considering the study's conditions and limitations [113].

Drawing from the challenges and enablers identified in this review, it was crafted five propositions that address issues such as investments in privacy programs, DS rights, records of processing activity, and data sharing and collection. Table 11 shows a comprehensive overview of these factors, complete with links to each proposition. Furthermore, other factors not discussed as a basis for propositions could serve as potential sources for future ones, as suggested as further conceptual research in section C, indicated by C2 in Fig. 5.

Proposition P1 delves into the complex issue of justifying the feasibility of investing in a project aimed at adapting to data protection legislation. This is due to the significant demand for human, financial, and long-term resources required for successful implementation.

By examining the perception of organizations towards the C3 challenge, this proposition can shed light on how it influences their decisions regarding the allocation of budgets and resources towards privacy programs, particularly in specific contexts.

Proposition P2 seeks to shed light on the difficulties organizations encounter when upholding the DS rights, specifically with regards to the right to be forgotten, the correction of personal data, and the revoke of consent. These challenges involve technical obstacles in modifying or erasing digital information.

How prevalent are these challenges, and to what extent do they pose a challenge? Additionally, how frequently do DS such requests, and how have organizations responded to them?

Proposition P3 states that compliance with data protection legislation encourages security and control over data sharing with the external environment. Organizations consider this situation one of the benefits of conformance with GDPR.

This proposition aims to advance the understanding of the B10 benefit by indicating that, following the law's enactment, there may have been more motivation to share PD due to the legislation's favorable treatment of both internal and external transit. Do organizations have the perception that the law has brought the benefit of greater security regarding the sharing of PD? Did the legislation promote facilities for the internal and external transit of PD? How have organizations been sharing data, considering the legislation?

TABLE 12. Research agenda.

ID	Research gap or opportunity	Research	Purpose
01	GDPR implementation gap when using ISO-based standards isolated.	Build an IG model for PD.	Represent organizational and relational practices of IG for PD and privacy practices under a process and information structure perspective.
02	The need to validate the suggested propositions via empirical research.	Empirical research using five propositions.	Extract insights from empirical research studies to enhance the existing knowledgebase.
03	Opportunity to expand the context of empirical findings from the previous empirical research (02).	Build hypothesis from empirical findings.	Expand the empirical findings to other contexts considering a set of relevant variables.
04	Opportunity to create new research using the challenges and enablers founded in this review.	Build new hypothesis or propositions from the review.	Develop new hypothesis or propositions for a more in-depth study of the challenges and enablers identified in this review.

Proposition P4 states that the lack of EA artifacts poses a challenge in constructing the RoPA. At the same time, the absence of a comprehensive RoPA makes it difficult to search for information about the PD and to locate the PD within an organization's environment.

P4 offers an opportunity for further exploration of the C13 challenge and its relationship with enablers for compliance through EAM, including E1, E2, and E3. Difficulty with C13 may impact the ability to fulfill requests from holders or returns for audit purposes, particularly in dispersed organizational environments. However, examining the relationship between the challenge and these enablers can shed new light on the role of EAM as a factor for IG, as well as Burmeister et al. [45] emphasis on the primary uses of EAM.

Proposition P5 shows that in organizations already in compliance with the GDPR, practices of identifying PD obtained indirectly or re-identifying anonymized PD to obtain subsequent consent are common and unhindered.

P5 raises questions about the ethical implications of such practices, and it would be interesting to further explore the extent to which these practices are being used and their potential consequences.

These propositions could be used in empirical research to be validated and estimate the capture of related privacy practice, as suggested the research agenda item 02 in the table, e propositions should be used in empirical research to be validated and stimulate the capture of related privacy practice, as suggests the research agenda item 02 in the table.

C. TWO TYPES OF HYPOTHESES FOR FUTURE SURVEYS

This session explores two types of hypotheses that can be developed and tested through quantitative surveys.

The first type involves formulating hypotheses by scrutinizing propositions derived from the empirical studies, which is indicated in Fig. 5 by C1. These hypotheses can help to generalize statements made in the field to other contexts, providing a broader scope for these studies. To develop such hypotheses, it is possible to consider some variables, such as:

a) Organization size.
b) Type of relationship model with the market (B2C, B2B).
c) Type of capital and corporate governance structure.
d) Implementation of data privacy programs.
e) Use of tools to manage the DS rights.
f) Use of data discovery tools.
g) Use of tools for risk management and privacy impact analysis.

By analyzing these variables, it's possible identify specific profiles for certain types of organizations or practices related to the use of privacy management tools, or other combinations of these variables.

The next avenue of research, as denoted by C2 in Figure 5, entails delving into challenges and enablers that were not utilized to devise the proposed propositions. These elements, as highlighted in the review, can be converted into hypotheses by analyzing the same variables previously mentioned, in order to obtain a more in-depth comprehension of these factors, including the intricacies of each variable and their combinations. Furthermore, based on the review's source, it is feasible to generate fresh propositions applying the same rationale as presented in Section A.

D. RESEARCH AGENDA

This section summarizes in Table 12 the research agenda based on the discussion from section A, B, and C.

VI. CONCLUSION

Ensuring compliance with GDPR or other data protection laws is of utmost importance for organizations. Therefore, it is imperative to have a thorough understanding of the challenges and enablers of compliance, as this is of significant value to both the corporate world and the academic community. To this end, pertinent literature on the subject matter was scrutinized in order to generate insights and enhance the existing body of knowledge.

This study provides a valuable addition to the existing knowledge by exploring six distinct research questions, developing five conceptual propositions, and outlining a comprehensive research agenda.

