Requirements Engineering
https://doi.org/10.1007/s00766-024-00423-4

ORIGINAL ARTICLE

Understanding the GDPR from a requirements engineering perspective—a systematic mapping study on regulatory data protection requirements

Claudia Negri-Ribalta[1,2] · Marius Lombard-Platet[2] · Camille Salinesi[1]

Received: 28 October 2023 / Accepted: 24 May 2024

Abstract

Data protection compliance is critical from a requirements engineering (RE) perspective, both from a software development lifecycle (SDLC) perspective and regulatory compliance. Not including these requirements from the early phases of the SDLC can prove costly and challenging afterward. The general data protection regulation (GDPR) from the European Union (EU) sets a list of requirements that organizations working within its scope should satisfy. However, these requirements are complex to work with, as legal prose tends to be vague and imprecise, and not all requirements have received the same attention from researchers. This study aims to identify the research published in RE for helping compliance with regulatory data protection requirements. We gathered and analyzed 90 articles from 2016 to 2022 through a systematic mapping study. We analyzed key trends in the sample, such as year of publication, publication venue, type of research, interdisciplinarity in the author's background, GDPR focus of compliance element, and type of proposal. Our main findings show ongoing interest, mostly published in conferences, in achieving overall compliance with the GDPR and consent as the most popular topics. Other topics, such as cookies or children's data, did not receive significant attention. Research over the whole RE process has been done. 20 (22%) of the papers have authors affiliated with non-computer science; however, most research seems not interdisciplinary. We finally discuss gaps in the literature, possible future areas of research, and the importance of interdisciplinary research for regulatory data protection requirements in RE.

Keywords Requirements · Compliance · Systematic mapping · Data protection · GDPR

1 Introduction

The general data protection regulation (GDPR) is an EU regulation that defines personal data lifecycle requirements at a European level. It ranges from data subjects' rights, fines, policies, or business processes. For example, fines for non-compliance can be up to 20 million euros, or up to 4% of the company's yearly global turnover [1]. Thus, entities working with information systems (IS) must pay close attention to the legal requirements, as non-compliance might cause them (on top of fines) a loss of reputation and increased human and monetary spending.

Even though 5 years have passed, companies are still regularly fined. For instance, in January 2023, Meta received a 390,000,000€ fine from the Irish Data Protection Commission [2]. According to [3], EU-wide, more than 1000 fines have been given between July 2018 and March 2022 for violations of GDPR. The average fine was of around 1 500 000€, the highest being a 746,000,000€ fine for Amazon Luxembourg, in July 2021, at the time of this paper's writing.

As such, it is clear that GDPR is, at best, partially implemented by many private actors despite the strong financial incentive to achieve compliance. In this context, the need

✉ Claudia Negri-Ribalta
claudia.negriribalta@uni.lu

Marius Lombard-Platet
marius.lombard-platet@uni.lu

Camille Salinesi
camille.salinesi@univ-paris1.fr

[1] Centre de Recherche en Informatique, Université Paris 1 Panthéon-Sorbonne, 75000 Paris, France

[2] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, 2 avenue de l'université, 10587 Belval, Luxembourg

Published online: 10 July 2024

to include GDPR and privacy requirements in the software development life cycle (SDLC) becomes imperative. However, handling requirements emanating from regulations and legal documents is challenging [4, 5]. This situation arises due to the conflicting nature of legal prose versus requirements and the SDLC [6, 7]. Legal prose tends to be vague, so it can travel through time and be applied in multiple contexts. Conversely, RE aims at having precise requirements [8, 9].

To address this issue, requirement engineering researchers have proposed, over the last years, various artifacts to tackle diverse aspects of GDPR compliance—either from a technical point of view or following a wider interdisciplinary approach. This paper aims to map and identify the approaches RE has proposed for GDPR compliance and understand the current state of the art through a systematic approach. Through a systematic mapping study, the objective is to identify what has been proposed and future areas of research, venues, and research methodology. Consequently, the results are to provide the reader with an exhaustive list of the artifacts proposed in the RE for GDPR compliance. The expected outcome is a list of diverse artifacts, ranging from frameworks to extensions of conceptual languages.

2 Background and related work

RE has a longstanding history with regulatory data protection requirements. In the early stages, the RE community researched and proposed about safety requirements for critical systems. Multiple lines of research have concluded that software engineers find regulatory requirements—including data protection regulations—challenging to understand and translate into the information system [4, 6, 10–14].

2.1 Privacy versus data protection regulatory requirements

There are several challenges with privacy requirements. Firstly, the definition of privacy may vary due to cultural elements, personal preferences, and conceptualization [15]. Given this situation, privacy can be a vague term that may encompass different issues [15]. Therefore, regulations dealing with personal data prefer to regulate information privacy or data protection—that is to say, issues regarding allowing the data subject to determine by themselves which type of personal data, how and when will be shared, including its' life cycle, in line with [16] definition of privacy[1] In other words, as a generalization, it is the individual who chooses how their data should be processed rather than the system itself..

Privacy requirements also differ from data protection regulatory requirements because the latter seeks to set requirements in one specific aspect of the former. Regulatory data protection requirements emanate from a regulation or legal body. Therefore, regulatory requirements come from a specific type of document(s) and may signal specific requirements. For example, regulation can mandate organizational requirements such as appointing a data protection officer or identifying the entity responsible for data processing—such as the [1]—which might not be present as an element in a privacy ontology. Using Glinz [9] taxonomy on requirements, regulatory requirements for data protection could be labeled as constraints. Even if the stakeholders do not agree on a requirement set by the regulation—for example, appointing a DPO—this requirement is a restriction set by the regulation—in our example, the GDPR [1]—.

Furthermore, working with regulatory requirements for data protection requires specific knowledge and expertise about that specific regulatory body [4], when the same is not necessarily the case for privacy requirements. The regulatory requirements can reference other pieces of regulation and evolve over time [4, 7]. For example, the GDPR entered into force in 2018 and interacts with the Privacy and Electronic Communications Directive (ePrivacy directive) or with the Digital Service Act (DSA) and Digital Markets Act (DMA), which have entered into force in the recent months. Consequently, knowledge of these policies and others is required for regulatory requirements for data protection in Europe, which is not the case for all privacy requirements.[2]

All in all, privacy requirements are not necessarily the same as regulatory requirements for data protection. The two have different origins, expectations, and specifications, among others. While stakeholders might have different conceptualizations of privacy, regulatory data protection requirements set out requirements independently of the privacy conceptualization, even if the wording allows for different interpretations.

2.2 Privacy requirements engineering

From an RE perspective, privacy is a well-established area of research [17]. Various research papers focus on privacy requirements, including legal concerns, each emphasizing

[1] "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve." [16]

[2] This also depends on the chosen ontology.

different levels or topics [18]. Several reviews—systematic or not—have been conducted on the subject.

Kalloniatis et al. [17] researched the management and elicitation of privacy requirements, taking a holistic view of privacy requirements. Their research does not follow a systematic approach but reviews well-known frameworks and approaches for privacy requirements [17]. In addition, they highlight the importance of including security and privacy requirements from the early phase of the software development lifecycle, in line with established academic work [4, 5, 17].

Morales-Trujillo et al. [19] share their results of a systematic mapping study on the privacy-by-design paradigm in software engineering. They report that there has been an increased interest in the subject in 2018, which they relate to the entry into force of the GDPR [19]. In addition, most papers propose models for the subject; however, most of the contributions are in the initial stages and need further development [19].

Netto et al. [20] carried out a systematic literature review of privacy requirements engineering, focused on the years from 2000 to 2016. In their research, most of the literature on requirements engineering would focus on the elicitation process on privacy requirements, followed by their analysis [20]. Furthermore, they highlight that language used in the legal text is very different from requirement engineering, which complicates the work between the two domains, and that there is a lack of modeling language that can bridge both said domains [20].

Recently [21] published a systematic literature review on privacy requirements and their perception across IT practitioners, understanding privacy requirements broadly. They provided a list of requirements elicitation techniques, methods, and frameworks published until 2021 [20]. They conclude that most used tools or frameworks in academia do not align with those in the private sector or practitioners [20].

All the previous works do not focus specifically on regulatory data protection requirements compliance. Some acknowledge the subject and discuss the implications of the corresponding regulation. For example, both [19, 21] point out that there seems to be a peak of published papers related to privacy requirements in 2018, which relate to the entry into force of the GDPR. However, they do not focus on the compliance of a specific regulation or the GDPR.

Several proposals are consistently mentioned and studied throughout these papers as ways to tackle privacy requirements. Some examples are:

- LINDDUN is a privacy threat modeling framework based on data flow diagrams that allow the analyst to elicit and model privacy threats from early stages SDLC [22, 23]. By including privacy concerns from the beginning of the SDLC, the idea is to help software developers build PbD software [23]. One of the latest development is LINDUUN GO, which is a lightweight and gamified approach to the framework [24].
- Privacy safeguard (PriS) is an organizational goal-oriented framework that helps analyze the business processes from a privacy perspective [18, 25, 26]. Based on the Enterprise Knowledge Development, “PriS provides a set of concepts for modeling privacy requirements in the organization domain and a systematic way-of-working for translating these requirements into system models” [25]. In fact, it identifies eight privacy goals—authentication, authorization, identification, data protection, anonymity, pseudonymity, unlinkability, and unobservability—and 7 privacy-process patterns that help to achieve the goals [25, 26]. Through a determined methodology that consists of 4 steps, PriS allows the practitioner to elicit privacy goals, analyze and understand the impact of these goals and identify which patterns and techniques may better support the achievement of the privacy goals [25, 26].
- The role-based access control (RBAC) approach is proposed by [5]. Through a goal-driven approach, their framework helps model privacy requirements from early phases in role engineering to bridge the gap between “high-level privacy requirements and low-level access control policies” [5]. Furthermore, their framework helps modeling and analyzing competing security and privacy requirements [5].
- Spiekermann and Cranor [27] suggests that privacy requirements should be tackled from an architectural (privacy-by-architecture) and policy (privacy-by-policy) point of view, taking a hybrid approach. Using the FIPPs principles and privacy reflections as a starting point, they identify that privacy can be divided into three spheres: the user, joint, and recipient spheres. “The ‘user sphere’ encompasses a user’s device [...] The ‘recipient sphere’ is a company-centric sphere of data control that involves back-end infrastructure and data sharing networks” [27] while the joint sphere denotes the services that companies provide to users [27]. Privacy requirements are essential in all three spheres and are divided into data transfer, storage, and processing [27]. Accordingly, they propose that taking a hybrid approach of privacy-by-policy—which focuses on choice and notice—and privacy-by-architecture—which focuses on data minimization, anonymization, and PETs—“satisfies business needs while minimizing privacy risk” [27].

Other methods and frameworks have also been proposed for requirements engineering on privacy.

Across all these proposals, the conceptual model of privacy is not necessarily the same. Each place emphasizes on different characteristics of privacy. Similarly to what was previously mentioned, these proposals do not focus primarily on regulatory data protection compliance or the GDPR. Indeed, some of the proposals discuss and touch on regulatory data protection, but it is not their main focus. Hence, their fit is more related to privacy requirements than to regulatory data protection requirements.

2.3 Regulatory data protection requirements engineering

Data protection and regulatory requirements have long been studied in RE [7, 28]. Multiple frameworks, tools, methodologies, and artifacts have been proposed, either for specific regulatory regimes (or applied to specific laws) or data protection regulatory requirements in a general manner.

[28] carried out a systematic literature mapping on modeling for regulatory compliance. The authors compared how the goal-based and non-goal-based approaches differ towards legal and regulatory compliance, highlighting their respective benefits and drawbacks. Their research found that compliance modeling and compliance checking were the most popular topics in modeling, followed by analysis [28]. Furthermore, healthcare was the domain that received the most attention, with the Health Insurance Portability and Accountability Act (HIPPA) the most popular legal document.

[29] identified the critical factors in implementing GDPR in general in organizations through a systematic literature review. In broad terms, they suggest that few papers discuss the GDPR [29]. They mention several benefits to implementing the GDPR in an organization, including but not limited to better data management, cost reduction, and better reputation [29]. They concluded that the main challenges are that the GDPR is a complex regulation—in line with what [6] indicates on regulatory data protection requirements engineering—and there is a lack of people with expertise on the subject [29]. In addition, finding data protections is difficult and expensive, and implementing the GDPR is time-consuming and costly in financial and human resources [29].

[30] carried out a systematic mapping study on automated GDPR compliance using natural language processing (NLP) tools in RE. In particular, they researched which "NLP approaches are useful for RE and for which RE activity?" [30]. They gathered papers up to 2021, and compliance is out of their scope [30]. They have identified that NLP for RE is an ongoing trend.

