Journal of High Speed Networks 30 (2024) 147–174
DOI 10.3233/JHS-230080
IOS Press

GDPR compliance through standard security controls: An automated approach

Daniele Granata [a,*], Michele Mastroianni [b], Massimiliano Rak [a], Pasquale Cantiello [c] and Giovanni Salzillo [a]

[a] *Department of Engeenering, University of Campania Luigi Vanvitelli, Aversa, Italy*
E-mails: daniele.granata@unicampania.it, massimiliano.rak@unicampania.it, giovanni.salzillo@unicampania.it
[b] *Department of Computer Science, University of Salerno, Fisciano, Italy*
E-mail: mmastroianni@unisa.it
[c] *Osservatorio Vesuviano, Istituto Nazionale di Geofisica e Vulcanologia, Napoli, Italy*
E-mail: pasquale.cantiello@ingv.it

Received 19 June 2023
Accepted 5 January 2024

Abstract. Since 2018, the enactment of the General Data Protection Regulation (GDPR) has bestowed distinct privileges upon each person while imposing protocols to safeguard personal information. The GDPR effectively tackles an evident requirement within our interconnected, social media-driven society. However, its compliance poses a considerable challenge, particularly for small and medium-sized businesses. This work aims to identify and select the proper countermeasures in order to comply with GDPR, by using standard security controls. Thus, we designed a tool to handle some phases of the compliance process in an almost semi-automated way. The proposed approach relies on standard security control frameworks (namely NIST SP-800-53) and can be easily adapted to different frameworks. The proposed technique was validated using our university as a case study, through a simple demonstrator, although the solution can be transparently applied to different contexts.

Keywords: GDPR, privacy, cloud, security policy, security control framework

1. Introduction

The extensive proliferation of high-speed networks and the pervasiveness of the new connected technologies (e.g. IoT), demanding perpetual data exchange and the outsourcing of resources to service providers has markedly heightened the necessity for safeguarding personal information. Service Providers collect the data of their customers and could be able to profile very accurately each user, to offer personalized services and advertisements, but also abuse the collected information, going deep into the personal data of each customer. Consequently, in recent years, governments have established and enforced novel regulations to safeguard the private sphere of each person. Starting from 2018, the General Data Protection Regulation (GDPR) has been implemented in Europe, bestowing distinct rights upon every individual while introducing fresh protocols for personal data protection.

The GDPR delineates precise entitlements for each European citizen, with a particular emphasis on their control over personal data. For instance, individuals possess the right to ascertain the custodians of their personal information and to request its deletion. In accordance with the GDPR, service providers may engage in data processing

*Corresponding author. E-mail: daniele.granata@unicampania.it.

without explicit consent only under specific circumstances as outlined in Articles 6, 9, and 10. They are also mandated to employ all requisite safeguards to ensure the security of such data and, in the event of a data breach, to promptly notify affected citizens.

The GDPR responds to a clear need to protect user data, today more exposed than before also because of the widespread use of *social networks*. However, an unintended consequence of these regulations is the revelation of the challenges faced by numerous legitimate enterprises, particularly small and medium-sized ones, in meeting these new mandates. The rights of a data subject (access, portability, deletion, ...) imply that a service provider should be able to keep track of any reference to an individual in its data set. In order to perform such data traceability, requires the Small and Medium-Sized Enterprises (SME) to have their data precisely organized, which is often hard to design and enforce. Another relevant example concerns data protection and security measures. In some cases, (stated by Art. 35) the service provider is required to carry out a risk analysis process, by completing the Data Privacy Impact Assessment (DPIA) and selecting the remediation. However, conducting a DPIA is not an effortless analysis and, for a correct risk assessment, the data controllers must demonstrate that all the security measures available in the state of the art, both organizational and technical, have been adopted. One of the suggested measures is the acquisition of security certifications (e.g. ISO 27000 [29]), although these are often both expensive and not a sufficient guarantee that all the possible privacy problems have been addressed.

The approach outlined in this paper squarely focuses on a highly particular concern: the identification of necessary countermeasures for showcasing adherence to GDPR requirements. Our suggestion involves the utilization of NIST's established security controls (SP 800-53 [31]), with the aim of offering a universally applicable solution.

As a result, this paper introduces the subsequent fresh and pioneering outcomes:

- The creation of a correlation between NIST's standard security controls and GDPR principles (described in a previous work [7], with the purpose of discerning collections of security controls that guarantee alignment with GDPR.
- A process that, using the proposed mapping, the actors of the GDPR (Data processor, Data Controller and/or DPO as described later) can be used to select the appropriate controls.
- A demonstrator tool that supports GDPR actors in the application of the process and its validation.[1]

It must be clarified that this is an ICT technical paper, not a legal paper. In order to guarantee (fully) legal compliance to GDPR, there is both technical and legal work to do. This paper focuses on the technical aspects. However, it should be noted that the GDPR (which is a regulation and implies mainly the work of a lawyer to guarantee compliance), has a lot of requirements from a technical perspective, which are very hard to address for non-technical experts. Just as an example, no lawyer can compare anonymization algorithms measuring the k-anonymity level that they can assure. But every lawyer will be able to say that if you can reconstruct the identified person, the adopted anonymization algorithm is incorrect. Our methodology aims to offer a technical solution that synthesizes the checks to be done (using standard references), so that the lawyer will have all the necessary information to demonstrate needed to demonstrate the correctness and compliance of the technical solution to GDPR.