The answer to the first question explains the progress of the GDPR discussion, illustrating an increasing number of publications from 2017 until 2021, stabilized until the end of 2023, the final date considered in this review. It shows that the CLSR and IEEE Access are prominent publishers in the

TABLE 13. 83 selected articles for extraction.

ID	Title	Reference	Category
1	Privacy-Preserving Solutions for Blockchain: Review and Challenges	[11]	T_BC_C
2	EU General Data Protection Regulation: Changes and implications for personal data collecting companies	[17]	DSR_C, DSR_T
3	GDPR-Compliant Personal Data Management: A Blockchain-Based Solution	[114]	GOV, T_BC_E
4	Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions	[8]	DSR_C
5	Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR	[96]	T_IoT_C
6	The right to data portability in the GDPR: Towards user-centric interoperability of digital services	[115]	DSR_C, T_BD
7	The impact of the EU general data protection regulation on scientific research	[59]	DSR_C, DSR_T
8	Smart City IoT Platform Respecting GDPR Privacy and Security Aspects	[97]	T_IoT_C, T_O
9	The Impact of GDPR on Global Technology Development	[116]	T_BC_C, DSR_C
10	Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0	[98]	T_IoT_C, DSR_C
11	The ICO and artificial intelligence: The role of fairness in the GDPR framework	[108]	T_AI_C
12	DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network	[117]	T_BC_E
13	Understanding the notion of risk in the General Data Protection Regulation	[85]	MISC
14	Designing a GDPR compliant blockchain-based IoV distributed information tracking system	[118]	T_BC_E
15	The impact of the General Data Protection Regulation on health research	[57]	DSR_C
16	When data protection by design and data subject rights clash	[73]	DSR_T, T_BD
17	Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond	[71]	DSR_T, T_AI_C
18	Data handling in industry 4.0: Interoperability based on distributed ledger technology	[101]	T_IoT_C, T_BC_E
19	GDPR Compliant Blockchains-A Systematic Literature Review	[12]	T_BC_C, T_BC_E
20	The Effect of the GDPR on Privacy Policies: Recent progress and future promise	[50]	GOV, DSR_T
21	Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective	[99]	T_IoT
22	A mapping of IoT user-centric privacy preserving approaches to the GDPR	[13]	T_IoT_C
23	The critical success factors of GDPR implementation: a systematic literature review	[10]	GOV
24	The margin between the edge of the world and infinite possibility: Blockchain, GDPR and information governance	[119]	T_BC_C, T_BC_E, GOV
25	How Data Protection Regulation Affects Startup Innovation	[79]	MISC
26	Having yes, using no? About the new legal regime for biometric data	[60]	DSR_C
27	Post-Quantum Era Privacy Protection for Intelligent Infrastructures	[111]	T_IoT_C, T_IoT_E
28	Regulatory Spillovers and Data Governance: Evidence from the GDPR	[120]	GOV, T_O
29	A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem	[102]	DSR_C, T_IoT_C, T_BC_E
30	Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency	[91]	MISC
31	Betraying Blockchain: Accountability, Transparency and Document Standards for Non-Fungible Tokens (NFTs)	[95]	T_BC_C, T_BC_E
32	Consumer Consent and Firm Targeting After GDPR: The Case of a Large Telecom Provider	[62]	DSR_C
33	Profiling tax and financial behaviour with big data under the GDPR	[110]	DSR_T, DSR_C, T_AI_C
34	Data protection, scientific research, and the role of information	[58]	DSR_T, DSR_C
35	Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach	[86]	MISC
36	Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship	[39]	GOV
37	Using artificial intelligence to support compliance with the general data protection regulation	[105]	T_IA_H
38	The benefits and challenges of general data protection regulation for the information technology sector	[49]	GOV
39	Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation	[84]	MISC

theme, considering the original samples of articles from WoS, Scopus, and the 83 selected articles performed by the review.

The second question unravels five categories that group challenges and enablers of GDPR compliance from the

TABLE 13. *(Continued.)* **83 selected articles for extraction.**

ID	Title	Reference	Category
40	An Analysis of Blockchain and GDPR under the Data Lifecycle Perspective	[121]	GOV, T_BC_E
41	From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR compliance controls	[34]	GOV
42	GDPR Interference With Next Generation 5G and IoT Networks	[112]	T_IoT_C
43	Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems	[88]	GOV
44	A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis	[92]	MISC
45	AI-Enabled Automation for Completeness Checking of Privacy Policies	[106]	GOV, T_AI_E
46	Please understand we cannot provide further information: evaluating content and transparency of GDPR-mandated AI disclosures	[109]	T_AI_C, DSR_T
47	DPIA in context: Applying DPIA to assess privacy risks of cyber physical systems	[82]	GOV
48	A Truly Future-Oriented Legal Framework for Fintech in the EU	[122]	T_BC_C
49	Semantic-based privacy settings negotiation and management	[103]	DSR_T, DSR_C, T_IoT_E
50	GDPR is here and it is time to get serious	[90]	MISC
51	Identifying critical success factors for the General Data Protection Regulation implementation in higher education institutions	[53]	DSR_C
52	Digitizing the Informed Consent Process: A Review of the Regulatory Landscape in the European Union	[67]	DSR_C
53	Fundamental rights, the normative keystone of DPIA	[87]	GOV
54	DAISY: A Data Information System for accountability under the General Data Protection Regulation	[48]	DSR_C, DSR_T, GOV
55	The Internet of Things ecosystem: The blockchain and data protection issues	[100]	T_IoT_C, T_BC_C, T_BC_E
56	The DAta Protection REgulation COmpliance Model	[36]	GOV, T_O
57	Design of a Compliance Index for Privacy Policies: A Study of Mobile Wallet and Remittance Services	[89]	GOV
58	Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think	[81]	GOV
59	Making Sense of Solid for Data Governance and GDPR	[32]	T_O
60	Finding, getting and understanding: the user journey for the GDPR's right to access	[72]	DSR_T
61	Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation	[78]	T_O
62	ISO/IEC 27701 standard: Threats and opportunities for GDPR certification	[33]	GOV
63	An AI framework to support decisions on GDPR compliance	[107]	T_AI_E
64	TR-Model. A Metadata Profile Application for Personal Data Transparency	[70]	DSR_T
65	GDPR compliance: proposed technical and organizational measures for cloud provider	[51]	GOV
66	Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?	[104]	T_AI_C
67	Building data management capabilities to address data protection regulations: Learnings from EU-GDPR	[123]	DSR_C
68	Five Ways to GDPR-Compliant Use of Blockchains	[124]	T_BC_E
69	Consent Verification Monitoring	[65]	DSR_C
70	Greece: The new data protection framework	[76]	GOV
71	Portugal: A Brief Overview of the GDPR Implementation	[75]	MISC
72	Factors determining the extent of GDPR implementation within organizations: Empirical evidence from Czech Republic	[77]	GOV
73	Formal models for consent-based privacy	[66]	DSR_C, T_BD
74	Technical Requirements and Approaches in Personal Data Control	[63]	DSR_C
75	Governance team leadership and business user participation: organizational practices for innovative customer engagement in data compliance project	[55]	GOV
76	Privacy Goals for the Data Lifecycle	[83]	DSR_C, DSR_T
77	A GDPR-Compliant Dynamic Consent Mobile Application for the Australasian Type-1 Diabetes Data Network	[69]	DSR_C, T_AI_E