From an ontological perspective, some proposals either fully seek to tackle requirements from the GDPR or include some of it. A non-exhaustive list is the following:

- PrOnto [31] proposes an ontology for GDPR requirements based on legal reasoning. It does not focus on privacy but on legal data protection aspects to check compliance. Another stated goal of PrOnto is to help with legal reasoning and "web of data and information retrieval" [31] that can be used for legal reasoning. The methodology used to develop the ontology is "methodology for building Legal Ontology" (MeLOn), which is frequently used in the legal domain to create ontologies [31]. For example, it has a variety of classes to represent regulatory data protection requirements, such as obligation, rights, or purpose class. From this work, the authors have extended their work to propose the DAPRECO [32] knowledge base.
- CoPRI is a privacy ontology proposed by Gharib et al. [33], that includes some aspects of the GDPR, even though it is not their main purpose to be a GDPR ontology. It includes elements that go beyond the scope of the GDPR. It does not use legal reasoning for the ontology.
- Similarly, LloPY also includes legal aspects to its ontology [34], although it focuses on IoT instruments. It seeks to include specific attributes of regulatory data protection requirements, such as consent or choice, into privacy policies [34]. It does not use legal reasoning for the ontology.
- The GDPRov family comprises of the GDPRov, GDPRtEXT, and GConsent proposals, which are combined ontologies that tackle specific legal requirements of the GDPR. [35–37]. GDPRov is an OWL2 ontology that focuses on the specific elements of the GDPR, namely "acquisition, usage, storage, deletion, and sharing of consent and data lifecycles" [35]. It focuses on processes like data deletion and access, consent management, and personal data [35]. GConsent [37] is more specific, focusing solely on GDPR consent requirements. The approach of these ontologies is similar to PrOnto as the GDPR plays a fundamental role, although they do not explicitly state they use legal reasoning.

In this manner, our work differs from other works in RE, as it focuses solely on data protection requirements, specifically the GDPR. Previous work has focused either on privacy requirements—which we have already discussed how they differ from data protection—or on compliance requirements in general. In comparison, data protection is becoming more standardized: the OECD privacy principles [38] and the GDPR became *de-facto* the international standards for data

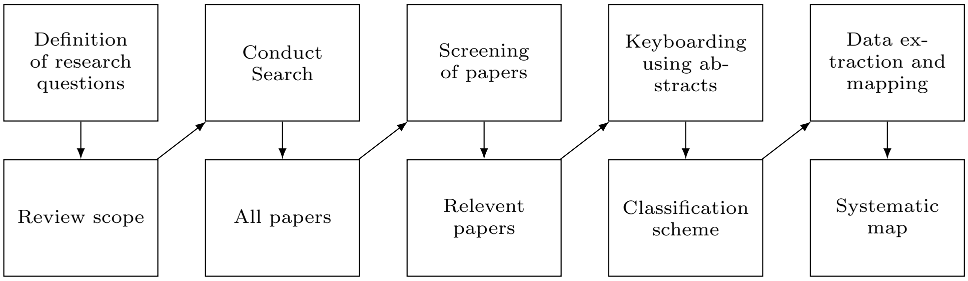

Fig. 1 Systematic mapping process by Petersen et al. [39]

protection legal instruments. Furthermore, this research aims at studying what has been done in RE to achieve or help compliance, and not GDPR requirements from a general perspective.

3 Research method

This research follows the guidelines from Petersen et al. [39–41] to gather, analyze and produce the systematic mapping study. Mapping studies' objective is to discover trends over a specific area, whereas a systematic literature review tries to answer a research question [40]. In this manner, a mapping does not necessarily need to find all the research articles that may answer a question nor have one, but instead grab a good representative sample of the area of interest [39, 40, 42]. Given this approach, mapping studies do not require a qualitative assessment [39].

Following what Petersen et al. [39] indicates, the approach of this study is a "'thematic analysis' that counts papers related to specific themes or categories". Similarly, this mapping study contains a few research questions closer to a systematic literature review than a mapping, as they cannot be answered only by reading the abstract. However, mappings and reviews can be considered a continuum, benefiting by using research strategies from one another [39]. Therefore the researcher does not necessarily have to restrict themself to read one part of the article when doing a mapping study [39].

3.1 Objective and mapping studies

This systematic mapping study was done with the guidelines from Petersen et al. [39–41] for planning the research, as seen in Fig. 1. In particular, the paper gathering sample plan is based Petersen et al. [39].

This mapping study aims to discover the trends of what initiatives have been proposed in requirement engineering to achieve GDPR compliance. Its main objective is to summarize and disseminate the current state of affairs of GDPR regulatory requirements in RE.

To discover the trends and fulfill the objective of the mapping study—as mapping studies do not necessarily answer a question [40]—the following sub-questions were chosen:

RQ1: When, where and in what type of venue has the research been published? (I.e: Type of venue)

RQ2: Are the authors of multiple disciplines?

RQ3: What type of research is it?

RQ4: On what stage of the RE process does the paper focus?

RQ5: What compliance elements of the GDPR does the research article focus on?

RQ6.1: What type of proposal is the paper?

RQ6.2: If a modeling language extension is proposed, it is an extension of which language?

This research understands initiatives in a broad manner, as artifacts or treatments proposed by Wieringa et al. [43]. Research is understood as investigations that tackles knowledge questions on the domain [43]. We are also interested in knowledge questions, as they act as guiding elements for research.

3.2 Search planning

In order to create the search string and define the exclusion and inclusion criteria, we followed the PICO (Population, Intervention, Comparison, and Outcomes) approach per Kitchenham and Charters [41]. Although the PICO approach is recommended for systematic reviews and not mappings, it does help identify keywords, as Petersen et al. [40] did on their mapping.

Population: Our population of interest is GDPR.
Intervention: "The intervention is the software methodology/tool/technology/procedure that addresses a specific

Table 1 Keywords and synonyms

Keyword	Synonyms
Compliance	Adherence, compliant
GDPR	Data protection regulation, General Data Protection Regulation
Requirements engineering	Requirement*, RE
Legal	Law, regulation, regulatory, law

issue" [41], which in our case is requirements engineering, more precisely compliance.

Comparison: We compare what has been proposed in RE, understanding proposals flexibly (so knowledge questions can be included). Following a similar strategy to Petersen et al. [40], we do not empirically compare the proposal, as this study aims to discover trends, not to do a systematic literature review.

Outcomes: As this research is a mapping study, as indicated by [40] this item does not necessarily apply to our research. However, the outcome is to have a systematic list of proposal from RE for GDPR compliance.

As a result, with PICO we have identified keywords. Overall, and taking a similar approach as Petersen et al. [40], there are four groups of words to be searched:

Set 1: Searching elements related to the GDPR, such as data protection regulation.

Set 2: The scope is within requirements engineering.

Set 3: The requirements need to be linked with compliance or adherence.

Set 4: The requirements must come from a legal or regulatory document.

Hence, a list of synonyms is identified and provided in Table 1. We performed the search string based on this identified synonyms.

3.3 Exclusion and inclusion criteria

For the exclusion of research articles, the following criteria was applied (Table 2).

These criteria have been chosen so that the selected articles align with the study's objective and PICO. Our interest in excluding research published in unranked venues is to perform a quality check, although this is not necessary for mapping studies [40]. Table 2 summarizes the exclusion/inclusion criteria.

Our primary concern is requirements engineering, and our exclusion criteria are all papers whose main focus is not requirements engineering. Although many research papers talk about requirements, they are be excluded if they are not specifically talking about achieving compliance with GDPR requirements. Similarly, if a specific framework was applied and tangentially showed compliance with the GDPR, it would also be excluded, as its primary concern was not achieving compliance with the GDPR. The reason behind this decision is because although these types of papers may be helpful for several reasons, requirements engineering and compliance with the GDPR are not their main focus. All technology that falls in scope with the GDPR shall comply with the GDPR. Hence briefly claiming compliance and/or discussing the GDPR regulatory requirement does not make the research article necessarily interesting for our research objective.

Other exclusion criteria are articles that are not primary studies, have not been peer-reviewed, or are grey literature. The focus of this study, as the research question shows, is what initiatives have been proposed for improved compliance in the GPDR. Hence, although some opinion articles may be interesting, they do not fall within the scope of our research question.

Table 2 Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Studies that are about requirements engineering	Study not peer-reviewed
Studies that have been published between January 2016 and December 2022	Books and book chapters
Studies that explicitly address GDPR and compliance	Study not available online
Papers written in English	Secondary research (SLR, summaries, guidelines/templates)
	Not about requirements engineering
	Unranked venues
	Grey literature
	Does not talk about GDPR (ex: talks about privacy, but from a cryptographic perspective; or other regulations)

Table 3 Search string per database

Database	Search string
IEEE	`(“All Metadata”:compliance OR “All Metadata”:compliant OR “All Metadata”:adherence) AND (“All Metadata”:GDPR OR “All Metadata”:general data protection regulation OR “All Metadata”:data protection regulation) AND (“All Metadata”:requirements OR “All Metadata”:RE OR “All Metadata”:requirements engineering) AND (“All Metadata”:legal OR “All Metadata”:regulatory OR “All Metadata”:regulation OR “All Metadata”:law) from 2016`
ACM	`((Abstract: “compliance”) OR (Abstract: “adherence”)) AND ((Abstract: “gdpr”) OR (Abstract: “general data protection regulation”) OR (Abstract: “data protection”)) AND ((Abstract: requirement*) OR (Abstract: “requirements engineering”) OR (Abstract: or “re”)) AND (E-Publication Date: (01/01/2016 TO 12/31/2022))`
SCOPUS	`TITLE-ABS-KEY(“compliance” OR “adherence”) AND TITLE-ABS-KEY(“GDPR” OR “general data protection regulation” OR “data protection regulation”) AND TITLE-ABS-KEY(“requirements” OR “RE” OR “requirements engineering”) AND TITLE-ABS-KEY(“law” OR “legal” OR “regulation” OR “regulatory”)`

3.4 Search string

The search string was carefully thought out to include synonyms of the identified keywords, allowing us to answer all the questions. Complementary to the PICO approach, we tested iteratively different strings to find the optimal solution (trying to find a trade-off between a sample too big too analyze of thousands of papers, to a extremely limited sample of a dozen). Furthermore, we would verify if the most important papers were still present in the new strings, following a similar approach as Kitchenham [44] of test-retest.

We decided not to include “privacy” in the search string, as the focus of this study is protecting personal data under the GDPR framework, not “privacy” in broad terms. This decision is: (1) based on the definition of privacy; and (2) due to the test-retest approach.

Firstly, defining privacy is challenging, as there is no clear-cut definition, and it encompasses a wide range of issues [15, 45]. This discussion is shared in Sect. 2. Our second reason for not using “privacy” in the search string is due to the test-retest approach. When the term privacy was used, the search results in the database increased enormously and included articles that were not within the scope of this research. Some of those articles, for instance, were about cryptography, the cloud, legal texts, philosophical texts, and formal code verification, among others. As a result, it was defined that the word “privacy" would not be used because the articles that appeared were not of interest. By excluding this synonym, we still found the research articles of interest and those identified as necessary from the domain.

Databases used to obtain the articles for this research were the following: IEEE, SCOPUS (which includes ScienceDirect and Springer), and ACM. These databases were chosen because of their notoriety and importance within the field of computer science.

Databases of law research were not selected, as they were preliminarly tested with our inclusion/exclusion criteria, and no papers with RE focused were found, and hence, were out of scope. At this phase, we queried the HeinOnline and JSTOR databases to identify papers of interest. We experimented with string with and without the keyword for requirements engineering. When querying with the keyword “requirements engineering” in JSTOR—for example—we got only 2 papers. Both of these papers were outside the scope of this research, as they did not discuss requirements engineering. Therefore, we decided not to query law databases, which we further discuss at Sect. 6 on the possible impacts.

We designed a specific search string for each database (see Table 3), following the flexibilities or restrictions of each platform. The queries (and subsequent data extraction) were carried in January 2023.

3.5 Data extraction

Once publications were selected/excluded regarding the previously mentioned restrictions, the remaining final publications were analyzed with the data extraction form, shown in Table 4. We conducted the data extraction and reviewed each other's work. Reviewing each other's work increases the study's validity and provides more robustness.

For tackling RQ3, we take the taxonomy proposed by [46] and [43]. Wieringa [46] has proposed that the engineering cycle can be divided into two main areas of research: knowledge questions and design research. Knowledge questions motivate research that seek to solve a question about the world [46]. The design research proposes an artifact to contributing, solving, improving, or making an environmental effect for a specific problem [47].

Similarly, Wieringa et al. [43] proposed a study classification taxonomy for papers, that we followed in this research. The proposed types of research defined by this taxonomy are:

Validation research: "This paper investigates the properties of a solution proposal that has not yet been implemented in the RE practice. [...] The investigation uses a thorough, methodologically sound research set up" [43].
Evaluation research: "Techniques are implemented in practice, and the technique is evaluated. That means, it is shown how the technique is implemented in practice..." [39].
Solution proposal: this type of article presents a solution to a defined problem [43]. "The solution can be novel or a significant extension of an existing technique" [39].
Conceptual proposal:"These papers sketch a new way of looking at things, a new conceptual framework" [43]. Following [42] we prefer to name this type of research as conceptual proposals, rather than philosophical papers [43], as it is more leading towards the objective of the mapping study.
*Experience papers:*the authors share their experience over a subject, where the focus is on the *how* rather than the *what* [39, 43].
Opinion papers: the authors present their opinion on some subject, without methodology [43].

We left out opinion papers, as they are not proposing or carrying out primary research.

Alongside these lines, we also classified the type of research method followed in papers categorized as validation or evaluation [46]. Although there are several types of research methods available, and labeling each precisely would be inconvenient, we followed the proposal made by Petersen et al. [40], which is based in Wieringa et al. [43], as shared in Table 5. In this manner, it is possible to see which research methods seem predominant in the field and identify trends.