Given such a clarification, it is worth noticing that we are going to adopt security controls in order to address privacy issues. Privacy and Security are strictly connected, but they are different topics: privacy addresses the identification of acceptable data processing, and identifying the requirements for the system, which, in turn, implies (mostly) security requirements: Only authorized people are able to address data/resources (confidentiality); Data and resources can only be altered by authorized individuals in authorized manners, ensuring their integrity. Additionally, data and resources are accessible to authorized individuals as needed. Synthetically, Privacy addresses WHAT should be granted, Security addresses HOW to address such requirements.

Security Controls, which we will define in a more detailed way in Section 3 are the way that enables us to verify that Security requirements are being correctly fulfilled. Adoption of security controls to address even privacy issues is, nowadays, a common practice, as illustrated in the state of art [35,42], as an example, Italian National

[1] You can find the tool at this repository: https://github.com/VSecLab/OpenData/tree/main/GDPRComplianceTool_MDPI_2022.

Cybersecurity framework (based on the NIST one) offers a profile for granting GDPR compliance, using as a reference framework the CIS Control framework (instead of the NIST one, as we made in this paper).

The paper is organized as follows: Section 2 outlines the existing challenges associated with GDPR adoption and privacy management, summarizing the findings and developments within the current state of the field. Section 3 describes the open issues, our proposed approach and the methodology behind the adoption of the standard NIST security controls to address GDPR compliance. Section 4 describes the tool we developed in order to implement such an approach. Section 5 describes a concrete case study and Section 6 summarizes the conclusions, presenting a set of future works.

2. Related works

The need to address compliance with the GDPR in a verifiable way and the correct adoption of security countermeasures capable of addressing privacy requirements is addressed by the standardization processes. In fact, a new ISO standard was recently issued, ISO/IEC 27701:2019 [30] which describes specific criteria for evaluating the GDPR. Additionally, the NIST's Cybersecurity Framework [35] represents a step forward in integrating privacy issues with the security controls offered by security frameworks. The NIST Framework collects the controls offered by different frameworks into categories and, for specific categories (i.e. subcategories), it reports the related GDPR articles. Furthermore, the NIST SP-800-53 security control framework (draft version 5, officially released in September 2020), proposes a series of tables outlining the relation between security controls to privacy requirements. It is worth noting that the release 5 of the same special publication has completely changed the approach to privacy management compared to previous versions (revisions 3 and 4 proposed a set of privacy controls in a further appendix). Section 3.2 discusses privacy management in the NIST framework in further detail.

A compelling approach that integrates semantic methods for GDPR compliance is shown in [19,20]: the authors created a comprehensive and semantically enriched knowledge graph, often referred to as an ontology, to encompass the regulations imposed by both PCI DSS[2] and the EU GDPR. The adopted approach reminds the one proposed within this work but differs in the type of the involved controls (PCI DSS instead of NIST Framework) and for a more explicit adoption of semantic techniques.

Another intriguing research direction can be found in [14,39], which aims to include rules related to GDPR into BPMN (Business Process Model and Notation). This augmentation is designed to support risk analysis procedures (e.g., [22,26]) and verification of compliance [27]. As detailed in Section 6, our goal is to integrate this approach with the one proposed here, mixing the semantic model, our conceptual map [7], and the use of standard security controls.

Another methodology, similarly grounded in ontologies, is presented in [38]. In this research, the authors introduce *PrOnto*, a tool designed to streamline the creation of legal knowledge related to privacy entities, data categories, processing activities, as well as entitlements and responsibilities. This is achieved through a methodology that combines legal theory analysis with ontological patterns.

In the work referenced as [13], they introduce an ontology-driven model aimed at encapsulating the data within PLAs. This allows various software tools to harness and manipulate this information for a range of applications, such as automating the discovery and comparison of service offerings.

A different approach to handling privacy requirements was studied by Rios et al. in [42]. They tried to use the ideas and outcomes from the MUSA project, which recommends a development process to meet security needs with Security Service Level Agreements. Their approach differs from the one presented in this paper because it mainly deals with Security SLAs and privacy, not compliance.

In [17], the authors suggest using ISO27000 controls to meet GDPR compliance. They pinpoint a set of controls in the ISO27000 framework and provide guidance on how to understand and apply them to adhere to GDPR rules. Although their approach resembles ours, they don't explain the control selection process in detail, leaving some

[2]PCI DSS: Payment Card Industry Data Security Standards – https://www.pcisecuritystandards.org/.

uncertainty about its thoroughness. Furthermore, they don't offer support for automating the process or applying it in real-world GDPR compliance verification.