review. Each selected article was usually associated with one to three categories. The first category, GOV, is related to GDPR and IG, EAM, ISO-based roadmaps, generic challenges, and enablers for compliance. The second and third

TABLE 13. *(Continued.)* **83 selected articles for extraction.**

ID	Title	Reference	Category
78	Consent for processing children's personal data in the EU: following in US footsteps?	[61]	DSR_C
79	Does personal data protection matter for ISO 9001 certification and firm performance?	[52]	GOV
80	The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law	[80]	T_O
81	The generic Informed Consent Service gICS®: implementation and benefits of a modular consent software tool to master the challenge of electronic consent management in research	[68]	DSR_C
82	Practical Privacy: Report from the GDPR World	[74]	GOV
83	Towards a readiness model derived from critical success factors, for the general data protection regulation implementation in higher education institutions	[125]	GOV, DSR_C, DSR_T

categories are related to DS rights to consent and transparency, respectively. The fourth category, MISC, concerns regulations in countries, GDPR and innovation, DPIA, and others. The fifth one is the technology category, discussed in the answer to the fifth question.

The answer to the third question regarding references or models that have been applied to reach GDPR compliance reveals that the use of ISO-based and other frameworks alone may result in incomplete compliance due to gaps in requirements such as DS rights, records of process activity, data sharing management, and PD collection. The development of this question helps to figure out a proposal for future research to construct an IG model for PD, considering components to represent the process and information structure using EA artifacts.

The fourth question was explained by each of the first four categories of challenges and enablers discovered by the review. These factors have three critical implications. Firstly, they highlight particular challenges and enablers that could be explored in future empirical research to support five propositions. Secondly, the main challenges and enablers from the review that were irrelevant to the propositions could be used to develop new hypotheses and variables for conceptual works, paving the way for further research. Finally, the third contribution suggests that new hypotheses could be formulated to generalize the results to other contexts using suggested variables once empirical research using the propositions is conducted.

The fifth question on how technology impacts GDPR compliance has been answered by analyzing the fifth category, decomposed into seven subcategories. Six of them focus on specific technologies, such as blockchain, IoT, and AI, either as enablers or challenges for compliance. The seventh subcategory (T-O) deals with technologies not mentioned above, such as GDPR, 5G, and quantum computing. One significant discovery in this category is the Solid project led by Tim Berners-Lee. The project proposes a revolutionary approach to privacy by creating a decentralized platform for data exchange. It aims to give users control over their data, moving away from the control of controllers.

The research agenda that answers the sixth question includes a contrivance to build a conceptual IG model, suggests empirical research to confront the propositions in the field, recommends the construction of new hypotheses after the execution of the empirical research to expand the context of the findings, considering other variables and, finally, proposes the design of new hypotheses or propositions considering the remaining challenges and enablers identified in the review.

This study has inherent limitations due to its research design, particularly the selection of samples from the first four steps of the phase I proposed to build the research protocol. The choice of academic databases, timeliness, search strings, inclusion and exclusion criteria, and a manual process may narrow the final sample. Moreover, this research is exploratory, and the content analysis of the final sample is subjective, particularly regarding the identification of challenges and enablers in each article and the proposed classification. Nonetheless, the authors have decided to focus their research agenda primarily on the IG model to cover the gap in the use of ISO-based standards for GDPR compliance and in the conceptual design of the propositions.

Hence, this SLR reach the objective to deep the knowledge about GDPR research regarding its challenges and enablers and to provide a comprehensive research agenda.

APPENDIX

See Table 13.

REFERENCES

[1] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Rev.*, vol. 4, no. 5, p. 193, Dec. 1890, doi: 10.2307/1321160.

[2] UN General Assembly. (1948). *Universal Declaration of Human Rights*. UN Gen. Assem. Accessed: Sep. 8, 2023. [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[3] P. Regulation, *Regulation (EU) 2016/679 of the European Parliament and of the Council*. Brussels, Belgium: Regulation (EU), 2016, p. 679.