For defining which process of the RE cycle the paper was focusing, we used the taxonomy provided by Pohl and Rupp [8] and add an extra element presented by Sommerville [48]. In particular, we divided the RE cycle as the following five categories:

Elicitation: Refers to the activity that seeks to inquire from different stakeholders that may be affected by the IS [8]. This can range from expectations and goals from users, to requirements set by legal documents. For this mapping study, the analysis process was also included in the elicitation phase [48].
Specification: "... is the process of writing down the user and system requirements in a requirements document. Ideally, the user and system requirements should be clear, unambiguous, easy to understand, complete, and consistent" [48].
Verification and validation: Requirements need to be validated (as for example, do they meet the objectives of the stakeholders?) and verified (are all the elements included?) [8]. In the GDPR context, certain articles specify what IS should and should not include. For example, privacy policies must fulfill a list of requirements to be considered valid.
Management: Requirements might evolve through time and change or have different prioritization, management is linked to all the other RE activities [8].
Documentation: Requirements need to be traced and their specification should be written in a document to keep track of them [8, 48].

Regarding the classification of GDPR topics, to the best of our efforts, we could not find a taxonomy or classification scheme for papers that would encompass the whole regulation. Given that the GDPR is a regulation with 99 articles and 173 recitals, classifying the research papers per article would not have been practical nor useful. Hence, in order to classify papers by the area of GDPR they discuss, the authors of this article came up with a classification scheme of topics they have experienced to be commonly discussed, grouped by sets. This situation, cataloged as "emerging classification" by Petersen et al. [40], is common between mapping studies. According to Petersen et al. [40], 40 of 55 studies reviewed in their mapping used an emerging classification.

The classification we created for this research is as follow:

GDPR principles: Are the guiding principles of the regulation. They are: (1) lawfulness, fairness, and transparency, (2) purpose limitation, (3) data minimization, (4) accuracy, (5) storage limitation, (6) integrity and confidentiality (security), and (7) accountability [1].
Legal basis for processing (except consent): This is the lawful basis for which a controller can process the data. The GDPR defines them in Art.6 [1].
Consent: Consent is a legal basis for data processing, part of the previous set. It is mentioned through the GDPR, which stands out as a legal basis with precise requirements, thus being classified in its own set. It is defined in Art.4(11), Art.6 sets it as a lawful basis, Art.7 defines its conditions, Art.8 sets the rules of consent for children, Art.9 defines how consent is to be gathered with special categories of data, among other articles and recitals [1, 49, 50]. Consent has a particular type of governance [49] that has sparked an area of research.
Data transfers to 3rd countries or international organizations: Is usually abbreviated as data transfer to 3rd countries. Chapter V (Art.44–50) of the [1] sets the requirements of data transfers to 3rd countries and international

organizations. Different mechanisms for doing so must fulfill a set of requirements, such as security, agreements, contracts, among others [1, 49].

Identification of actors: Organizations must identify the actors involved in an information system to define its duties and requirements. Accordingly, it must identify the data protection officer (DPO; Art.37), who is the processor and controller (Art.26-29, for example), if the processor or controller is not in the European Union (Art.27), and who is the data subject, among others.

Duties of actors: The obligations of processors and controllers are stipulated in chapter IV of the [1].

*Data subject rights:*These are data subjects' rights over their personal data, as stated in Chapter III of the [1]. Among these rights are the rights: (1) to be informed, (2) to access, (3) to rectification, (4) to erasure, (5) to restrict processing, (6) to data portability, (7) to object, and (8) concerning automated decision making and profiling. These different rights impose several requirements on the information system.

Privacy policies: Privacy policies are related to the requirement of transparency by the [1]. It is expressed explicitly under Chapter III, as part of the data subjects' rights, in Art.12–14 of [1], and also relates to the right to be informed. The objective of a privacy policy is to inform the data subject about the data governance model.

Privacy-by-Design-and-Default (PbD &D): Relates mainly to the Art.25 of the [1]. The idea of PbD &D is that privacy elements and requirements should be from a design point of view in IS [51]. In other words, privacy requirements are dealt with from the early stages of the SDLC, they should not conflict with other requirements of the IS, and they should be the default setting IS and be user-centric [51].

Security requirements: Refers mainly to the requirement set in Art.32 of the [1] among others (such as recital 83 or 49). The idea is that technical and organizational measures (TOMs) should be in place to secure the data processing, particularly based on the risk of such processing [1, 49, 50, 52].

Other: category created to keep track of other elements outside this list. This category would keep a record of the different elements.

Specific articles: A classification created if a paper would discuss a specific article outside the scope of the proposed classification

This classification was created for articles that would either:

General:

(a) Discuss GDPR compliance on general terms, without referencing articles, reflecting about compliance at high level

(b) Focus on GDPR compliance as a whole while also addressing some specific articles and issues whose main purpose was GDPR compliance.

In this classification, we created "Other" and "Specific Articles" categories to avoid missing topics that could be labeled but did not fall into any of the proposed sets. "Specific Articles" would record if a research article only focuses on a specific article not part of the GDPR principles (legal basis, consent, data transfer, identification of actors, duties of actors, data subjects rights, privacy policies, PbD &D, or security). Therefore, we can track which specific article the paper would focus. At the same time, "Other" could be another area of interest without touching a specific article of the GDPR (such as a record of processing activities in a generic manner). We do not claim that this classification scheme is final or robust, but it was the method we chose to fulfill this study's objective [40]. To the best of our knowledge, there is no widely accepted taxonomy or classification of interest areas for the GDPR.

In order to give more robustness to this classification, we decided to record all GDPR articles mentioned in the sampled papers, regardless of whether the paper focused on that GDPR article or not. In this way, several GDPR articles could be mentioned throughout the paper but are not necessarily the main interest of the research article. To illustrate, a paper could focus on consent but mention articles: 4–8, 25 and 44; even when not all these articles are directly linked to consent.

4 Results from the mapping

The total number of studies per database is presented in Table 6. For the sample selection, we found a total of 402 papers. The final sample is of 90 papers. The selection process is described in Fig. 2 and the list of the papers is provided in "Appendix 1".

4.1 RQ1: When, where and in what type of venue has the paper been published?

4.1.1 When: year of publication

Looking at the numbers of publications by year as seen in Fig. 3, it can be seen that most of the publications happened after 2018, the year the GDPR came into force. Although there are publications since the year of the signing of the GDPR (2016), the highest number of publications is in the year 2019 (25 publications, 27,8%), followed by 2020 (20 publications, 22,2%) and 2022 (20 publications, 22,2%).

4.1.2 Where: venue published

We see no clear trend concerning where the sample papers are published. No specific venue has more than five publications (shown at Table 17 in "Appendix 2"). Table 7 shows the frequency of the venues that have published more than one paper. As it can be seen, only seven venues have published more than three, and more precisely, only three venues have published more than four papers on the subject. The central theme of the first two venues are privacy and security (Information and Computer Security and ESORICs workshops), while the third venue's main topic is requirements engineering (RE).

4.1.3 In what: type of venue

If we divide by type of venue where the research has been published, we obtain the following data: 44 articles (48.9%) have been published in conferences, 33 (36.7%) in journals, and finally, 13 (14.4%) in workshops; as shared in Fig. 4.

4.2 RQ2: Are the authors from multiple disciplines?

As mentioned above, each paper author was reviewed to check their affiliations. If the affiliation was not in the paper, it was searched through a search engine. After this research, we found that there were 20 articles,representing 22% of the paper sample (as shown in Table 8), in which at least one of the authors is not affiliated with a department of computer science or business informatics.

Besides computer science and business informatics, authors came from the following areas: Humanities and arts, Business Administration and Management, Law, Archival and Library and Information Science, Medicine, Philosophy, Health science, and Economics.[3]

4.3 RQ3: What type of research is it?

Using the taxonomy presented in Sect. 3 and Table 9 it can be seen that 11 papers (12%) were classified as only knowledge questions—i.e., not related to the design science process. When focusing on the design science research category done, a significant percentage of the papers have some validation or evaluation (44 articles, corresponding to 48%).

At the same time, there is a high number of papers that could not be defined under a single category. 40 papers (44%) correspond to only one category. The most frequent single categorization is "knowledge question", followed by solution proposal. In comparison, 39 (43%) papers were categorized under two categories, with "solution proposal" and "proposal validation", and "solution proposal" and "proposal evaluation" being the two most popular combination of research type. Finally, 11 (12%) of the remaining papers were classified under three categories (such as "knowledge question" and "solution proposal" and "validation proposal").

When we revise what research methods have been applied for validation or evaluation, case studies, industrial case studies, prototypes, and controlled experiments with practitioners are the most popular (Table 10).

4.4 RQ4: On what stage of the RE process does the paper focus?

As this is a mapping study, we followed a high-level classification of the RE process. It was difficult to classify the majority papers into a single category within the RE cycle, as most times they would fall under the scope of 2 or more. Therefore, 44 (48.9%) items were classified under a single category, 45 (50%) have two or more categories, and 1 (1.1%) of them could not be classified under any part of the requirements lifecycle.[4] The largest number of articles is found under the elicitation category, followed by verification and validation. The classification is presented in Table 11.

In order to analyze what areas of interest exist in the RE process, we grouped the data based on whether the papers touched or discussed that area. In this way, the total number of individual occurrences is 154 since—as previously mentioned—a paper can have more than one area of interest in the RE process.

47 papers address the requirements elicitation stage. This is followed by specification with 35 papers, and verification and validation with 33 papers. As presented in Sects. 1 and 2, the focus on elicitation may be related to the fact that the GDPR requirements must be interpreted, as they are emanating from legal prose. This task of interpreting regulation into software requirements calls for a particular set of skills. A more detailed reflection is presented in Sect. 5.

4.5 RQ5: What compliance elements of the GDPR does the research article focus on?

Quite a few articles touch on only one aspect of the GDPR and seek to contribute only to it. Table 12 shows the areas

[3] For a detailed categorization of the sampled papers, please refer to https://zenodo.org/records/10040309.

[4] Kuehnel and Zasada [53] propose a framework for analyzing the monetary cost of not meeting the requirements and it could not be identified to which part of the RE process it relates to.

Fig. 2 Selection of sample papers for the mapping study

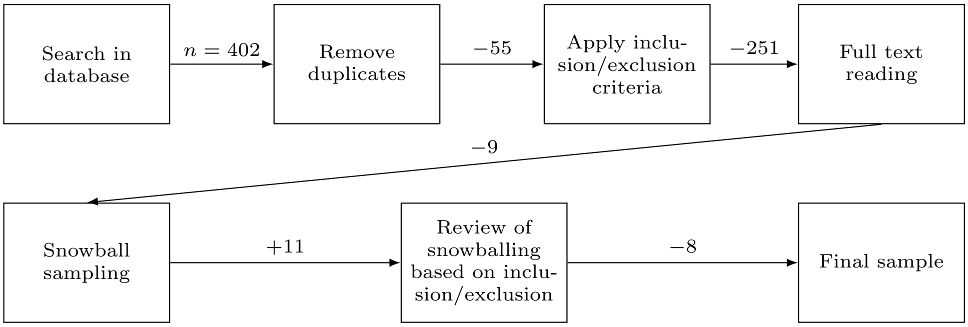

Table 4 Extraction form

Data item	Value	RQ
Article name	Name of the article	
Author names	Name of the authors	RQ2
Year of publication	Civil year calendar	RQ1
Type of publication	Journal, conference, workshop	RQ1
Venue name	Name of the venue where the article was published	RQ1
Interdisciplinarity	Are all the authors from computer science? If false, identify the areas	RQ2
	Identification of other areas	
Classification	What type of research is it?	RQ3
Evaluation and validation methods	What type of validation and evaluation research method uses?	RQ3
GDPR compliance	In what GDPR elements does the research focus?	RQ5
	List out all the GDPR articles that are mentioned—not necessarily discussed in depth	
	Comments or details on the GDPR focus of the article	
RE process	At what level of the RE process does it focus	RQ4
Proposal	What type of proposal? [If any]	RQ6
	If a modeling language or an extension of a modeling language is proposed, which is the base language?	RQ6.1

Table 5 Evaluation and validation research category, proposed by Petersen et al. [40], based on [43]

Evaluation research
Industrial case study
Controlled experiment with practitioners
Practitioner targeted survey
Action survey
Ethnography
Validation research
Simulation as an empirical method
Laboratory experiments (machine or human)
Prototyping
Mathematical analysis and proof of properties
Academic case study (e.g. with students)

of interest in the GDPR per year and the total of research articles that discussed the topic. In order to gather more insight to answer this research question, we kept track of which articles were mentioned in the papers, as previously stated. Consequently, for example, if a research article mentioned Art.4, this would be recorded as a mention.

57 papers also refer to the GDPR in a general manner, either mentioning some articles for exemplification purposes but not focusing on these; or just discussing the GDPR without mentioning or making references to specific articles. Hence, the category "General GDPR" is the most popular topic. In second place, there is consent, with 27 papers discussing the subjects. Following are privacy policies and, afterward, security elements.