The same team explored GDPR compliance in different settings (public administration and crowdsourcing) using less formal techniques in [16] and in [15]. However, their method is distinct from ours as they analyze each GDPR article to propose changes to ISO 27001 and ISO 27002 standards to meet GDPR requirements.

To analyse the GDPR impact on research activities, there are many sources to read, and – not surprisingly – they are found in clinical scientific journals.

In order to enforce security measures for data processing, two different techniques can be used [12]:

- *Anonymization*: Information that does not relate to a named or distinguishable natural person, or information that has been made anonymous in a way making it nearly impossible to identify the data subject.
- *Pseudonymization*: Any personally identifiable information is replaced with a pseudonym (a value that prevents the data subject from being directly identified).

The concept of pseudonymization is explored in greater detail in [34]. It's important to note that the definition of pseudonymization is not meant to determine whether data qualifies as personal under the GDPR; it's evident that data to which pseudonymization is applied still retains its status as personal data. In essence, pseudonymization should not be confused with anonymization. Instead, Recital 26 of the GDPR should be utilized to determine whether data qualifies as personal.

Additionally, practical illustrations that emphasize the contrast between anonymization and pseudonymization can be found in [36].

In the literature, there are also different approaches based on blockchain technology for GDPR compliance, mainly focusing on the monitoring of the activities affecting the users' data than the enforcement of any preventive security measure. The authors of [5] proposed a formal model for supporting GDPR compliance checking from smart (IoT) devices based on smart contracts. The idea that there is behind is to track the operations carried out by a device on a distributed and immutable ledger to check whether it infringes user privacy.

In [4], The authors described a novel strategy based on encoding GDPR rules into smart contract opcodes. These operations are then recorded on a blockchain to enable auditing. They developed an abstract model to show how cloud service providers could use a blockchain-based virtual machine to access and carry out the smart contracts. Additionally, they presented a case study to exemplify their approach. Readers looking for more research on using blockchain for GDPR compliance management can explore further studies in [33] and [32].

In [28], the authors leveraged a machine learning approach to automate GDPR compliance checking. They develop specific methods to automate compliance checking of privacy policies, relying on NLP to extract data practices from privacy policies and then encoding GDPR rules to check the presence of mandatory information.

Authors of [6] proposed a framework for small and medium-sized enterprises based on a three-step methodology (analysis, design and implementation) and tested it empirically against three case studies.

In [41], the authors proposed a framework to test the compliance of Big Data systems, proposing a guideline for GDPR verification and implementation in Big Data systems. They translated GDPR requirements to IT Security requirements.

Furthermore, authors of [37] presented a proof-of-concept to detect infringements of privacy norms or to prevent possible violations using BPMN in the GDPR domain.

Finally, in [40], the authors describe a technique to automatically evaluate the compliance of the security policies of a system against formal rules derived from legal provisions.

The results described in [2,3] and [1], by the same research team, focus on the idea of Privacy Level Agreements (PLAs), proposed by the Cloud Security Alliance [8]. The authors propose a PLA metamodel in [2], relating together the concepts of privacy and security, trying to understand how to address GDPR rules with their model, in order to express both users needs and providers capabilities. In [1] the focus is moved to the risk analysis, to help users to identify their own requirements with respect to PLAs, whereas in [3] they try to assess the impact of the taken choices, identifying at the same time the standard security controls proposed by CCM (Cloud Control Matrix) [11].

It is worth noticing that the approach proposed by those authors differs from the vision we explore within this work: we focus on legal compliance, i.e. we try to help providers demonstrate compliance to GDPR, instead the above-cited papers focus more on the user's requirements and their match with the providers' offerings. The proposed PLA metamodel is a complementary effort with respect to our GDPR conceptual map [7]. Their risk and impact assessment could be in future compared with our approach based on NIST security controls (a map among NIST and CSA controls is available).

In the paper by Granata et al. [25], the authors detail an innovative approach that utilizes business processes, specifically Business Process Model and Notation (BPMN), to assess security and privacy. A goal of this approach is to automatically generate the GDPR treatment register, documenting data processing activities as mandated by GDPR.

In conclusion, there are many different approaches to assessing privacy compliance of software frameworks, due to new regulations and the new challenges given by the growth of ICT services, especially these days, in which many researchers are developing programs and apps devoted to the fight against Covid-19 pandemic, and in these tools, there are several critical aspects related to privacy. Therefore, it is of paramount importance to develop methodologies and tools that help researchers and companies to respect privacy constraints.

3. Compliance verification through standard security control

Verifying GDPR compliance can be quite a convoluted task and raises several issues, particularly for SMEs. To illustrate, consider Article 25, which requires that data processing comply with the principles set in Article 5 and requires the implementation of the privacy-by-design and privacy-by-default principles [10]. The GDPR outlines the limitations but does not offer any particular method to put them into practice. Instead, it gives the Data Controller the authority (and the responsibility) to choose the technical answers. In any case, the GDPR assumes that there is no way to absolutely guarantee that there won't ever be a security breach and requires the data controller to take all reasonable precautions.