[4] A. F. S. Borges, F. J. B. Laurindo, M. M. Spínola, R. F. Gonçalves, and C. A. Mattos, "The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions," *Int. J. Inf. Manage.*, vol. 57, Apr. 2021, Art. no. 102225.

[5] S. Dash, S. K. Shakyawar, M. Sharma, and S. Kaushik, "Big data in healthcare: Management, analysis and future prospects," *J. Big Data*, vol. 6, no. 1, pp. 1–25, Dec. 2019.

[6] V. Venkatraman, *The Digital Matrix: New Rules for Business Transformation through Technology*. Los Angeles, CA, USA: LifeTree Media, 2017.

[7] S. Agarwal, "Towards dealing with GDPR uncertainty," in *Proc. 11th IFIP Summer School Privacy Identity Manag.*, Karlstad, Sweden, Aug. 2016, pp. 1–7.

[8] E. Politou, E. Alepis, and C. Patsakis, "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," *J. Cybersecurity*, vol. 4, no. 1, Jan. 2018, Art. no. tyy001.
[9] G. A. Teixeira, M. M. da Silva, and R. Pereira, "The critical success factors of GDPR implementation: A Delphi study," in *Information Systems Development: Crossing Boundaries between Development and Operations (DevOps)*, E. Insfran, F. González, S. Abrahão, M. Fernández, C. Barry, H. Linger, M. Lang, and C. Schneider, Eds. Valencia, Spain: Universitat Politécnica de Valéncia, 2021.
[10] G. A. Teixeira, M. M. da Silva, and R. Pereira, "The critical success factors of GDPR implementation: A systematic literature review," *Digit. Policy, Regulation Governance*, vol. 21, no. 4, pp. 402–418, Jun. 2019.
[11] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.
[12] A. B. Haque, A. K. M. N. Islam, S. Hyrynsalmi, B. Naqvi, and K. Smolander, "GDPR compliant blockchains—A systematic literature review," *IEEE Access*, vol. 9, pp. 50593–50606, 2021.
[13] A. D. Kounoudes and G. M. Kapitsaki, "A mapping of IoT user-centric privacy preserving approaches to the GDPR," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100179.
[14] M. Batikas, C. Peukert, S. Bechtold, and T. Kretschmer, "European privacy law and global markets for data," *Acad. Manage. Proc.*, vol. 2021, no. 1, p. 12506, Aug. 2021.
[15] G. Greeleaf. (2023). *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills*," Privacy Laws and Business International Report (PLBIR). Accessed: Sep. 8, 2023. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146
[16] P. Voigt and A. von dem Bussche, *The EU Gen. Data Protection Regulation (GDPR): A Practical Guide*, vol. 10, 1st ed. Cham: Springer International Publishing, 2017, p. 5555.
[17] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU general data protection regulation: Changes and implications for personal data collecting companies," *Comput. Law Secur. Rev.*, vol. 34, no. 1, pp. 134–153, Feb. 2018.
[18] M. D. C. Freitas and M. Mira da Silva, "GDPR compliance in SMEs: There is much to be done," *J. Inf. Syst. Eng. Manage.*, vol. 3, no. 4, p. 30, Nov. 2018.
[19] C. Addis and M. Kutar, "The General Data Protection Regulation (GDPR), emerging technologies and UK organisations: Awareness, implementation and readiness," in *Proc. UK Acad. Inf. Syst. Conf.*, 2018, p. 29.
[20] L. Magnusson and S. Iqbal, "Implications of EU-GDPR in low-grade social, activist and NGO settings," *Int. J. Bus. Technol.*, vol. 6, no. 3, pp. 1–7, May 2018.
[21] J. Khan, "The need for continuous compliance," *Netw. Secur.*, vol. 2018, no. 6, pp. 14–15, Jun. 2018, doi: 10.1016/S1353-4858%2818%2930057-6.
[22] P. Lindgren, "GDPR regulation impact on different Bus. Models and businesses," *J. Multi Bus. Model Innov. Technol.*, vol. 4, no. 3, pp. 241–254, 2018. [Online]. Available: http://www.riverpublishers.com/journal_read_html_article.php?j=JMBMIT/4/3/4
[23] W. Presthus and H. Sørum, "Are consumers concerned about privacy? An online survey emphasizing the general data protection regulation," *Proc. Comput. Sci.*, vol. 138, pp. 603–611, Jan. 2018.
[24] D. Allen, A. Berg, C. Berg, and J. Potts, "Some economic consequences of the GDPR," *SSRN Electron. J.*, vol. 39, no. 2, pp. 785–797, Jan. 2018. Accessed: Sep. 8, 2023. [Online]. Available: https://www.ssrn.com/abstract=3160404
[25] E. van der Marel, M. Bauer, H. Lee-Makiyama, and B. Verschelde, "A methodology to estimate the costs of data regulations," *Int. Econ.*, vol. 146, pp. 12–39, Aug. 2016.
[26] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quart.*, vol. 26, no. 2, pp. 8–23, 2002.
[27] Y. Levy and T. J. Ellis, "A systems approach to conduct an effective literature review in support of information systems research," *Informing Sci., Int. J. Emerg. Transdiscipline*, vol. 9, pp. 181–212, Jan. 2006.
[28] B. Kitchenham and S. Charters, *Guidelines for Performing Systematic Literature Reviews in Software Engineering*, document EBSE/EPIC-2007-01, 2007.
[29] S. Fabbri, C. Silva, E. Hernandes, F. Octaviano, A. Di Thommazo, and A. Belgamo, "Improvements in the StArt tool to better support the systematic review process," in *Proc. 20th Int. Conf. Eval. Assessment Softw. Eng.*, Jun. 2016, pp. 1–5.