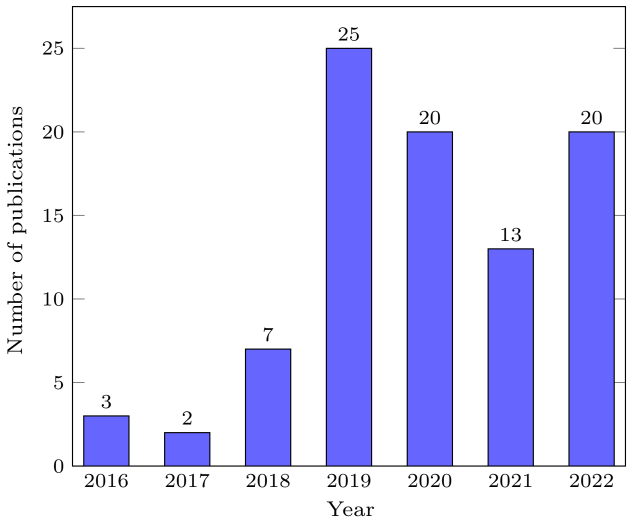

Fig. 3 Number of publications per year

Table 6 Search results per database

Database	Search results
IEEE	73
ACM	22
SCOPUS	307

Consent is a popular topic in the paper sample. A significant percentage of the sample acknowledges it as a topic directly in scope of their paper (27 papers, see Table 14). 31 papers also mention consent somewhere (measured per references to Art.7). Similarly, Art.6 which deals with the legal basis for processing—including consent—is mentioned 37 times. Many of the proposals relate specifically to consent management. Compared to the other legal basis, only 12 papers focus on the other legals basis aside from consent, yet Art.6 is mentioned more frequently, as shown in Table 13.

The third most popular topic is privacy policies. This topic is the main focus in 21 papers of the sample. Privacy policies requirements are specified mainly—but not solely—from Art.12–14 of [1]. Art.12 is mentioned 19 times, Art.13 29 times and Art.14 30 times.

In order to identify which other elements may have been of interest, these were coded as “Other” and specified which element they focused on, as seen in Table 14. In this category, record of processing activities was the focus of four papers.

4.6 RQ6.1: What type of proposal is the paper?

Frameworks and conceptual frameworks are the two most common proposal types, with 22 and 18 papers classified as such accordingly, as shown in Table 15. Due to the extension and scope of the GDPR, a framework seems to be a logical proposal. Tools are the third most common type of proposal. Table 15 shows the frequency of other types of proposals, with no clear tendency from the fourth position onwards.

As specified in Sect. 3, “Knowledge questions” articles and some “Experience papers” do not provide a type of proposal. Hence, they were not categorized for this question.

4.7 RQ6.2: If a modeling language extension is proposed, it is an extension of which language?

When reviewing the proposed modeling languages or proposition of extension of existing modeling language, we see

Table 7 Venues that have published more than one article on the topic

Venue name	Number of articles
Information and Computer Security	5
European Symposium on Research in Computer Security International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT (ESORICS workshops)	4
International Requirements Engineering Conference Workshops (REW)	4
Annual International Conference on Privacy, Security and Trust (PST)	3
IEEE Access	3
Information (Switzerland)	3
Annual ACM Symposium on Applied Computing (SAC)	2
IEEE European Symposium on Security and Privacy Workshops (EuroS &PW)	2
International Conference on Trust, Privacy and Security in Digital Business (TrustBus)	2
International Requirements Engineering Conference (RE)	3
Journal of Logical and Algebraic Methods in Programming	2
The IFIP WG8.1 Working Conference on the Practice of Enterprise Modelling (PoEM)	2
VLDB Endowment Proceedings (VLDB)	2

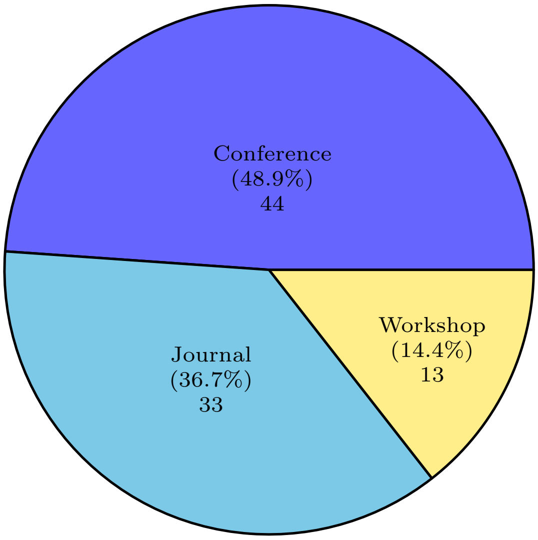

Fig. 4 Number of publications per venue

Table 8 Research articles that have at least one author not affiliated to computer science or informatics

Interdisciplinary authors	Frequency
No	70
Yes	20

that STS-ml [54] has been the basis for three investigations. The rest of the languages are: Secure Tropos [55], Goal-oriented language [56], Unified Modeling Language [57], and Process Reference Model, as shown in Table 16.

Table 9 Type of research, based on [43]

Type of research	Frequency
Solution proposal, Validation proposal	13
Evaluation proposal, Solution proposal	13
Knowledge question	11
Solution proposal	10
Conceptual proposal	9
Evaluation proposal, Knowledge question, Solution proposal	7
Conceptual proposal, Validation proposal	6
Knowledge question, Solution proposal	5
Knowledge question, Solution proposal, Validation proposal	4
Experience paper	4
Validation proposal	4
Conceptual proposal, Evaluation proposal	2
Evaluation proposal	2

Table 10 Validation and evaluation research research method

Research method	Frequency
Evaluation—Industrial case study	9
Validation—Academic case study (e.g. with students)	9
Validation—Prototyping	8
Evaluation—Controlled experiment with practitioner	8
Validation—Laboratory experiment (machine or human)	5
Evaluation—Action research	4
Evaluation—Practitioner targeted survey	4
Validation—Mathematical analysis and proof of properties	4

5 Discussion

Some trends and research gaps have been identified and analyzed using the mapping study's information.

5.1 RQ1: When, where and in what type of venue has the paper been published?

The number of publications per year shows that the topic of requirements compliance for the GDPR seems still attractive. Most papers were published in 2019, 1 year after the entry into force of the regulation, and there is a drop in 2021, which the COVID-19 pandemic could potentially explain. It would be interesting to check if the publication in other areas dropped in the same manner.

On the other hand, it is interesting to note that prior to 2018 (the year GDPR came into force), up to five papers were published in the sample. This means that organizations had limited tools, artifacts, methodologies, or approaches to handle the regulatory requirements of the GDPR. Even in 2018, only seven articles were published. Consequently, organizations did not have much work available from an RE perspective.

Regarding the venues where research was published, there is no trend of preference. Indeed, although there are 3 top venues, none have published more than five articles. A possible explanation might be that, given the importance of the GDPR for organizations, the regulation applies to a wide range of areas.

Similarly, there does not seem to be a significant difference between conferences and journals. However, there are considerably fewer publications in workshops.

5.2 RQ2: Are the authors from multiple disciplines?

Around 22% of the articles selected in the mapping study are written by multidisciplinary teams with at least one author not related to computer science. This is a significant portion

Table 11 RE process frequency in papers

RE process	Frequency
Elicitation	47
Specification	36
Verification and validation	33
Documentation	23
Management	16
Total	154

of the articles. Given that the GDPR is a legal text related to ethical matters, this is not surprising.

However, it would be interesting to compare the approaches and interpretation of GDPR articles between research conducted by interdisciplinary and monodisciplinary. The interpretation of legal texts and their translation into requirements is a challenging task, which is usually difficult for software engineers to carry out [5, 10]. For example, does research conducted by teams that includes lawyers consider consent or PbD &D in a different way? What are the approaches to specific technologies (such as blockchain, for example) and their compliance? These questions could be addressed in future research.

5.3 RQ3: What type of research is it?

The papers sampled used a wide variety of research methods, with proposals focusing on presenting some type of validation or evaluation to their proposals. 26 solution proposals are simultaneously either an evaluation or a validation. 7 solution proposals also address a knowledge question and include an evaluation. At the same time, 4 solution proposals address a knowledge question and include a validation. Similarly, 11 papers present knowledge questions alone, and 10 are just proposed solutions. These metrics show that the community is interested in grounding its work in real life and provide evidence of how it interacts with stakeholders or the context. In other words, the community seeks for application of the proposal, avoiding leaving it as just a theoretical proposal and sharing its validation and evaluation accordingly.

5.4 RQ4: On what stage of the RE process does the paper focus?

Overall, there is interest in the requirements elicitation stage. As the GDPR is a new regulation, understanding, interpreting, and extracting the requirements from this law can be regarded as a new activity. Moreover, since the GDPR is not straightforward in what it expects, interpretations on how to comply will be context-dependent.

The specification stage was the second process which attracted the most interest, and verification and validation was a close third. GDPR requirements are context-dependent, for instance, it is not the same to gather consent for a smartphone game for children than for a website. As a consequence, specifications may vary significantly and affect the design of the IS. On the other side, the verification and validation stage are addressed through the problem of compliance verification. More specifically, there is an interest in validating requirements, such as privacy policies, by addressing questions such as: is the privacy policy meeting all the GDPR requirements? Tools for verifying and validating GDPR requirements would be useful for organizations and regulators. Organizations could use them to check their requirements, while regulators would be able to audit organizations faster.

Table 12 GDPR subjects of interest per year

	2016	2017	2018	2019	2020	2021	2022	**Total**
General GDPR (doesn’t specify; or it is for all GDPR)	1	0	4	18	16	8	10	**57**
Consent	1	1	2	6	7	3	7	**27**
Privacy policies	0	0	1	8	3	2	7	**21**
Security elements	1	2	2	6	4	1	2	**18**
Principles	0	0	1	5	1	1	4	**12**
Privacy-by-Design-and-Default	0	0	1	5	0	0	6	**12**
Data transfer (3rd parties)	2	1	1	3	1	1	2	**11**
Roles and duties	0	1	1	3	4	1	1	**11**
Subjects rights	1	0	0	5	1	0	4	**11**
Identification of actors	0	1	1	2	3	0	1	**8**
Legal basis (except consent)	0	1	0	1	2	1	3	**8**
Specific articles	1	0	1	1	2	1	1	**7**
Other	1	1	1	5	2	4	2	**16**

Table 13 Number of papers mentionning each GDPR article

1	1	**11**	5	**21**	21	**31**	4	**41**	1	**51**	4	**61**	0	**71**	0	**81**	0	**91**	1
2	2	**12**	19	**22**	16	**32**	25	**42**	4	**52**	1	**62**	0	**72**	0	**82**	3	**92**	1
3	8	**13**	29	**23**	5	**33**	14	**43**	2	**53**	2	**63**	1	**73**	0	**83**	6	**93**	2
4	30	**14**	30	**24**	19	**34**	14	**44**	10	**54**	1	**64**	0	**74**	0	**84**	1	**94**	1
5	44	**15**	30	**25**	29	**35**	15	**45**	11	**55**	4	**65**	0	**75**	0	**85**	1	**95**	1
6	37	**16**	22	**26**	9	**36**	6	**46**	13	**56**	4	**66**	0	**76**	0	**86**	0	**96**	0
7	31	**17**	29	**27**	6	**37**	13	**47**	9	**57**	1	**67**	0	**77**	0	**87**	2	**97**	1
8	14	**18**	18	**28**	15	**38**	3	**48**	6	**58**	2	**68**	0	**78**	0	**88**	1	**98**	0
9	24	**19**	14	**29**	6	**39**	7	**49**	12	**59**	1	**69**	0	**79**	0	**89**	4	**99**	1
10	6	**20**	22	**30**	24	**40**	3	**50**	2	**60**	0	**70**	0	**80**	1	**90**	1		

The GDPR article is in bold and the number to its right is the number of papers explicitly referencing that article

Because it was almost impossible to frame research papers into just one part of the RE cycle, as some papers did not specify in which area they were interested, some papers may address two or more RE process.

Future research could focus on benchmarking and comparing the different proposals, which we do not address in this research, as it is outside of scope. However, it would be an interesting future work. For example, for the verification and validation tool, which areas of the GDPR do they focus on? If they focus on privacy policies, what do they verify and validate? Do they use AI? What tools are there proposed for requirements management? Are the proposed specifications GDPR compliant from legal reasoning?

Table 14 Other GDPR topics of interest, with their references

Others	Reference ID based on Appendix 1
Age verification	[ID1]
Record of processing activities	[ID2–ID5]
Data subject privacy preferences	[ID6]
Cookies and tracking	[ID1]
Data retention time	[ID3]
Intervenability	[ID7]
Data breaches	[ID3]
Data collection scheme	[ID8]
DPIA	[ID9, ID10]
Data protection agreements	[ID5]
Privacy shield	[ID11]
Children's rights	[ID12]

Table 15 Frequency and percentage of type of proposal

Type of proposal	Frequency	Percentage (%)
Framework	22	24.44
Conceptual framework	18	20.00
Tool	15	16.67
Extension of framework	7	7.78
Artifact	7	7.78
Extension of a modeling language	5	5.56
Modeling language	2	2.22

Knowledge questions are not included

5.5 RQ5: What compliance elements of the GDPR does the research article focus on?

The most significant area of interest for the GDPR was compliance with the regulation at a general level. Although some of these research papers would discuss specific regulation elements, others would barely discuss them. As this is a mapping study, we did not check for paper's quality. However, discussing or reference to specific elements of data protection regulation should be considered in quality check in future systematic literature reviews. Given the complexity and extensiveness of the regulation, in future research, claims of compliance with the GDPR should be verified against law and other regulatory texts.