More specifically, Article 32 lists the requirements for processing security, while Article 33 cites the actions to be taken in the event of a data breach. The trade-off is that the Data Controller must prove they took all necessary steps to ensure the behavior was correct. To the best of the authors' knowledge, there are no practical solutions in the state of the art, as stated in Section 2.

The approach we propose is based on the definition of a systematic *security assessment process* that can be clearly documented and whose compliance with the GDPR can be demonstrated. In order to be applicable, even by SMEs, the technique was built to require a limited effort by security experts, automating as much as possible the process activities. The solution proposed relies on the following concepts:

- A **Security Policy** should outline the technical and organizational steps required to verify the compliance to GDPR of system operations.
- The policy previously defined must be articulated using **standard security controls**, which are not tied to specific systems or technologies.
- It is crucial to document the selection of security controls and establish a direct connection to GDPR regulations. This dual purpose serves as the foundation for security assessments and provides a transparent display of compliance with the regulations.

As a reference standard, the NIST security control framework [31] has been chosen, which is further detailed in the subsequent subsection.

Subsequently, a comprehensive analysis of the control framework has been conducted, meticulously mapping security controls to GDPR articles. The outcome of this phase is a NIST to GDPR article *mapping table*, which can be found in the Appendix, Table 7.

After all, has been implemented a simple procedure to identify the required security controls for each component of the infrastructure in order to document and evaluate the security policy for that infrastructure. As a result of this procedure, each component gets its own unique set of security restrictions.

3.1. NIST security controls

As previously mentioned, we used revision 5 of the NIST control framework, issued in September 2020, in order to employ well-known, acknowledged, and repeatable security countermeasures.

Several alternative frameworks are available in the literature, such as:

- ISO/IEC 27002 specification [17];
- CIS (Center for Internet Security) security controls;
- Cloud Security Alliance's (CSA) Cloud Control Matrix.

Appendix I in the NIST SP-800-53 book explains how the suggested controls connect with global standards. CIS and CSA offer different ways to link their controls with the NIST Framework. We used the NIST framework because it's easy to find and made it our main reference for our work.

A system security policy can be represented through the concept of "capabilities," which are further articulated in the context of a standardized set of "security controls." NIST provides a comprehensive list of security controls that encompass a wide array of security domains, spanning both technical and organizational aspects. As an illustration, the NIST Security Control Framework (currently integrated into our process) encompasses over 900 controls distributed across 20 distinct "control families." These control families include access control (AC), identification and authentication (IA), physical and environmental protection (PE), and awareness and training (AT).

These security controls are systematically categorized into families, each of which is named in a manner that intuitively identifies the specific capabilities addressed by the controls. Additionally, each family is associated with a distinct acronym for easy identification.

The NIST framework uses structured language to describe security controls. Each control has a name and an identifier (e.g., AC-1). The first control in a family is an organizational directive and offers a general overview. Control descriptions specify implementation steps and "supplemental guides" for human operators. Related controls impact or support implementation. Control Enhancements strengthen base controls, identified by an incremental value (e.g., AC-2(1)).

An example can be: the security control **PT-2**, named **AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION** has the following description:[3]

- *Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and*
- *b. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.*

An example of enhancement is **PT-2 (1)** DATA TAGGING, that imposes to **Attach data tags containing [Assignment: organization-defined permissible processing] to [Assignment: organization-defined elements of personally identifiable information]**. To keep it concise, we have not included the complete control and control enhancement descriptions (after the brief description offered above, there is always a *Discussion* that helps in interpreting the control description), we invite the interested reader to refer to the NIST document for further details.

3.2. Relation between security controls and GDPR

The NIST Security Control Framework comprises close to a thousand security controls, including enhancements. Consequently, the process of choosing controls (tailoring) can be quite challenging. NIST recommends using their risk-based approach and provides a baseline that specifies the risk level at which each control should be taken into account.

For what regards privacy, the NIST framework adopts, as a reference, the U.S. laws that differ from the European regulations. In order to facilitate the tailoring process and identification of controls related to privacy, a draft version of the security control framework revision 5, contained a dedicated table that outlines:

[3]The text reported is directly extracted from NIST document.

- whether a security control is privacy-related and
- whether the security control is executed by a system through technical or organizational methods.