[30] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, May 2014, pp. 1–10.
[31] E. Z. Milian, M. D. M. Spinola, and M. M. D. Carvalho, "Fintechs: A literature review and research agenda," *Electron. Commerce Res. Appl.*, vol. 34, Mar. 2019, Art. no. 100833. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1567422319300109
[32] H. J. Pandit,"Making sense of solid for data governance and GDPR," *Information*, vol. 14, no. 2, p. 114, Feb. 2023.
[33] E. Lachaud, "ISO/IEC 27701 standard: Threats and opportunities for GDPR certification," *Eur. Data Protection Law Rev.*, vol. 6, no. 2, pp. 194–210, 2020.
[34] V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR compliance controls," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 645–662, 2020.
[35] M. J. Anwar and A. Gill, "Developing an integrated ISO 27701 and GDPR based information privacy compliance requirements model," in *Proc. Australas. Conf. Inf. Syst.*, 2020, pp. 1–12.
[36] C. Bartolini, G. Lenzini, and L. Robaldo, "The DAta protection REgulation COmpliance model," *IEEE Secur. Privacy*, vol. 17, no. 6, pp. 37–45, Nov. 2019.
[37] A. Gobeo, C. Fowler, and W. J. Buchanan, *GDPR and Cyber Security for Business Information Systems*. Boca Raton, FL, USA: CRC Press, 2022.
[38] A. D. S. Dharni, "Data privacy compliance using COBIT 2019 and development of MISAM audit caselet," Concordia Univ. Edmonton, Canada, Project Rep., pp. 1–36, 2020.
[39] K. Yeung and L. A. Bygrave, "Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship," *Regulation Governance*, vol. 16, no. 1, pp. 137–155, Jan. 2022.
[40] C. B. Assis, "Information governance: Enablers and inhibitors for organizational adoption," Ph.D. dissertation, Polytechnic School, Univ. São Paulo, São Paulo, 2018, doi: 10.11606/T.3.2018.tde-27042018-102121.
[41] CGOC Compliance, Governance and Oversight Council, "CGOC information governance benchmark survey report," , Ph.D. dissertation, Information governance: Enablers and Inhibitors Organizational Adoption, Dept. Prod. Eng., Polytech. School, Univ. São Paulo, São Paulo, Brazil, 2018.
[42] F. Burmeister, P. Drews, and I. Schirmer, "A privacy-driven enterprise architecture meta-model for supporting compliance with the General Data Protection Regulation," Tech. Rep., 2019.
[43] M. Hauder, "Organizational factors influencing enterprise architecture management challenges," in *Proc. 21st Eur. Conf. Inf. Syst. (ECIS)*, Utrecht, The, Netherlands, Jun. 2013, pp. 1–12.
[44] T. T. Lajara and A. C. G. Maçada, "Information governance framework: The defense manufacturing case study," in *Proc. 19th Americas Conf. Inf. Syst.*, Chicago, IL, USA, Aug. 2013, pp. 1–10.
[45] F. Burmeister, D. Huth, P. Drews, I. Schirmer, and F. Matthes, "Enhancing information governance with enterprise architecture management: Design principles derived from benefits and barriers in the GDPR implementation," in *Proc. 53rd Hawaii Int. Conf. Syst. Sci.* Hawaii: Univ. of Hawai'i at Mānoa, 2020, pp. 5593–5602.
[46] D. Huth, A. Tanakol, and F. Matthes, "Using enterprise architecture models for creating the record of processing activities (Art. 30 GDPR)," in *Proc. IEEE 23rd Int. Enterprise Distrib. Object Comput. Conf. (EDOC)*, Oct. 2019, pp. 98–104.
[47] E. Truli, *The General Data Protection Regulation and Civil Liability*. Berlin, Germany: Springer, 2018.
[48] R. Becker, P. Alper, V. Grouès, S. Munoz, Y. Jarosz, J. Lebioda, K. Rege, C. Trefois, V. Satagopam, and R. Schneider, "DAISY: A data information system for accountability under the general data protection regulation," *GigaScience*, vol. 8, no. 12, Dec. 2019, Art. no. giz140.
[49] N. Poritskiy, F. Oliveira, and F. Almeida, "The benefits and challenges of general data protection regulation for the information technology sector," *Digit. Policy, Regulation Governance*, vol. 21, no. 5, pp. 510–524, Aug. 2019.
[50] R. N. Zaeem and K. S. Barber, "The effect of the GDPR on privacy policies: Recent progress and future promise," *ACM Trans. Manage. Inf. Syst.*, vol. 12, no. 1, pp. 1–20, Mar. 2021.
[51] Z. Georgiopoulou, E.-L. Makri, and C. Lambrinoudakis, "GDPR compliance: Proposed technical and organizational measures for cloud provider," *Inf. Comput. Secur.*, vol. 28, no. 5, pp. 665–680, Jun. 2020.

[52] E. Siougle, S. Dimelis, and N. Malevris, "Does personal data protection matter for ISO 9001 certification and firm performance?" *Int. J. Productiv. Perform. Manage.*, vol. 73, no. 3, pp. 749–774, Mar. 2024.

[53] J. Fernandes, C. Machado, and L. Amaral, "Identifying critical success factors for the general data protection regulation implementation in higher education institutions," *Digit. Policy, Regulation Governance*, vol. 24, no. 4, pp. 355–379, Sep. 2022.

[54] P. P. Tallon, R. V. Ramirez, and J. E. Short, "The information artifact in IT governance: Toward a theory of information governance," *J. Manage. Inf. Syst.*, vol. 30, no. 3, pp. 141–178, Dec. 2013.