Consent was the second topic of interest of the selected papers. One possible explanation is the requirements for valid consent (Art.7 [1]). The fact that consent must be free, specific, informed, and unambiguous puts stringent requirements on organizations. How can "specific" be translated into a specification? How can it be proved that it was informed? Would just ticking a box make consent informed?

These requirements have less to do with the business model and more with requirements on how consent is gathered. In other words, it can relate to human-computer interaction, requirements traceability, documentation, and others. Another aspect of consent that differs from other legal basis in the GDPR, is that the user has complete control over the legal basis, and may withdraw it when they wish. This legal basis being in the user's control, a process

Table 16 Which modelling language is a proposal based on

Base modelling language	Reference
Socio-technical System ml (STS-ml)	3
Process reference model (PRM)	1
Goal-oriented language (GRL)	1
Secure Tropos (SecTro)	1
UML	1

for withdrawing consent must be implemented, as well as keeping a record of it and other requirements [1]. This could explain why consent has attracted so much interest compared to other legal basis, such as legitimate interest, contract fulfillment, a public interest, among others. Specific topics that papers discuss for consent management include user interfaces, privacy policies, semantic web, and consent "receipts", among others.

Interesting future research could analyze users' acceptability of the proposal that deals with them directly. Furthermore, comparisons and benchmarking of the different proposals would also be interesting. Given the amount of research related to consent, the different proposals should be analyzed to identify under which context they can be implemented.

On the other hand, other areas have attracted considerably less interest. For example, GDPR articles about data transfer to third parties impose strict requirements—from security elements to contractual agreements—that do not seem as popular in the RE literature as consent or privacy policies. For example, given the usage of cloud services, controllers must verify that the cloud service is compliant with the GDPR if they use it to process data in any way. Similarly, the GDPR principles have not received much attention in the RE literature, even though they are the guiding ideas of the regulation.

5.6 RQ6.1: What type of proposal is the paper?

The literature provides a number of conceptual frameworks on regulatory requirements for the GDPR. Given the novelty of the GDPR, the number of conceptual frameworks that aim to provide a high view of the world [43] is not surprising. Probably the new elements of the GDPR sparked a strong interest in proposing a new conceptual framework, as new ontologies or taxonomies are necessary. Similarly, different frameworks have been proposed for achieving compliance with the GDPR. Each framework focuses on a different aspect of the regulation.

GDPR compliance tools have been proposed too. It would be interesting to research which technologies and frameworks these tools work with. For example, do they use artificial intelligence (AI)? If they do, how were the models trained? Did a lawyer provide advice or not? If a conceptual model was used in a specific part of the creation of the tool, did this conceptual model include legal reasoning? What is the degree of reliability of these tools?

5.7 RQ6.2: If a modeling language extension is proposed, it is an extension of which language?

The modeling languages (or extensions of these) used in the selected papers are predominantly goal-oriented (such as GRL, SecTro, and STS-ml). For instance, both SecTro and the STS-ml use primitives from the i* framework [54]. Both modeling languages have a strong emphasis on security requirements. In future research, the use of these modeling languages in industrial environments should be empirically studied and receive feedback from practitioners.

6 Threat to validity

As with most systematic mapping studies, there are reliability and validity concerns over the results obtained. As reflected by [42], secondary research can have significant problems with reliability. Even if the same classification for papers is used in two different secondary research, the same research article may be classified differently [42]. This situation can have multiple causes such as the authors' expertise and background, the need for a more concrete classification or even unclear writing by the research article author's being judged [42]. We cannot rule out that this bias can be present in this mapping. However, we did the best of our efforts to use clear and defined classification schemes with known research methodologies and the two first authors constantly comparing their results. By having two researchers reviewing each other's work, we aimed to improve reliability in the classification of papers and results of this mapping. Furthermore, we have tried to provide as much detail as possible on our process to help the reliability of the study.

The application inclusion/exclusion criteria and the data extraction were conducted using the same pairing strategy. The papers were divided in two, so each researcher could apply the inclusion/exclusion criteria and extract information. Once the tasks were achieved, the researchers would review each other work. If disagreements arose, a meeting would be held to discuss each other points and come to a conclusion. This approach is based on Petersen et al. [39] and Wohlin et al. [42] recommendations for reliability issues.

The study uses well-known and accepted classification schemes and methodologies to gather results. By using well-known accepted guidelines and methodologies, we aim at reducing bias [39].

One of the biggest threats of this research is the classification scheme used for classifying the area of interest for the GDPR. In our preliminary research, we could not find a classification scheme for the different GDPR or data protection requirements that would fulfill the objective of this research. In this phase, with unsuccessful results, we queried different legal databases, such as HeinOnline, in the search for GDPR or regulatory data protection requirements schemes. From a computer science perspective, GDPR ontologies exist, such as [31], but they were unsuitable for our research objective. Furthermore, we could have used the different chapters of the GDPR to classify the requirements. If we had taken this approach, we would have lost valuable information we were interested in. In addition, elements—such as consent—may appear in several articles and chapters of the GDPR.

In order to face this challenge, we decided to create a classification scheme based on different GDPR guidelines [49, 50, 52, 58], ontologies and vocabularies [31, 59], and the GDPR itself [1]. We proceeded with this approach as previous literature had reported it in other systematic studies, making it a valid option[40]. Indeed, [40] found that 40 out of 55 papers in their sample used this approach, denominating it as an "emerging classification". Our classification scheme used in this article has not been proposed or validated elsewhere; thus, it may faces low reliability and validity. To re-emphasize, the sole purpose of it is to help us analyze and gather data for this mapping study.

The content validity of our classification scheme may be low, as we are unsure that the classification captures the whole nature of the GDPR—or at least, of areas of interest in the GDPR for software engineering. For that reason, the classification may contain bias. Furthermore, it may be inadequate for capturing all the relationships and aspects of the GDPR, either being too narrow or too broad. For these reasons, to mitigate the threats, we also provide the GDPR chapters where each element can be found. Moreover, we discussed the classification scheme with different data protection lawyers, albeit in a non-systematic manner. This classification scheme should be taken cautiously, and its context validity checked.

In this light, no better approach was available to classify the interest in the GDPR apart from categorizing per article. This approach would have been impractical for a mapping study, as it would provide too many details. Furthermore, it would require a precise and detailed analysis of each paper, which would fall under the scope of a systematic literature review.

Thus, to provide more validity and mitigate threats the classification scheme included "Other" and "Specific article" in case the classification sets provided insufficient. As seen in Sect. 4, a record of processing activities was a category not proposed by our classification that appeared in 4 papers. Hence, if our classification scheme did not capture an important aspect, we could still record it with these other elements. This gave us more flexibility for the classification and helped us mitigate the fact that we might have avoided important GDPR aspects.

All-in-all, given this threat on the usage of a made-up classification scheme, future work could focus on creating a classification scheme for regulatory data protection requirements. A possible approximation could be the creation of an international regulatory data protection ontology.

On another topic, some databases' search strings only included abstracts, keywords, and titles. Therefore, some papers could have been missed from the sample gathered. Some well-known papers were added with snowballing, but this method is not enough to alleviate the inherent threats of search string [42]. Likewise, as this is a mapping study, the inclusion/exclusion criteria were based on the abstracts and meta-data of the population of papers found. How much to read or not to read is subjective and dependent on the authors [60].

However, we do not consider this element a big threat to the validity of our research. As the literature suggests, mapping studies should aim at having a good representative sample of the study area rather than all the papers [39, 40, 42]. Hence, even if our sample might miss some papers, this is an accepted feature between mapping studies, as it differentiates them from literature reviews.

7 Conclusion

GDPR compliance has been an area of interest for the requirements engineering community since the GDPR was signed in 2016 and enacted in 2018. The GDPR lists functional and non-functional requirements, ranging from transparency to specific system functionalities as retention periods. As a result, many requirements researchers have investigated and proposed different artifacts to help organizations achieve compliance with the GDPR.

From a chronological point of view, before the GDPR was enacted, only 12 papers had been published from our sample, meaning that practitioners had limited tools at the moment that organizations were expected to comply. From that date to the present, there has been a growing and ongoing interest regarding requirements for GDPR compliance. The trend seems to keep on going, with new proposals appearing. With the advent of new technological regulations around the world and the EU, it seems that the RE domain will continue studying the subject.

Most papers (57 out of 90) from the sample discussed GDPR compliance as a whole, therefore not focusing on specific elements to achieve GDPR compliance. Based on topics of interest, consent sprung as the subject that attracted the most interest, followed by privacy policies. In both cases, these GDPR articles have very specific requirements that organizations must follow to show compliance. The creation of tools using AI for checking privacy policies seems to be a growing area, that future research should focus on. Regarding the methodology done for validation or evaluating research, the sample does not show a trend and a diversity of methods are used.

As the GDPR is a legal text that may require knowledge of other regulations or laws, interdisciplinary research is essential. Lawyers and policy experts may have different mental models than software engineering over what the law entitles and how to translate it into requirements. For example, erasure may imply the deletion of the data and may be unreadable [61]. In the sample, 20 (22%) papers have at least one author not affiliated with computer science or business informatics, which leads us to deduce they did interdisciplinary research. This result is encouraging, as it means that a 22% of the papers selected may be cataloged as interdisciplinary. It could be interesting for future studies to compare how the analysis of the GDPR requirements differ between papers with at least one author unrelated to computer science/informatics and those where all the authors are from this discipline.

The most popular publication venue is conferences, with 44 papers of the sample being published there. Journals follow with 33 papers, and workshops with 13 papers. Even with 48,9% of papers published in conferences, no conference or venue has published more than 5 papers, as seen in Table 17. Indeed, the venues that have published more than 1 paper on the subject are provided in Table 7. Therefore, the venues of publications are still dispersed. This situation could be explained by the fact that GDPR requirements affect a range of disciplines and not only requirements engineering.

All in all, requirements engineering for GDPR compliance seems to be a well-established study area with ongoing interest. Given the range of proposals for different matters, future studies could focus on comparing the different proposals. Furthermore, as new technological regulations enter into force, the research could focus on whether it is possible to reuse the proposal or artifacts for the GDPR if they have elements in common and which lessons can be learned.

Appendix 1: Papers selected for the mapping study

ID1 Vallina, P., Feal, A., Gamba, J., Vallina-Rodriguez, N., Anta, A.F.: Tales from the porn: A comprehensive privacy analysis of the web porn ecosystem. In: Proceedings of the Internet Measurement Conference. IMC ’19, pp. 245–258. Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3355369.3355583 . https://doi.org/10.1145/3355369.3355583

ID2 Pandit, H.J., O’Sullivan, D., Lewis, D.: Test-driven approach towards gdpr compliance. In: Acosta, M., Cudré-Mauroux, P., Maleshkova, M., Pellegrini, T., Sack, H., Sure-Vetter, Y. (eds.) Semantic Systems. The Power of AI and Knowledge Graphs, pp. 19–33. Springer, Cham (2019)

ID3 Shastri, S., Banakar, V., Wasserman, M., Kumar, A., Chidambaram, V.: Understanding and benchmarking the impact of gdpr on database systems. Proc. VLDB Endow. **13**(7), 1064–1077 (2020) https://doi.org/10.14778/3384345.3384354

ID4 Ryan, P., Brennan, R., Pandit, H.J.: Dpcat: Specification for an interoperable and machine-readable data processing catalogue based on gdpr. Information **13**(5), 244 (2022) https://doi.org/10.3390/info13050244

ID5 Amaral, O., Abualhaija, S., Sabetzadeh, M., Briand, L.: A model-based conceptualization of requirements for compliance checking of data processing against gdpr. In: 2021 IEEE 29th International Requirements Engineering Conference Workshops (REW), pp. 16–20 (2021). https://doi.org/10.1109/REW53955.2021.00009

ID6 Diamantopoulou, V., Mouratidis, H.: Practical evaluation of a reference architecture for the management of privacy level agreements. Information & Computer Security **27**(5), 711–730 (2019) https://doi.org/10.1108/ICS-04-2019-0052

ID7 Meis, R., Heisel, M.: Computer-aided identification and validation of intervenability requirements.