It's important to highlight that we are striving to utilize the control framework innovatively, introducing a novel approach to security control tailoring with a strong emphasis on EU legislation. Consequently, we conducted a comprehensive analysis of all the frameworks, scrutinizing their compatibility with EU regulations. A detailed analysis of the framework is an error-prone activity, so we built a list of security controls relevant to GDPR. We built such a list following the procedure here described:

(1) Commencing with an analysis of the GDPR, we assigned a label to each GDPR article, indicating whether it pertains to Technical (T) or Organizational (O) means.
(2) We then selected all privacy-related controls and individually examined their alignment with corresponding GDPR articles of the same type. When a control was deemed capable of ensuring compliance with a GDPR article, we:
    - Described how the security control facilitates compliance with the GDPR article.
    - Outlined the limitations of such compliance, specifying what the control, in its current state, cannot guarantee with respect to GDPR requirements.
    - Indicated whether the control pertains to System, Data, or Organizational means.
    - Listed the necessary security control enhancements to ensure compliance with the regulation.
(3) Once the privacy-related controls (along with their enhancements) had been analyzed, we restarted the process for all security controls listed in the "related controls" of the selected controls. For each of them:
    - If we considered the security control relevant for GDPR compliance, we applied the process outlined in step 2.
    - If we regarded the security control as an alternative or useful improvement, we included the control's ID in the description of the control that recommended it.
    - If we deemed the security control irrelevant for GDPR compliance, we simply disregarded it.
(4) We analyzed all security controls that had not yet been examined and, if necessary, applied the process detailed in step 2, subsequently analyzing the related controls.
(5) We conducted a final review of the entire framework, which was performed twice by two different experts.

It's important to note that, although we eventually examined the entire framework, the process we employed assisted us in enhancing the consistency of our analysis and reducing the potential for errors. Table 1 describes briefly each field of the final mapping table, in order to help the reader correctly interpret the result.

To showcase the outcome of our mapping process and provide a reference for understanding it, we will briefly explain the process using the examples of GDPR articles 7 (concerning consent) and 33 (involving notification).

Table 1
NIST-GDPR mapping table fields

Field	Values	Description
Art.	Number	Article number
Title	Text	Title of the article
Type	T, O	Technical (T) or organizational (O)
Notes	Text	Additional notes
Control	NIST ID	NIST security control identification (family-number)
Motivation	Text	Explanation of how the security control addresses the article prescription
Limits	Text	Description of article provisions that the security control does not cover
Target	D, S, O	Data (D), system (S), or organization (O) target
En.	NIST ID	ID of security control enhancement needed (family-number-number)
Related	NIST ID	Identifiers of related NIST security controls necessary to address the article prescription (family-number)

Table 2
The section of NIST-GDPR mapping table related to art. 7 and 33

Art.	Title	Type	Notes	Ctrl	Motivation	Limits	T	En.	Rel.
7	Conditions for consent	T	Consent from the data subject to personal data processing	PT-4	Consent		D	PT-4(1) PT-4(2) PT-4(3)	PT-5
				AC-1			D		
				AC-3			D	AC-3(8) AC-3(14)	
				PM-20			D		
				PT-5			D	PT-5(2)	
				PT-6			D		
				AC-21	Ensures that information sharing is authorized respecting the purpose		D		
				AC-3	Allows consent revocation		S	AC-3(8)	
				PM-26	Complaint Management		O		
				PT-2	Determines the authority that processes information		O		
33	Notification of a personal data breach to the supervisory authority	O		IR-6	Ensures that an incident reporting policy exists	Time constraints for notification are missing		IR-6(2)	

Given space limitations, we cannot provide a comprehensive description of every legal article and its corresponding mapping here. However, you can find the complete mapping in the appendix. A portion of the table is displayed in Table 2 for reference.

As detailed in [10], Article 7 pertains to the "Conditions for Consent," which we classify as a technical measure. This is because the consent needs to be gathered, stored within the system, and must encompass a distinct set of data. Consequently, we've identified ten standard security controls that govern the consent management process: PT-4, AC-1, AC-3, PM-20, PT-5, PT-6, AC-21, AC-3, and PM-26. They are listed in the fifth column of the table and briefly described in the sixth one. It is worth noticing that the first one (PT-4) relates to data (and it is about the conditions of the consent). In fact, it is classified as *Data Oriented Target(D)*. Moreover, this control has two enhancements that we suggest adopting (PT-4(1), PT-4(2) and PT-4(3)) and a related security control PT-5, that, in fact, we included in the list of supported controls. The AC-3 control is a system-related control, we suggest it due to the AC-3(14) and AC-3(8) enhancement. The first one regulates the individual access to the data, while the second one is specific for consent revocation (needed by GDPR). These two controls, together with AC-1, PM-20, PT-5, PT-6, provide a means to manage the *Consent from the data subject to personal data processing*. The last three security controls (PM-26, PT-2, and PT-5) pertain to the "Organization (O)," and as such, they don't directly impact our systems. Instead, they should be integrated through internal procedures adopted within the organization. As demonstrated, a comprehensive analysis of the table enables us to pinpoint the security controls that need implementation, thus facilitating an internal self-assessment aimed at ensuring and demonstrating GDPR compliance.