[55] M. Vojvodic and C. Hitz, "Governance team leadership and business user participation: Organizational practices for innovative customer engagement in data compliance project," *Central Eur. Bus. Rev.*, vol. 8, no. 2, pp. 15–45, 2019.

[56] *COBIT 2019 Framework: Governance and Management Objectives*, ISACA, Schaumburg, IL, USA, 2018, p. 300.

[57] V. Chico, "The impact of the general data protection regulation on health research," *Brit. Med. Bull.*, vol. 128, no. 1, pp. 109–118, Dec. 2018.

[58] R. Ducato, "Data protection, scientific research, and the role of information," *Comput. Law Secur. Rev.*, vol. 37, Jul. 2020, Art. no. 105412.

[59] G. Chassang, "The impact of the EU general data protection regulation on scientific research," *ecancermedicalscience*, vol. 11, pp. 1–12, Jan. 2017.

[60] E. J. Kindt, "Having yes, using no? About the new legal regime for biometric data," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 523–538, Jun. 2018.

[61] M. Macenaite and E. Kosta, "Consent for processing children's personal data in the EU: Following in US footsteps?" *Inf. Commun. Technol. Law*, vol. 26, no. 2, pp. 146–197, May 2017.

[62] M. G. de Matos and I. Adjerid, "Consumer consent and firm targeting after GDPR: The case of a large telecom provider," *Manage. Sci.*, vol. 68, no. 5, pp. 3330–3378, May 2022.

[63] J. Sim, B. Kim, K. Jeon, M. Joo, J. Lim, J. Lee, and K.-K.-R. Choo, "Technical requirements and approaches in personal data control," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–30, Sep. 2023.

[64] M. Robol, "Modeling and reasoning about privacy-consent requirements," in *Proc. Modeling Reasoning About Privacy-Consent Requirements*, Vienna, Austria. Cham, Switzerland: Springer, Oct. 2018, pp. 238–254.

[65] M. Robol, T. D. Breaux, E. Paja, and P. Giorgini, "Consent verification monitoring," *ACM Trans. Softw. Eng. Methodol.*, vol. 32, no. 1, pp. 1–33, Jan. 2023.

[66] N. Peyrone and D. Wichadakul, "Formal models for consent-based privacy," *J. Log. Algebr. Methods Program.*, vol. 128, Aug. 2022, Art. no. 100789.

[67] E. De Sutter, J. Meszaros, P. Borry, and I. Huys, "Digitizing the informed consent process: A review of the regulatory landscape in the European union," *Frontiers Med.*, vol. 9, p. 1445, May 2022.

[68] H. Rau, L. Geidel, M. Bialke, A. Blumentritt, M. Langanke, W. Liedtke, S. Pasewald, D. Stahl, T. Bahls, C. Maier, H.-U. Prokosch, and W. Hoffmann, "The generic informed consent service gICS: Implementation and benefits of a modular consent software tool to master the challenge of electronic consent management in research," *J. Transl. Med.*, vol. 18, no. 1, pp. 1–12, Dec. 2020.

[69] Z. Wang, A. Stell, and R. O. Sinnott, "A GDPR-compliant dynamic consent mobile application for the Australasian type-1 diabetes data network," *Healthcare*, vol. 11, no. 4, p. 496, Feb. 2023.

[70] T. A. Coleti, P. L. P. Corrêa, L. V. L. Filgueiras, and M. Morandini, "TR-model. A metadata profile application for personal data transparency," *IEEE Access*, vol. 8, pp. 75184–75209, 2020.

[71] M. Brkan, "Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond," *Int. J. Law Inf. Technol.*, vol. 27, no. 2, pp. 91–121, Jun. 2019.

[72] D. Pins, T. Jakobi, G. Stevens, F. Alizadeh, and J. Krüger, "Finding, getting and understanding: The user journey for the GDPR'S right to access," *Behaviour Inf. Technol.*, vol. 41, no. 10, pp. 2174–2200, Jul. 2022.

[73] M. Veale, R. Binns, and J. Ausloos, "When data protection by design and data subject rights clash," *Int. Data Privacy Law*, vol. 8, no. 2, pp. 105–123, May 2018.

[74] S. Doe, "Practical privacy: Report from the GDPR world," *Legal Inf. Manage.*, vol. 18, no. 2, pp. 76–79, Jun. 2018.

[75] A. B. Cordeiro, "Portugal: A brief overview of the GDPR implementation," *Eur. Data Protection Law Rev.*, vol. 5, p. 533, Jan. 2019.

[76] L. Mitrou, "Greece: The new data protection framework," *Eur. Data Protection Law Rev.*, vol. 6, p. 107, Feb. 2020.

[77] A. Faifr and M. Januška, "Factors determining the extent of GDPR implementation within organizations: Empirical evidence from Czech Republic," *J. Bus. Econ. Manag.*, vol. 22, no. 5, pp. 1611–1699, 2021.

[78] E. D. Canedo, A. T. S. Calazans, I. N. Bandeira, P. H. T. Costa, and E. T. S. Masson, "Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation," *Requirements Eng.*, vol. 27, no. 4, pp. 545–567, Dec. 2022.

[79] N. Martin, C. Matt, C. Niebel, and K. Blind, "How data protection regulation affects startup innovation," *Inf. Syst. Frontiers*, vol. 21, no. 6, pp. 1307–1324, Dec. 2019.

[80] R. Gadoni Canaan, "The effects on local innovation arising from replicating the GDPR into the Brazilian general data protection law," *Internet Policy Rev.*, vol. 12, no. 1, pp. 1–15, Feb. 2023.