Information **8**(1) (2017) https://doi.org/10.3390/info8010030

ID8 Fan, M., Yu, L., Chen, S., Zhou, H., Luo, X., Li, S., Liu, Y., Liu, J., Liu, T.: An empirical evaluation of gdpr compliance violations in android mhealth apps. In: 2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE), pp. 253–264 (2020). https://doi.org/10.1109/ISSRE5003.2020.00032

ID9 Georgiou, D., Lambrinoudakis, C.: Data protection impact assessment (dpia) for cloud-based health organizations. Future Internet **13**(3), 66 (2021) https://doi.org/10.3390/fi13030066

ID10 Timón López, C., Alamillo Domingo, I., Valero Torrijos, J.: Approaching the data protection impact assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. a special reference to identity management systems. In: Proceedings of the 16th International Conference on Availability, Reliability and Security. ARES 21. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3465481.3469207 . https://doi.org/10.1145/3465481.3469207

ID11 Colesky, M., Ghanavati, S.: Privacy shielding by design - A strategies case for near-compliance. In: 24th IEEE International Requirements Engineering Conference, RE 2016, Beijing, China, September 12-16, 2016, pp. 271–275. IEEE Computer Society, Washington, USA (2016). https://doi.org/10.1109/REW.2016.051 . https://doi.org/10.1109/REW.2016.051

ID12 García, K., Zihlmann, Z., Mayer, S., Tamò-Larrieux, A., Hooss, J.: Towards privacy-friendly smart products. In: 2021 18th International Conference on Privacy, Security and Trust (PST), pp. 1–7 (2021). https://doi.org/10.1109/PST52912.2021.9647826

ID13 Gjermundrød, H., Dionysiou, I., Costa, K.: privacytracker: A privacy-by-design gdpr-compliant framework with verifiable data traceability controls. In: Casteleyn, S., Dolog, P., Pautasso, C. (eds.) Current Trends in Web Engineering, pp. 3–15. Springer, Cham (2016)

ID14 Kabanov, I.: Effective frameworks for delivering compliance with personal data privacy regulatory requirements. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 551–554 (2016). https://doi.org/10.1109/PST.2016.7907015

ID15 Robol, M., Salnitri, M., Giorgini, P.: Toward gdpr-compliant socio-technical systems: Modeling language and reasoning framework. In: Poels, G., Gailly, F., Serral Asensio, E., Snoeck, M. (eds.) The Practice of Enterprise Modeling, pp. 236–250. Springer, Cham (2017)

ID16 Sousa, M., Ferreira, D., Santos-Pereira, C., Bacelar, G., Frade, S., Pestana, O., Cruz-Correia, R.: openEHR based systems and the general data protection regulation (GDPR). Stud Health Technol Inform **247**, 91–95 (2018)

ID17 Kuehnel, S., Zasada, A.: An approach toward the economic assessment of business process compliance. In: Woo, C., Lu, J., Li, Z., Ling, T.W., Li, G., Lee, M.L. (eds.) Advances in Conceptual Modeling, pp. 228–238. Springer, Cham (2018)

ID18 Robol, M., Paja, E., Salnitri, M., Giorgini, P.: Modeling and reasoning about privacy-consent requirements. In: Buchmann, R.A., Karagiannis, D., Kirikova, M. (eds.) The Practice of Enterprise Modeling, pp. 238–254. Springer, Cham (2018)

ID19 Karegar, F., Gerber, N., Volkamer, M., Fischer-Hübner, S.: Helping john to make informed decisions on using social login. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. SAC '18, pp. 1165–1174. Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3167132.3167259 . https://doi.org/10.1145/3167132.3167259

ID20 Mannhardt, F., Petersen, S.A., Oliveira, M.F.: Privacy challenges for process mining in human-centered industrial environments. In: 2018 14th International Conference on Intelligent Environments (IE), pp. 64–71 (2018). https://doi.org/10.1109/IE.2018.00017

ID21 Reinhartz-Berger, I., Zamansky, A., Koschmider, A.: Towards privacy-aware software reuse. In: Proceedings of the 7th International Conference on Model-Driven Engineering and Software Development. MODELSWARD 2019, pp. 448–453. SCITEPRESS - Science and Technology Publications, Lda, Setubal, PRT (2019). https://doi.org/10.5220/0007566204480453 . https://doi.org/10.5220/0007566204480453

ID22 Bartolini, C., Daoudagh, S., Lenzini, G., Marchetti, E.: Gdpr-based user stories in the access control perspective. In: Piattini, M., Cunha, P., Guzmán, I., Pérez-Castillo, R. (eds.) Quality of Information and Communications Technology, pp. 3–17. Springer, Cham (2019)

ID23 Müller, N.M., Kowatsch, D., Debus, P., Mirdita, D., Böttinger, K.: On gdpr compliance of companies' privacy policies. In: Ekštein, K. (ed.) Text, Speech, and Dialogue, pp. 151–159. Springer, Cham (2019)

ID24 Cortina, S., Valoggia, P., Barafort, B., Renault, A.: Designing a data protection process assessment model based on the gdpr. In: Walker, A., O'Connor, R.V., Messnarz, R. (eds.) Systems, Software and Services Process Improvement, pp. 136–148. Springer, Cham (2019)

ID25 Arfelt, E., Basin, D., Debois, S.: Monitoring the gdpr. In: Sako, K., Schneider, S., Ryan, P.Y.A. (eds.) Computer Security – ESOR 2019, pp. 681–699. Springer, Cham (2019)

ID26 De Vos, M., Kirrane, S., Padget, J., Satoh, K.: Odrl policy modelling and compliance checking. In: Fodor, P., Montali, M., Calvanese, D., Roman, D. (eds.) Rules and Reasoning, pp. 36–51. Springer, Cham (2019)

ID27 Diamantopoulou, V., Tsohou, A., Karyda, M.: General data protection regulation and iso/iec 27001:2013: Synergies of activities towards organisations' compliance. In: Gritzalis, S., Weippl, E.R., Katsikas, S.K., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) Trust, Privacy and Security in Digital Business, pp. 94–109. Springer, Cham (2019)

ID28 Piras, L., Al-Obeidallah, M.G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J.B., Fiorani, M., Magkos, E., Sanz, A.C., Pavlidis, M., D'Addario, R., Zorzino, G.G.: Defend architecture: A privacy by design platform for gdpr compliance. In: Gritzalis, S., Weippl, E.R., Katsikas, S.K., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) Trust, Privacy and Security in Digital Business, pp. 78–93. Springer, Cham (2019)

ID29 Mohan, J., Wasserman, M., Chidambaram, V.: Analyzing gdpr compliance through the lens of privacy policy. In: Gadepally, V., Mattson, T., Stonebraker, M., Wang, F., Luo, G., Laing, Y., Dubovitskaya, A. (eds.) Heterogeneous Data Management, Polystores, and Analytics for Healthcare, pp. 82–95. Springer, Cham (2019)

ID30 Gonçalves-Ferreira, D., Sousa, M., Bacelar-Silva, G.M., Frade, S., Antunes, L.F., Beale, T., Cruz-Correia, R.: OpenEHR and general data protection regulation: Evaluation of principles and requirements. JMIR Med Inform **7**(1), 9845 (2019)

ID31 Hofman, D., Lemieux, V.L., Joo, A., Batista, D.A.: "the margin between the edge of the world and infinite possibility". Records Management Journal **29**(1/2), 240–257 (2019) https://doi.org/10.1108/RMJ-12-2018-0045

ID32 Hasan, M.M., Anagnostopoulos, D., Kousiouris, G., Stamati, T., Loucopoulos, P., Nikolaidou, M.: An ontology based framework for e-government regulatory requirements compliance. International Journal of E-Services and Mobile Applications (IJESMA) **11**(2), 22–42 (2019) https://doi.org/10.4018/IJESMA.2019040102

ID33 Zemler, F., Westner, M.: Blockchain and gdpr: Application scenarios and compliance requirements. In: 2019 Portland International Conference on Management of Engineering and Technology (PICMET), pp. 1–8 (2019). https://doi.org/10.23919/PICMET.2019.8893923

ID34 Li, Z.S., Werner, C., Ernst, N.: Continuous requirements: An example using gdpr. In: 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), pp. 144–149 (2019). https://doi.org/10.1109/REW.2019.00031

ID35 Gerl, A., Meier, B.: Privacy in the future of integrated health care services - are privacy languages the key? In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 312–317 (2019). https://doi.org/10.1109/WiMOB.2019.8923532

ID36 Becker, R., Alper, P., Grouès, V., Munoz, S., Jarosz, Y., Lebioda, J., Rege, K., Trefois, C., Satagopam, V., Schneider, R.: DAISY: A Data Information System for accountability under the General Data Protection Regulation. GigaScience **8**(12) (2019) https://doi.org/10.1093/gigascience/giz140https://academic.oup.com/gigascience/article-pdf/8/12/giz140/31731275/giz140_reviewer_2_report_original_submission.pdf. giz140

ID37 Truong, N.B., Sun, K., Lee, G.M., Guo, Y.: Gdpr-compliant personal data management: A blockchain-based solution. IEEE Transactions on Information Forensics and Security **15**, 1746–1761 (2020) https://doi.org/10.1109/TIFS.2019.2948287

ID38 Diamantopoulou, V., Tsohou, A., Karyda, M.: From iso/iec 27002:2013 information security controls to personal data protection controls: Guidelines for gdpr compliance. In: Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J., Antón, A., Gritzalis, S., Pallas, F., Pohle, J., Sasse, A., Meng, W., Furnell, S., Garcia-Alfaro, J. (eds.) Computer Security, pp. 238–257. Springer, Cham (2020)

ID39 Tsohou, A., Magkos, M., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., Debussche, J., Rotoloni, M., Crespo, B.G.-N.: Privacy, security, legal and technology acceptance requirements for a gdpr compliance platform. In: Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J., Antón, A., Gritzalis, S., Pallas, F., Pohle, J., Sasse, A., Meng, W., Furnell, S., Garcia-Alfaro, J. (eds.) Computer Security, pp. 204–223. Springer, Cham (2020)

ID40 Lioudakis, G.V., Koukovini, M.N., Papagiannakopoulou, E.I., Dellas, N., Kalaboukas, K., Carvalho, R.M., Hassani, M., Bracciale, L., Bianchi, G., Juan-Verdejo, A., Alexakis, S., Gaudino, F., Cascone, D., Barracano, P.: Facilitating gdpr compliance: The h2020 bpr4gdpr approach. In: Pappas, I.O., Mikalef, P., Dwivedi, Y.K., Jaccheri, L., Krogstie, J., Mäntymäki, M. (eds.) Digital Transformation for a Sustainable Society in the 21st Century, pp. 72–78. Springer, Cham (2020)

ID41 Rabinia, A., Ghanavati, S., Humphreys, L., Hahmann, T.: A methodology for implementing the formal legal-grl framework: A research preview. In: Madhavji, N., Pasquale, L., Ferrari, A., Gnesi, S. (eds.) Requirements Engineering: Foundation for Software Quality, pp. 124–131. Springer, Cham (2020)

ID42 Barati, M., Rana, O., Petri, I., Theodorakopoulos, G.: Gdpr compliance verification in internet of things. IEEE Access **8**, 119697–119709 (2020) https://doi.org/10.1109/ACCESS.2020.3005509

ID43 Ferreyra, N.E.D., Tessier, P., Pedroza, G., Heisel, M.: Pdp-reqlite: A lightweight approach for the elicitation of privacy and data protection requirements. In: Garcia-Alfaro, J., Navarro-Arribas, G., Herrera-Joancomarti, J. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 161–177. Springer, Cham (2020)

ID44 Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S., Charalabidis, Y.: Preserving digital privacy in e-participation environments: Towards gdpr compliance. Information **11**(2), 117 (2020) https://doi.org/10.3390/info11020117

ID45 Rau, H., Geidel, L., Bialke, M., Blumentritt, A., Langanke, M., Liedtke, W., Pasewald, S., Stahl, D., Bahls, T., Maier, C., Prokosch, H.-U., Hoffmann, W.: 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 **18**(1), 287 (2020)

ID46 Valença, G., Kneuper, R., Rebelo, M.E.: Privacy in software ecosystems - an initial analysis of data protection roles and challenges. In: 2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), pp. 120–123 (2020). https://doi.org/10.1109/SEAA51224.2020.00028

ID47 Debruyne, C., Pandit, H.J., Lewis, D., O'Sullivan, D.: "just-in-time" generation of datasets by considering structured representations of given consent for gdpr compliance. Knowledge and Information Systems **62**(9), 3615–3640 (2020) https://doi.org/10.1007/s10115-020-01468-x

ID48 Serrado, J., Pereira, R.F., Silva, M., Scalabrin Bianchi, I.: Information security frameworks for assisting gdpr compliance in banking industry. Digital Policy, Regulation and Governance **22**(3), 227–244 (2020) https://doi.org/10.1108/DPRG-02-2020-0019

ID49 Tsohou, A., Magkos, E., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., Debussche, J., Rotoloni, M., Gallego-Nicasio Crespo, B.: Privacy, security, legal and technology acceptance elicited and consolidated requirements for a gdpr compliance platform. Information & Computer Security **28**(4), 531–553 (2020) https://doi.org/10.1108/ICS-01-2020-0002

ID50 Diamantopoulou, V., Tsohou, A., Karyda, M.: From iso/iec 27001:2013 and iso/iec 27002:2013 to gdpr compliance controls. Information & Computer Security **28**(4), 645–662 (2020) https://doi.org/10.1108/ICS-01-2020-0004

ID51 Agbo, C.C., Mahmoud, Q.H.: Design and implementation of a blockchain-based e-health consent management framework. In: 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 812–817 (2020). https://doi.org/10.1109/SMC42975.2020.9283203

ID52 Georgiopoulou, Z., Makri, E.-L., Lambrinoudakis, C.: Gdpr compliance: Proposed technical and organizational measures for cloud providers. In: Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J., Antón, A., Gritzalis, S., Pallas, F., Pohle, J., Sasse, A., Meng, W., Furnell, S., Garcia-Alfaro, J. (eds.) Computer Security, pp. 181–194. Springer, Cham (2020)