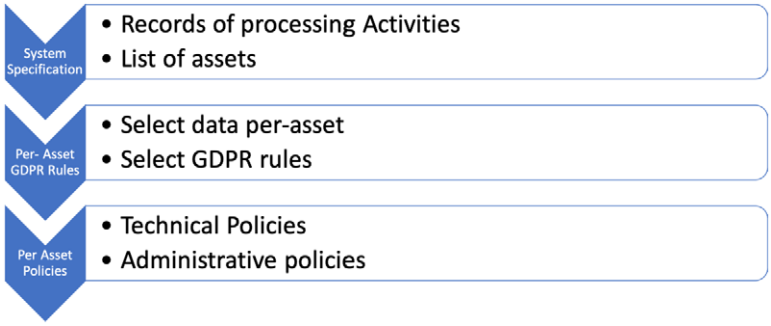

Fig. 1. GDPR compliance security assessment process.

It's important to note that not all law provisions can be entirely fulfilled by a single control. For instance, Article 33 mandates notifying the supervisory authority of a personal data breach within a strict time frame (2 weeks). However, while security control IR-6 (along with enhancement IR-6(2)) addresses the notification requirement, it lacks an enhancement or additional control that enforces the two-week deadline. In such cases, we indicate this limitation of the suggested control in column 7. The Data Protection Officer (DPO) should advise the Data Controller to implement an additional check to meet this requirement.

4. Automatic definition of compliant security and privacy policies

The GDPR Conceptual Map and the Security controls mapping table constitute the ground data model respectively

- represents law rules and;
- verify system and administrative compliance to the prescribed rules.

This section illustrates how to concretely apply these data models to (semi-) automatically define a security policy for an enterprise infrastructure, in order to enable a correct security assessment.

Following our approach, a DPO professional implements the steps described in Fig. 1 to support Data Controllers and Data Processors. We assume that the Controller has already built the Record of Processing Activities (as imposed by article 30).[4]

During the first step of the process, the DPO should identify the assets within the target enterprise and indicate the processing activities in which each asset is involved. Section 5 describes these activities for a university that has multiple sites distributed on a large territory, composed of a central management system and many peripheral systems that manage (some of) the data. At this stage of the process, we assume that the DPO (and/or Data Controller) has identified both the data to protect and the infrastructure in terms of involved assets. Next, the security policy adopted by the administration must be defined. Note that, SMEs almost never define formally such a policy and, as a consequence, they can hardly demonstrate compliance and/or assess the security level of their own infrastructure.

The second step of the methodology addresses this issue: starting from the assets, the Data Controller and the DPO identify the GDPR articles that each subsystem is specifically subject to, depending on the locally processed data. It is worth noticing that, whenever the system is made of a single centralized system, the first two steps simply collapse in describing the hosting system and listing all the articles applied to it.

[4]Note that we developed a tool that simply applies the steps described here and maintains the proposed table in a specific database, moreover it supports the definition of the record of activities.

The final step, which is the most critical one, defines the security policy each asset of the target system should implement. As a starting point, note that a security policy is made of both organizational and technical countermeasures. As outlined in the previous section, security controls are classified by NIST in categories and we reported them in our table. Moreover, since we are interested in data protection, in our analysis we outlined which controls affect data-specific aspects, in order to help us in the selection. As a final result, the security policy will be a list of standard controls that each asset should implement and that could be verified through dedicated audits. Moreover, thanks to the classification of the controls, we subdivided the resulting security policy into two different lists of countermeasures, the technical ones, which we use as prescriptions for the technical staff, and the organisational ones, used as rules and criteria to be respected from an administrative point of view.

The procedure described relies on:

- adoption of standard, accepted and verifiable security controls;
- the capability of selecting such security controls, according to GDPR rules.

5. A case study: The GDPR in a university context

This section describes a concrete case study by applying the proposed approach for the GDPR-compliance of a University infrastructure. In particular, we refer to the University of Campania Luigi Vanvitelli for this case study, and accordingly, we briefly introduce the specific GDPR issues within a University context, then it is presented the approach to address them following the proposed methodology.

It should be noticed that the recent implementation of the GDPR caused significant concerns within the research and academic communities [18,34,43]. In short, the concern arises from the possibility that new data protection regulations might impede innovative research within the EU, potentially hindering research freedom. Scientific institutions often handle highly sensitive data, such as genetic, biometric, and health information. To address this, GDPR has a general prohibition on processing sensitive personal data (Article 9), although exceptions exist for research and archiving in the public interest (Articles 9 and 89). These exceptions cover data processing principles, data subject rights, and potential national implementations of scientific exceptions by member states [21].

Research institutions have voiced worries about the potential for fragmentation due to Member States' exceptions. These exceptions could create unequal conditions for researchers and complicate research cooperation among Member States and globally. There are also questions about how the new data protection rules might affect international and global scientific research collaborations, especially concerning data sharing [21].

Moreover, GDPR article 89 states that processing for archiving purposes in the public interest, scientific research, historical or statistical purposes, shall be subject to appropriate safeguards to ensure data minimisation, i.e. data processing should only use as much personal data as is required to successfully accomplish a given task. The data minimisation principle may be achieved using the two different techniques named *anonymization* and *pseudonomization* as already seen in Section 2.