[81] G. Comandè and G. Schneider, "Differential data protection regimes in data-driven research: Why the GDPR is more research-friendly than you think," *German Law J.*, vol. 23, no. 4, pp. 559–596, May 2022.

[82] J. Henriksen-Bulmer, S. Faily, and S. Jeary, "DPIA in context: Applying DPIA to assess privacy risks of cyber physical systems," *Future Internet*, vol. 12, no. 5, p. 93, May 2020.

[83] J. Henriksen-Bulmer, C. Yucel, S. Faily, and I. Chalkias, "Privacy goals for the data lifecycle," *Future Internet*, vol. 14, no. 11, p. 315, Oct. 2022.

[84] K. Demetzou, "Data protection impact assessment: A tool for accountability and the unclarified concept of 'high risk' in the general data protection regulation," *Comput. Law Secur. Rev.*, vol. 35, no. 6, Nov. 2019, Art. no. 105342.

[85] R. Gellert, "Understanding the notion of risk in the general data protection regulation," *Comput. Law Secur. Rev.*, vol. 34, no. 2, pp. 279–288, Apr. 2018.

[86] C. Quelle, "Enhancing compliance under the general data protection regulation: The risky upshot of the accountability- and risk-based approach," *Eur. J. Risk Regulation*, vol. 9, no. 3, pp. 502–526, Sep. 2018.

[87] D. Hallinan and N. Martin, "Fundamental rights, the normative keystone of DPIA," *Eur. Data Protection Law Rev.*, vol. 6, no. 2, pp. 178–193, 2020.

[88] M. Todde, M. Beltrame, S. Marceglia, and C. Spagno, "Methodology and workflow to perform the data protection impact assessment in healthcare information systems," *Informat. Med. Unlocked*, vol. 19, Jan. 2020, Art. no. 100361.

[89] O. Akanfe, R. Valecha, and H. R. Rao, "Design of a compliance index for privacy policies: A study of mobile wallet and remittance services," *IEEE Trans. Eng. Manag.*, vol. 70, no. 3, pp. 864–876, Mar. 2023.

[90] G. Miglicco, "GDPR is here and it is time to get serious," *Comput. Fraud Secur.*, vol. 2018, no. 9, pp. 9–12, Jan. 2018.

[91] M. Hintze, "Viewing the GDPR through a de-identification lens: A tool for compliance, clarification, and consistency," *Int. Data Privacy Law*, vol. 8, no. 1, pp. 86–101, Feb. 2018.

[92] M. Christofidou, N. Lea, and P. Coorevits, "A literature review on the GDPR, COVID-19 and the ethical considerations of data protection during a time of crisis," *Yearbook Med. Informat.*, vol. 30, no. 1, pp. 226–232, Aug. 2021.

[93] M. Gharib, P. Giorgini, and J. Mylopoulos, "An ontology for privacy requirements via a systematic literature review," *J. Data Semantics*, vol. 9, no. 4, pp. 123–149, Dec. 2020.

[94] A. K. M. N. Islam, M. Mäntymäki, and M. Turunen, "Why do blockchains split? An actor-network perspective on Bitcoin splits," *Technolog. Forecasting Social Change*, vol. 148, Nov. 2019, Art. no. 119743.

[95] K. Cornelius, "Betraying blockchain: Accountability, transparency and document standards for non-fungible tokens (NFTs)," *Information*, vol. 12, no. 9, p. 358, Aug. 2021.

[96] S. Wachter, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 436–449, Jun. 2018.

[97] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Smart city IoT platform respecting GDPR privacy and security aspects," *IEEE Access*, vol. 8, pp. 23601–23623, 2020.

[98] X. Larrucea, M. Moffie, S. Asaf, and I. Santamaria, "Towards a GDPR compliant way to secure European cross border healthcare Industry 4.0," *Comput. Standards Interface*, vol. 69, Mar. 2020, Art. no. 103408.

[99] M. N. Asghar, N. Kanwal, B. Lee, M. Fleury, M. Herbst, and Y. Qiao, "Visual surveillance within the EU general data protection regulation: A technology perspective," *IEEE Access*, vol. 7, pp. 111709–111726, 2019.