ID53 Ghayyur, S., Pappachan, P., Wang, G., Mehrotra, S., Venkatasubramanian, N.: Designing privacy preserving data sharing middleware for internet of things. In: Proceedings of the Third Workshop on Data: Acquisition To Analysis. DATA '20, pp. 1–6. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3419016.3431484 . https://doi.org/10.1145/3419016.3431484

ID54 Bonatti, P.A., Ioffredo, L., Petrova, I.M., Sauro, L., Siahaan, I.R.: Real-time reasoning in owl2 for gdpr compliance. Artificial Intelligence **289**, 103389 (2020) https://doi.org/10.1016/j.artint.2020.103389

ID55 István, Z., Ponnapalli, S., Chidambaram, V.: Software-defined data protection: Low overhead policy compliance at the storage layer is within reach! Proceedings of the VLDB Endowment **14**(7), 1167–1174 (2021) https://doi.org/10.14778/3450980.3450986

ID56 Gómez-Martínez, E., Marroyo, M., Acuna, S.T.: Towards the integration of the gdpr in the unified software development process. In: Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE, pp. 199–204 (2021). Knowledge Systems Institute Graduate School

ID57 Al Bassit, A., Krasnashchok, K., Skhiri, S., Mustapha, M.: Policy-based automated compliance checking. In: Moschoyiannis, S., Peñaloza, R., Vanthienen, J., Soylu, A., Roman, D. (eds.) Rules and Reasoning, pp. 3–17. Springer, Cham (2021)

ID58 Menges, F., Latzo, T., Vielberth, M., Sobola, S., Pöhls, H.C., Taubmann, B., Köstler, J., Puchta, A., Freiling, F., Reiser, H.P., Pernul, G.: Towards gdpr-compliant data processing in modern siem systems. Computers & Security **103**, 102165 (2021) https://doi.org/10.1016/j.cose.2020.102165

ID59 Marikyan, D., Llanos, J., Barati, M., Aujla, G., Li, Y., Adu-Duodu, K., Tahir, S., Rana, O., Papagiannidis, S., Ranjan, R., Carr, M.: Privacy & cloud services: Are we there yet? In: 2021 IEEE International Conference on Service-Oriented System Engineering (SOSE), pp. 11–19 (2021). https://doi.org/10.1109/SOSE52839.2021.00006

ID60 Rhahla, M., Allegue, S., Abdellatif, T.: Guidelines for gdpr compliance in big data systems. Journal of Information Security and Applications **61**, 102896 (2021) https://doi.org/10.1016/j.jisa.2021.102896

ID61 Bonatti, P.A., Sauro, L., Langens, J.: Representing consent and policies for compliance. In: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS &PW), pp. 283–291 (2021). https://doi.org/10.1109/EuroSPW54576.2021.00036

ID62 Alkubaisy, D., Piras, L., Al-Obeidallah, M.G., Cox, K., Mouratidis, H.: A framework for privacy and security requirements analysis and conflict resolution for supporting gdpr compliance through privacy-by-design. In: Ali, R., Kaindl, H., Maciaszek, L.A. (eds.) Evaluation of Novel Approaches to Software Engineering, pp. 67–87. Springer, Cham (2022)

ID63 Diamantopoulou, V., Karyda, M.: Integrating privacy-by-design with business process redesign. In: Katsikas, S., Lambrinoudakis, C., Cuppens, N., Mylopoulos, J., Kalloniatis, C., Meng, W., Furnell, S., Pallas, F., Pohle, J., Sasse, M.A., Abie, H., Ranise, S., Verderame, L., Cambiaso, E., Maestre Vidal, J., Sotelo Monge, M.A. (eds.) Computer Security. ESORICS 2021 International Workshops, pp. 127–137. Springer, Cham (2022)

ID64 Almeida, J., Cunha, P.R., Pereira, A.D.: Gdpr-compliant data processing: Practical considerations. In: Themistocleous, M., Papadaki, M. (eds.) Information Systems, pp. 505–514. Springer, Cham (2022)

ID65 Baramashetru, C.P., Tapia Tarifa, S.L., Owe, O., Gruschka, N.: A policy language to capture compliance of data protection requirements. In: Beek, M.H., Monahan, R. (eds.) Integrated Formal Methods, pp. 289–309. Springer, Cham (2022)

ID66 Cozar, M., Rodriguez, D., Del Alamo, J.M., Guaman, D.: Reliability of ip geolocation services for assessing the compliance of international data transfers. In: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS &PW), pp. 181–185 (2022). https://doi.org/10.1109/EuroSPW55150.2022.00024

ID67 Bateni, N., Kaur, J., Dara, R., Song, F.: Content analysis of privacy policies before and after gdpr. In: 2022 19th Annual International Conference on Privacy, Security & Trust (PST), pp. 1–9 (2022). https://doi.org/10.1109/PST55820.2022.9851983

ID68 Leite, L., Santos, D.R., Almeida, F.: The impact of general data protection regulation on software engineering practices. Information & Computer Security **30**(1), 79–96 (2022) https://doi.org/10.1108/ICS-03-2020-0043

ID69 Tokas, S., Owe, O., Ramezanifarkhani, T.: Static checking of gdpr-related privacy compliance for object-oriented distributed systems. Journal of Logical and Algebraic Methods in Programming **125**, 100733 (2022) https://doi.org/10.1016/j.jlamp.2021.100733

ID70 Chhetri, T.R., Kurteva, A., DeLong, R.J., Hilscher, R., Korte, K., Fensel, A.: Data protection by design tool for automated gdpr compliance verification based on semantically modeled informed consent. Sensors **22**(7), 2763 (2022) https://doi.org/10.3390/s22072763

ID71 Li, Z.S., Werner, C., Ernst, N., Damian, D.: Towards privacy compliance: A design science study in a small organization. Information and Software Technology **146**, 106868 (2022) https://doi.org/10.1016/j.infsof.2022.106868

ID72 Becher, S., Gerl, A.: ConTra preference language: Privacy preference unification via privacy interfaces. Sensors (Basel) **22**(14) (2022)

ID73 Peyrone, N., Wichadakul, D.: Formal models for consent-based privacy. Journal of Logical and Algebraic Methods in Programming **128**, 100789 (2022) https://doi.org/10.1016/j.jlamp.2022.100789

ID74 Ayala-Rivera, V., Pasquale, L.: The grace period has ended: An approach to operationalize gdpr requirements. In: 2018 IEEE 26th International Requirements Engineering Conference (RE), pp. 136–146 (2018). https://doi.org/10.1109/RE.2018.00023

ID75 Guamán, D.S., Del Alamo, J.M., Caiza, J.C.: Gdpr compliance assessment for cross-border personal data transfers in android apps. IEEE Access **9**, 15961–15982 (2021) https://doi.org/10.1109/ACCESS.2021.3053130

ID76 Ujcich, B.E., Sanders, W.H.: Data protection intents for software-defined networking. In: 2019 IEEE Conference on Network Softwarization (NetSoft), pp. 271–275 (2019). https://doi.org/10.1109/NETSOFT.2019.8806684

ID77 Sion, L., Dewitte, P., Van Landuyt, D., Wuyts, K., Emanuilov, I., Valcke, P., Joosen, W.: An architectural view for data protection by design. In: 2019 IEEE International Conference on Software Architecture (ICSA), pp. 11–20 (2019). https://doi.org/10.1109/ICSA.2019.00010

ID78 Abualhaija, S., Arora, C., Sleimi, A., Briand, L.C.: Automated question answering for improved understanding of compliance requirements: A multi-document study. In: 2022 IEEE 30th International Requirements Engineering Conference (RE), pp. 39–50 (2022). https://doi.org/10.1109/RE54965.2022.00011

ID79 Negri-Ribalta, C., Noel, R., Herbaut, N., Pastor, O., Salinesi, C.: Socio-technical modelling for gdpr principles: an extension for the sts-ml. In: 2022 IEEE 30th International Requirements Engineering Conference Workshops (REW), pp. 238–234 (2022). https://doi.org/10.1109/REW56159.2022.00052

ID80 Davari, M., Bertino, E.: Access control model extensions to support data privacy protection based on gdpr. In: 2019 IEEE International Conference on Big Data (Big Data), pp. 4017–4024 (2019). https://doi.org/10.1109/BigData47090.2019.9006455

ID81 Torre, D., Abualhaija, S., Sabetzadeh, M., Briand, L., Baetens, K., Goes, P., Forastier, S.: An ai-assisted approach for checking the completeness of privacy policies against gdpr. In: 2020 IEEE 28th International Requirements Engineering Conference (RE), pp. 136–146 (2020). https://doi.org/10.1109/RE48521.2020.00025

ID82 Amaral, O., Abualhaija, S., Torre, D., Sabetzadeh, M., Briand, L.C.: Ai-enabled automation for completeness checking of privacy policies. IEEE Transactions on Software Engineering **48**(11), 4647–4674 (2021)

ID83 Jesus, V., Pandit, H.J.: Consent receipts for a usable and auditable web of personal data. IEEE Access **10**, 28545–28563 (2022) https://doi.org/10.1109/ACCESS.2022.3157850

ID84 McDonald, S., Towey, D., Brusic, V.: Social impact of smart environments: Software engineering perspectives and challenges. In: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1592–1597 (2022). https://doi.org/10.1109/COMPSAC54236.2022.00253

ID85 Stach, C., Gritti, C., Przytarski, D., Mitschang, B.: Can blockchains and data privacy laws be reconciled? a fundamental study of how privacy-aware blockchains are feasible. In: Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing. SAC '22, pp. 1218–1227. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3477314.3506986 . https://doi.org/10.1145/3477314.3506986

ID86 Rahat, T.A., Long, M., Tian, Y.: Is your policy compliant? a deep learning-based empirical study of privacy policies' compliance with gdpr. In: Proceedings of the 21st Workshop on Privacy in the Electronic Society. WPES'22, pp. 89–102. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3559613.3563195 . https://doi.org/10.1145/3559613.3563195

ID87 Robol, M., Breaux, T.D., Paja, E., Giorgini, P.: Consent verification monitoring. ACM Trans. Softw. Eng. Methodol. (2022) https://doi.org/10.1145/3490754 . Just Accepted

ID88 Torre, D., Soltana, G., Sabetzadeh, M., Briand, L.C., Auffinger, Y., Goes, P.: Using models to enable compliance checking against the gdpr: An experience report. In: 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS), pp. 1–11 (2019). https://doi.org/10.1109/MODELS.2019.00-20

ID89 Tom, J., Sing, E., Matulevičius, R.: Conceptual representation of the gdpr: Model and application directions. In: Zdravkovic, J., Grabis, J., Nurcan, S., Stirna, J. (eds.) Perspectives in Business Informatics Research, pp. 18–28. Springer, Cham (2018)

ID90 Vanezi, E., Kapitsaki, G.M., Kouzapas, D., Philippou, A., Papadopoulos, G.A.: Diálogop - a language and a graphical tool for formally defining gdpr purposes. Lecture notes in business information processing (2020) https://doi.org/10.1007/978-3-030-50316-1_40

Appendix 2: Venues of the selected papers

See Table 17.

Table 17 Venues of selected sample papers

Venue name	Number of articles
ACM Transactions on Software Engineering and Methodology (TOSEM)	1
ACM/IEEE International Conference on Model-Driven Engineering Languages and Systems (Models)	1
Annual ACM Symposium on Applied Computing (SAC)	2
Annual Computers, Software, and Applications Conference (COMPSAC)	1
Annual International Conference on Privacy, Security and Trust (PST)	3
Artificial Intelligence (AIJ)	1
CCS Workshops: Workshop on Privacy in the Electronic Society (WPES)	1
Computers and Security	1
Conference International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ)	1
Digital Policy, Regulation and Governance	1
Euromicro Conference on Software Engineering and Advanced Applications (SEAA)	1
European Conference on Software Process Improvement (EuroSPI)	1
European Symposium on Research in Computer Security (ESORICS)	1
European Symposium on Research in Computer Security International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT (ESORICS workshops)	4
↪International Workshop on Security and Privacy Requirements Engineering (SECPRE)	3
↪DPM Workshop: Obfuscation, Contact Tracing and Engineering	1
European, Mediterranean, and Middle Eastern Conference on Information Systems (EMCIS)	1
Future Internet	1
GigaScience	1
IEEE Access	3
IEEE European Symposium on Security and Privacy Workshops (EuroS &PW)	2
↪International Workshop on Consent Management in Online Services, Networks and Things (COnSeNT)	1
↪International Workshop on Privacy Engineering—IWPE	1
IEEE International Conference on Big Data (Big Data)	1
IEEE International Conference on Systems, Man and Cybernetics (SMC)	1
IEEE International Conference on Wireless and Mobile Computing Networking and Communications (WiMOB)	1
IEEE Transactions on Information Forensics and Security (IEEE TIFS)	1
IEEE Transactions on Software Engineering (IEEE TSE)	1
IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society (I3E)	1
Information (Switzerland)	3
Information and Computer Security	5
Information and Software Technology	1
International Conference on Conceptual Modeling (ER)	1
International Conference on Model-Driven Engineering and Software Development (MODELSWARD)	1
International Conference on Network Softwarization (Netsoft)	1
International Conference on Semantic Systems (SEMANTiCS)	1
International Conference on Service-Oriented System Engineering (SOSE)	1
International Conference on Software Architecture (ICSA)	1
International Conference on Software Engineering and Knowledge Engineering (SEKE)	1
International Conference on Text Speech and Dialogue (TSD)	1
International Conference on the Quality of Information and Communications Technology (QUATIC)	1
International Conference on Trust, Privacy and Security in Digital Business (TrustBus)	2
International Conference on Web Engineering (ICWE)	1
International Conference on integrated Formal Methods (iFM)	1
International Journal of E-Services and Mobile Applications (IJESMA)	1
International Requirements Engineering Conference (RE)	3
International Requirements Engineering Conference Workshops (REW)	4