A recent study commissioned by the EU Parliament [21] on the comprehensive assessment of the expected impact of the GDPR on scientific research in Europe, pointed out many issues related to knowledge-based, technical, and regulatory aspects, and policy options are proposed. One of the issues is the lack of software tools to assess GDPR compliance that may assist universities and researchers.

5.1. GDPR-issues

Table 3, reworked from [21], reports the main issues of GDPR on research activity, as well as the policy options that must be implemented for compliance. Additionally, in the third column is reported the body responsible for the implementation of policy options (E = external body with respect to Universities, e.g. European/National Data Protection Authority; I = Internal university body, e.g. Ethics committees, Scientists).

Table 3
GDPR issues

+	Issue	Policy option	Resp.	Art.
Regulatory issues	Conflict between specific informed consent and broad consent in scientific research.	Reconcile GDPR's specific informed consent requirement with the need for broad consent in scientific research and align it with consent requirements in associated regulations.	E/I	7, 9, 89
	Broad interpretation of processing for statistical purposes under Article 89 (1) for non-scientific purposes.	Clarify exceptions under Article 89 (1) regarding processing for statistical and scientific purposes.	E	89
	Unclear best practices for anonymization and pseudonymization.	Establish data handling guidelines for anonymization and pseudonymization in different contexts.	E	6, 25, 32, 40, 89
	Unclear conditions for transnational data transfers outside the EU in transnational scientific projects.	Develop guidelines for researchers involved in transnational data transfers in collaborative scientific projects.	E/I	6, 7, 44-50
	Limited or inconsistent GDPR compliance guidelines by research institutions.	Create consistent GDPR compliance guidelines for researchers, focusing on areas between personal and non-personal data.	E/I	24, 40-43
	Conflict between data subject rights under GDPR and protection of database rights under the sui generis database regime.	Resolve the conflict between GDPR data subject rights and protection of database rights under the sui generis database regime.	E	12-20
	Lack of harmonization of national GDPR derogations.	Monitor derogations for research and create codes of conduct to address harmonization gaps.	E	49
Procedural issues	Ambiguous interpretation of data processing accuracy under Article 5(1)(d).	Develop consistent accuracy standards across scientific research domains related to data processing principles.	I	5
	Need for data management best practices.	Implement robust data management practices.	I	24, 32
	Absence of suitable data governance frameworks.	Develop adaptable data governance frameworks.	E	24
	Lack of anonymization and pseudonymization standardization.	Develop technical standards for anonymization and pseudonymization based on best practices.	I	32
	Lack of user-friendly GDPR compliance software tools for researchers.	Develop user-friendly GDPR compliance software, especially open access tools for data portability.	I	32
Transitional & capacity building	Transitional & capacity building	Organize educational activities and training sessions for data protection literacy among researchers, students, and scientific trainees.	I	24
	Uncertainty about administrative resources needed for GDPR compliance.	Support more research on impact assessment.	I	24, 35
	Scientific community's perceptions of potential GDPR compliance obstacles/burdens.	Monitor attitudes and develop tailored data protection literacy interventions.	I	24
	Limited media coverage of GDPR rights and obligations in research.	Raise public awareness of GDPR rights and obligations through awareness activities.	I	89

5.2. *System specification*

The University of Campania is distributed in five cities, between the provinces of Naples and Caserta, as shown in Fig. 2. The whole network is composed of dark optical fibers, placed between the cities and, in each city, organized in a 48-fiber ring (see Fig. 3). The main data centre is placed in Naples, and the workstations of University researchers and clerks are placed in different buildings (for a total of 15) in each city.

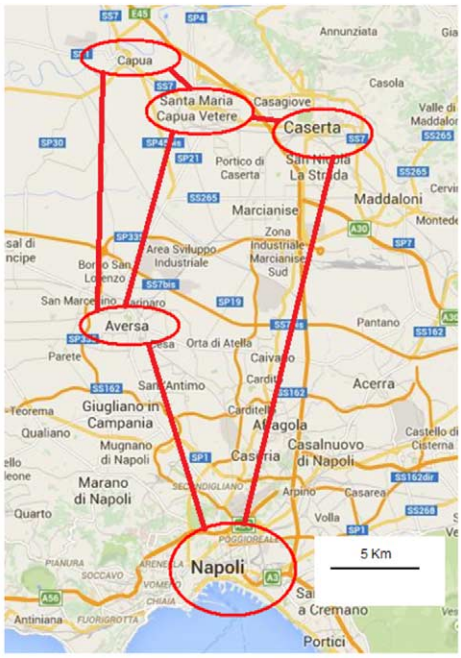

Fig. 2. The university network.