[100] N. Fabiano, "The Internet of Things ecosystem: The blockchain and privacy Issues. The challenge for a global privacy standard," *Adv. Sci., Technol. Eng. Syst.*, vol. 3, no. 2, pp. 1–7, 2018.
[101] S. Sun, X. Zheng, J. Villalba-Díez, and J. Ordieres-Meré, "Data handling in Industry 4.0: Interoperability based on distributed ledger technology," *Sensors*, vol. 20, no. 11, p. 3046, May 2020.
[102] K. Rantos, G. Drosatos, A. Kritsas, C. Ilioudis, A. Papanikolaou, and A. P. Filippidis, "A blockchain-based platform for consent management of personal data processing in the IoT ecosystem," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Oct. 2019.
[103] O. R. Sanchez, I. Torre, and B. P. Knijnenburg, "Semantic-based privacy settings negotiation and management," *Future Gener. Comput. Syst.*, vol. 111, pp. 879–898, Oct. 2020.
[104] P. T. Kramcsák, "Can legitimate interest be an appropriate lawful basis for processing artificial intelligence training datasets?" *Comput. Law Secur. Rev.*, vol. 48, Apr. 2023, Art. no. 105765.
[105] J. Kingston, "Using artificial intelligence to support compliance with the general data protection regulation," *Artif. Intell. Law*, vol. 25, no. 4, pp. 429–443, Dec. 2017.
[106] O. Amaral, S. Abualhaija, D. Torre, M. Sabetzadeh, and L. C. Briand, "AI-enabled automation for completeness checking of privacy policies," *IEEE Trans. Softw. Eng.*, vol. 48, no. 11, pp. 4647–4674, Nov. 2022.
[107] F. Lorè, P. Basile, A. Appice, M. de Gemmis, D. Malerba, and G. Semeraro, "An AI framework to support decisions on GDPR compliance," *J. Intell. Inf. Syst.*, vol. 61, no. 2, pp. 541–568, Oct. 2023.
[108] M. Butterworth, "The ICO and artificial intelligence: The role of fairness in the GDPR framework," *Comput. Law Secur. Rev.*, vol. 34, no. 2, pp. 257–268, Apr. 2018.
[109] A. J. Wulf and O. Seizov, "Please understand we cannot provide further information: Evaluating content and transparency of GDPR-mandated AI disclosures," *AI & Society*, vol. 39, pp. 235–256, May 2022.
[110] E. Politou, E. Alepis, and C. Patsakis, "Profiling tax and financial behaviour with big data under the GDPR," *Comput. Law Secur. Rev.*, vol. 35, no. 3, pp. 306–329, May 2019.
[111] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevicius, A.-A.-O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, "Post-quantum era privacy protection for intelligent infrastructures," *IEEE Access*, vol. 9, pp. 36038–36077, 2021.
[112] S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, "GDPR interference with next generation 5G and IoT networks," *IEEE Access*, vol. 8, pp. 108052–108061, 2020.
[113] P. A. C. Miguel, "Case research in production engineering: Structure and recommendations for its conduction," *Production*, vol. 17, no. 1, pp. 216–229, Apr. 2007.
[114] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A blockchain-based solution," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1746–1761, 2020.
[115] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, and I. Sanchez, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services," *Comput. Law Secur. Rev.*, vol. 34, no. 2, pp. 193–203, Apr. 2018.
[116] H. Li, L. Yu, and W. He, "The impact of GDPR on global technology development," *J. Global Inf. Technol. Manage.*, vol. 22, no. 1, pp. 1–6, Jan. 2019.
[117] J. A. Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, "DNS-IdM: A blockchain identity management system to secure personal data sharing in a network," *Appl. Sci.*, vol. 9, no. 15, p. 2953, Jul. 2019.
[118] L. Campanile, M. Iacono, F. Marulli, and M. Mastroianni, "Designing a GDPR compliant blockchain-based IoV distributed information tracking system," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102511.
[119] D. Hofman, V. L. Lemieux, A. Joo, and D. A. Batista, "'The margin between the edge of the world and infinite possibility': Blockchain, GDPR and information governance," *Records Manage. J.*, vol. 29, nos. 1–2, pp. 240–257, Mar. 2019.
[120] C. Peukert, S. Bechtold, M. Batikas, and T. Kretschmer, "Regulatory spillovers and data governance: Evidence from the GDPR," *Marketing Sci.*, vol. 41, no. 4, pp. 746–768, Jul. 2022.
[121] G. P. Freund, P. B. Fagundes, and D. D. J. de Macedo, "An analysis of blockchain and GDPR under the data lifecycle perspective," *Mobile Netw. Appl.*, vol. 26, no. 1, pp. 266–276, Feb. 2021.
[122] I. Kapsis, "A truly future-oriented legal framework for fintech in the EU," *Eur. Bus. Law Rev.*, vol. 31, no. Issue 3, pp. 475–514, May 2020.
[123] C. Labadie and C. Legner, "Building data management capabilities to address data protection regulations: Learnings from EU-GDPR," *J. Inf. Technol.*, vol. 38, no. 1, pp. 16–44, Mar. 2023.
[124] J. Erbguth, "Five ways to GDPR-compliant use of blockchains," *Eur. Data Prot. L. Rev.*, vol. 5, p. 427, Jan. 2019.
[125] J. Fernandes, C. Machado, and L. Amaral, "Towards a readiness model derived from critical success factors, for the general data protection regulation implementation in higher education institutions," *Strategic Manage.*, vol. 28, no. 1, pp. 4–19, 2023.

NEMER ALBERTO ZAGUIR was born in São Paulo, Brazil, in 1965. He received the B.S. degree from the Physics Institute at the University of São Paulo (USP) in 1987, a certificate in project management from George Washington University, and the M.S. and Ph.D. degrees from the Production Engineering Department at the Polytechnic School of the USP in 2017 and 2024, respectively. Nemer is an experienced business and IT leader focused on developing enterprise transformation and technology programs to drive operational efficiency and growth. His research interests include technology adoption, IT business strategic alignment, industry 4.0, artificial intelligence, innovation management, and information governance.

GUILHERME HENRIQUE DE MAGALHÃES was born in Alvinópolis, Minas Gerais, Brazil, in 1993. He received the B.S. degree in production engineering from the Federal University of Ouro Preto, in 2019, and the M.B.A. degree in data engineering from XP Education, in 2023. He is currently pursuing the M.S. degree with the Production Engineering Department, Polytechnic School, University of São Paulo (EPUSP). His research interests include production engineering, information technology management, enterprise architecture management, artificial intelligence, cloud computing, and industry 4.0.

MAURO DE MESQUITA SPINOLA was born in São Paulo, Brazil, in 1956. He received the B.S. degree in electronics engineering from the Technological Institute of Aeronautics (ITA), in 1979, the M.S. degree in applied computing from the National Institute of Space Research (INPE), in 1986, and the Ph.D. degree in engineering from the Polytechnic School, University of São Paulo (EPUSP), in 1999. He is currently an Associate Professor with the Production Engineering Department, EPUSP. His current research interests include production engineering, information technology management, software production, artificial intelligence, and industry 4.0.