Table 17 (continued)

Venue name	Number of articles
↪Evolving Security and Privacy Requirements Engineering Workshop (ESPRE)	2
↪International Workshop on Requirements Engineering and Law (RELAW)	1
↪Model-Driven Requirements Engineering (MoDRE) Workshop	1
International Symposium on Software Reliability Engineering (ISSRE)	1
International conference on Evaluation of novel approaches to software engineering (ENASE)	1
Internet Measurement Conference (IMC)	1
JMIR Medical Informatics	1
Journal of Information Security and Applications	1
Journal of Logical and Algebraic Methods in Programming	2
Journal of Translational Medicine	1
Knowledge and Information Systems (KAIS)	1
Perspectives in Business Informatics Research (BIR)	1
Portland International Conference on Management of Engineering and Technology: Technology Management in the World of Intelligent Systems (PICMET)	1
Records Management Journal	1
Research Challenges in Information Science (RCIS)	1
Rules and Reasoning (RuleML+RR)	1
Sensors	2
Sensys Workshops: Workshop on Data: Acquisition To Analysis (DATA)	1
Studies in Health Technology and Informatics	1
The IFIP WG8.1 Working Conference on the Practice of Enterprise Modelling (PoEM)	2
The International Conference on Availability, Reliability and Security (ARES)	1
The International Conference on Intelligent Environments (IE)	1
VLDB Endowment Proceedings (VLDB)	2
VLDB workshops: International Workshop on Polystores and Other Systems for Heterogeneous Data (DMAH, Poly)	1

Acknowledgements The authors would like to thank the anonymous reviewers as well as René Noël and Nicolas Herbaut for their feedback. The authors would also like to thank Daniel Amyot,Oscar Pastor, Saïd Assar, Jolita Ralyte, Irina Rychkova for their comments during the redaction of this paper.

Funding This project has received funding from the Luxembourg National Research Fund (FNR), grant NCER22/IS/16570468/NCER-FT. The authors have no other interests to disclose.

Data availability Data used for the mapping study is available anonymously at the following link https://zenodo.org/records/10040309. The repository includes: The data set of all the research papers collected and how they were tagged: accepted, rejected or duplicate. It also includes the reason for rejection. The final sample of papers used for the mapping, including those that were snowballed.

Declarations

Conflict of interest Part of this works was part of the first author PhD thesis at Université Paris 1 Panthéon-Sorbonne, Paris, France.

References

1. European Union: Regulation (EU) 2016/678 of the European Parliament and of the Council—General Data Protection Regulation
2. Data Protection Commission: Data Protection Commission announces conclusion of two inquiries into Meta Ireland | 04/01/2023 | Data Protection Commission. https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland. Accessed 27 Jan 2023
3. Schmidt A, Esser L (2022) Numbers and figures | GDPR Enforcement Tracker Report 2022. https://cms.law/en/fra/publication/gdpr-enforcement-tracker-report/numbers-and-figures. Accessed 27 Jan 2023

4. Breaux TD, Antón AI (2007) A systematic method for acquiring regulatory requirements: a frame-based approach. RHAS-6), Delhi, India
5. He Q, Antón AI et al (2003) A framework for modeling privacy requirements in role engineering. In: Proceedings of REFSQ, vol 3, pp 137–146
6. Breaux T, Antón A (2008) Analyzing regulatory rules for privacy and security requirements. IEEE Trans Softw Eng 34(1):5–20
7. Breaux T, Norton T (2022) Legal accountability as software quality: a U.S. data processing perspective. In: 2022 IEEE 30th international requirements engineering conference (RE). IEEE
8. Pohl K, Rupp C (2015) Requirements engineering fundamentals: a study guide for the certified professional for requirements engineering exam—foundation level—IREB compliant. Rocky Nook computing. Rocky Nook, Santa Barbara, CA 93103, USA. https://books.google.fr/books?id=bM1YrgEACAAJ
9. Glinz M (2007) On non-functional requirements. In: 15th IEEE international requirements engineering conference (RE 2007). IEEE, pp 21–26
10. Breaux TD, Anton AI, Vail MW (2006) Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. North Carolina State University. Department of Computer Science, Technical report
11. Hadar I, Hasson T, Ayalon O, Toch E, Birnhack M, Sherman S, Balissa A (2018) Privacy by designers: Software developers' privacy mindset. In: Proceedings of the 40th international conference on software engineering, Gothenburg, Sweden. ICSE '18, p. 396. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3180155.3182531
12. Senarath A, Arachchilage NAG (2018)Why developers cannot embed privacy into software systems? an empirical investigation. In: Proceedings of the 22nd international conference on evaluation and assessment in software engineering 2018. EASE'18, pp. 211–216. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3210459.3210484
13. Birnhack M, Toch E, Hadar I (2014) Privacy mindset, technological mindset. Jurimetrics 55:55
14. Mouratidis H, Kalloniatis C, Islam S, Hudic A, Zechner L (2012) Model based process to support security and privacy requirements engineering. Int J Secure Softw Eng 3:1–22. https://doi.org/10.4018/jsse.2012070101
15. Solove DJ (2006) A taxonomy of privacy. University of Pennsylvania law review, pp 477–564
16. Westin AF, Solove DJ (2015) Privacy and Freedom. Ig Publishing, New York, NY 10163 . https://books.google.fr/books?id=1RXqoAEACAAJ
17. Kalloniatis C, Kavakli E, Gritzalis S (2009) Methods for designing privacy aware information systems: a review. In: 2009 13th Panhellenic conference on informatics. IEEE, pp 185–194
18. Pattakou A, Mavroeidi AG, Diamantopoulou V, Kalloniatis C, Gritzalis S (2018) Towards the design of usable privacy by design methodologies, pp 1–8. https://doi.org/10.1109/ESPRE.2018.00007
19. Morales-Trujillo ME, García-Mireles GA, Matla-Cruz EO, Piattini M (2019) A systematic mapping study on privacy by design in software engineering. CLEI Electron J 22(1):4–1
20. Netto D, Peixoto MM, Silva C (2019) Privacy and security in requirements engineering: Results from a systematic literature mapping. In: WER
21. Canedo ED, Bandeira IN, Calazans ATS, Costa PHT, Cançado ECR, Bonifácio R (2023) Privacy requirements elicitation: a systematic literature review and perception analysis of it practitioners. Requir Eng 28(2):177–194
22. Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W (2011) A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir Eng 16(1):3–32
23. Wuyts K, Joosen W (2015) LINDDUN privacy threat modeling: a tutorial. Department of Computer Science, KU Leuven, Leuven, Belgium (2015-07-01)
24. Wuyts K, Sion L, Joosen W (2020) LINDDUN GO: A lightweight approach to privacy threat modeling. In: IEEE European symposium on security and privacy workshops, EuroS &P workshops 2020, Genoa, Italy, September 7–11, 2020. IEEE, test, pp 302–309. https://doi.org/10.1109/EuroSPW51379.2020.00047
25. Kalloniatis C, Kavakli E, Gritzalis S (2008) Addressing privacy requirements in system design: the pris method. Requir Eng 13(3):241–255
26. Kavakli E, Kalloniatis C, Loucopoulos P, Gritzalis S (2006) Incorporating privacy requirements into the system design process: the pris conceptual framework. Internet research
27. Spiekermann S, Cranor LF (2009) Engineering privacy. IEEE Trans Software Eng 35(1):67–82. https://doi.org/10.1109/TSE.2008.88
28. Akhigbe O, Amyot D, Richards G (2019) A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance. Requir Eng 24:459–481
29. Almeida Teixeira G, Silva M, Pereira R (2019) The critical success factors of GDPR implementation: a systematic literature review. Digit Policy Regul Gov 21(4):402–418
30. Aberkane A-J, Poels G, Broucke SV (2021) Exploring automated GDPR-compliance in requirements engineering: A systematic mapping study. IEEE Access 9:66542–66559
31. Palmirani M, Martoni M, Rossi A, Bartolini C, Robaldo L (2018) Pronto: privacy ontology for legal reasoning. In: International conference on electronic government and the information systems perspective. Springer, pp 139–152
32. Robaldo L, Bartolini C, Palmirani M, Rossi A, Martoni M, Lenzini G (2020) Formalizing GDPR provisions in reified i/o logic: the dapreco knowledge base. J Logic Lang Inform 29(4):401–449
33. Gharib M, Mylopoulos J, Giorgini P (2020) Copri—a core ontology for privacy requirements engineering. In: International conference on research challenges in information science. Springer, pp 472–489
34. Loukil F, Ghedira-Guegan C, Boukadi K, Benharkat AN (2018) Liopy: A legal compliant ontology to preserve privacy for the internet of things. In: 2018 IEEE 42nd annual computer software and applications conference (COMPSAC), vol 2. IEEE, pp 701–706
35. Pandit HJ, Lewis D (2017) Modelling provenance for GDPR compliance using linked open data vocabularies. In: PrivOn@ ISWC, pp 39–40
36. Pandit HJ, Fatema K, O'Sullivan D, Lewis D (2018) Gdprtext—GDPR as a linked data resource. In: Gangemi A, Navigli R, Vidal M-E, Hitzler P, Troncy R, Hollink L, Tordai A, Alam M (eds) The semantic web. Springer, Cham, pp 481–495
37. Pandit HJ, Debruyne C, O'Sullivan D, Lewis D (2019) Gconsent-a consent ontology based on the GDPR. In: European semantic web conference. Springer, pp 270–282
38. Economic Co-Operation O (1980) Development: OECD guidelines on the protection of privacy and transborder flows of personal data. Technical report. https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum
39. Petersen K, Feldt R, Mujtaba S, Mattsson M (2008) Systematic mapping studies in software engineering. In: 12th international conference on evaluation and assessment in software engineering (EASE), vol 12, pp 1–10
40. Petersen K, Vakkalanka S, Kuzniarz L (2015) Guidelines for conducting systematic mapping studies in software engineering: an update. Inf Softw Technol 64:1–18

41. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering, vol 2
42. Wohlin C, Runeson P, Neto PADMS, Engström E, Carmo Machado I, De Almeida ES (2013) On the reliability of mapping studies in software engineering. J Syst Softw 86(10):2594–2610
43. Wieringa R, Maiden N, Mead N, Rolland C (2006) Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requir Eng 11(1):102–107
44. Kitchenham B (2010) What's up with software metrics? A preliminary mapping study. J Syst Softw 83:37–51. https://doi.org/10.1016/j.jss.2009.06.041
45. Nissenbaum H (2004) Privacy as contextual integrity. Wash. L. Rev. 79:119
46. Wieringa RJ (2014) Design science methodology for information systems and software engineering. Springer, Cham
47. Wieringa R (2014) Empirical research methods for technology validation: scaling up to practice. J Syst Softw 95:19–31
48. Sommerville I (2015) Software engineering, 10th edn. Pearson, Amsterdam
49. Voigt P, Bussche A (2017) The EU general data protection regulation (GDPR): a practical Guide. https://doi.org/10.1007/978-3-319-57959-7
50. Ustaran E (2019) European data protection: law and practice. An IAPP Publication, International Association of Privacy Professionals, Portsmouth, NH, USA
51. Cavoukian A (2009) Privacy by design
52. Information Commissioner's Office: Guide to the General Data Protection Reuglation (GDPR). Technical report, Information Commissioner's Office (January 2021). https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf
53. Kuehnel S, Zasada A (2018) An approach toward the economic assessment of business process compliance. In: Woo C, Lu J, Li Z, Ling TW, Li G, Lee ML (eds) Advances in conceptual modeling. Springer, Cham, pp 228–238
54. Dalpiaz F, Paja E, Giorgini P (2016) Security requirements engineering: designing secure socio-technical systems. Massachusetts, Cambridge
55. Mouratidis H, Giorgini P (2007) Secure tropos: a security-oriented extension of the tropos methodology. Int J Software Eng Knowl Eng 17(02):285–309
56. Amyot D, Ghanavati S, Horkoff J, Mussbacher G, Peyton L, Yu E (2010) Evaluating goal models within the goal-oriented requirement language. Int J Intell Syst 25(8):841–877. https://doi.org/10.1002/int.20433
57. Booch G (2005) The unified modeling language user guide. Pearson Education India, Chennai
58. European Data Protection Board: Guidelines 4/2019 on article 25 data protection by design and by default version 2.0. Technical report, European Data Protection Board (October 2020). Guidelines adopted
59. Community W, Process BG (2022) Data Privacy Vocabulary (DPV). https://www.w3.org/community/reports/dpvcg/CG-FINAL-dpv-20221205/
60. Souag A, Salinesi C, Mazo R, Comyn-Wattiau I (2015) A security ontology for security requirements elicitation. In: ESSoS. Springer, pp 157–177
61. Finck M (2018) Blockchains and data protection in the European union. Eur Data Prot Law Rev 4:17–35

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.