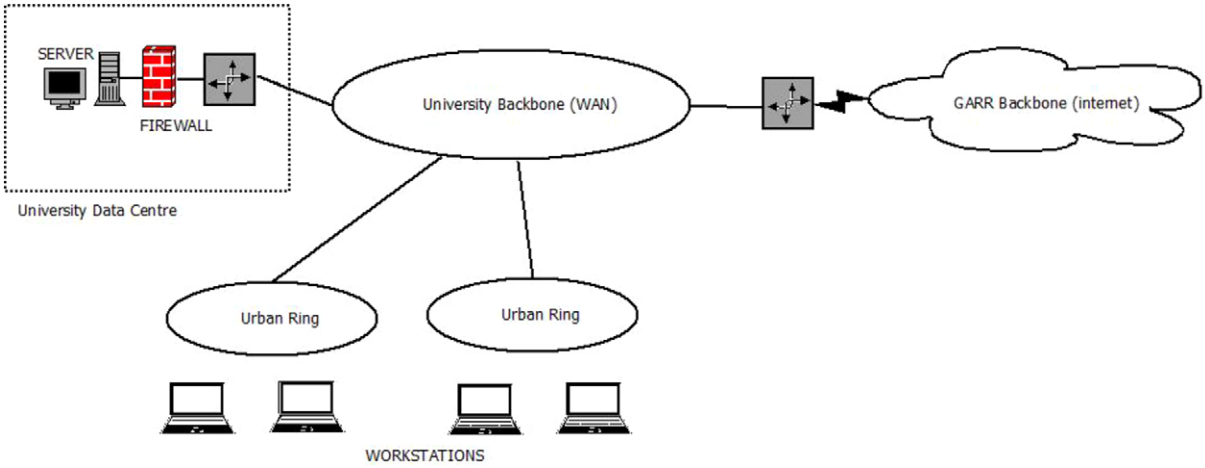

Fig. 3. The university network: topology and components.

As outlined above, the application of GDPR to Universities poses new challenges, which are multiplied in this case by the distributed nature of our departments: in order to manage the ICT infrastructure, in fact, we have multiple organization domains, each of them involved in the maintenance and processing of different data. According to the methodology we proposed, the *System Specification* is the first step needed to guarantee that data are maintained in accordance with GDPR regulation. This implies i) building up the records of processing activities and ii) identify and list all the involved assets in the university infrastructure. As already outlined, the records of processing activities for Italian universities can be built in accordance with [9] and it is the first duty executed by

Table 4
Record of processing activities – items related to students

Item	Purpose of processing
5.2.1	Study advisory service
5.2.2	Entrance exam
5.2.3	Student career (from first registration to degree)
5.2.4	Trainee-ship
5.2.5	Job placement
5.2.6	Fundraising, institutional communication
5.2.7	Statistics and teaching evaluation
5.2.8	Academic thesis publishing
5.2.9	Tutoring and social inclusion
5.2.10	Services for right of study
5.2.11	Disciplinary proceedings

our university DPO. In this work, to help readability, we restricted the analysis only to the processing activities for the students (chapter 5.2 of our Record of Processing Activities – RPA, [9] items 5.2.1 to 5.2.11). A summary of the main information contained in the RPA is shown in Table 4. As already outlined, in this analysis we focus only on such data and related processing activities.

In order to complete the first step we need to identify the core assets and to reduce the complexity of the problem and help the readability of the paper, we focused only on the technical assets in the ICT infrastructure. It should be considered that researchers, clerks and students may access most of the services from outside the university network. All the student services are served by a software framework, called *esse3*, produced by CINECA, a Consortium that builds and maintains software for the universities. The framework itself guarantees that:

- students may operate only on their own data
- professors may operate only on their own exam data
- clerks may operate on all data, depending on authorization given

According to such considerations, we briefly summarize our University ICT infrastructure in Fig. 3 which is a very simplified network scheme, the original one involves 22 different routers and a structured network for each different site. The sites are connected through a WAN fibre backbone and upstream to the Internet through the GARR[5] national research network. However, the simplified scheme helps to easily identify that four kinds of components are involved in order to ensure security and GDPR compliance:

- The **Server** farm in which framework esse3 is running, and the framework itself
- The **Firewall** in university data centre
- The university **Network**
- The **Workstations** of clerks and professors

5.3. Per-asset GDPR analysis

The second step of our methodology imposes to list, for each identified asset, the data that the asset processes and the GDPR rules that apply. For what concerns the data selection, our analysis focuses on the students' data that in different ways, go through each of the listed assets. Instead, for regulation compliance, it should be noted that, although every component contributes to GDPR compliance, each component is responsible for different aspects regarding the assurance of compliance. First, all components must follow the rules stated in Article 5 (i.e. processing of personal data) and article 32 (i.e. security of processing), as in these articles state the basic principles and rules needed to ensure user rights and correct data processing. The Firewall, in addition to articles 5 and 32,

[5]Gruppo Armonizzazione Reti di Ricerca.

Table 5
Mapping GDPR articles to components

Component	GDPR articles involved
Server	5, 7, 15 to 20, 24, 25, 32
Firewall	5, 24, 32
Network	5, 24, 32
Workstations	5, 24, 32

is also responsible for ensuring respect to article 22 (automated individual decision-making, including profiling), because this component must guarantee that no arbitrary profiling may be done on the data subject. Finally, the Server (and the software framework too), in addition to articles 5, 32 and 22, is also responsible for respecting articles 15 to 20 (right of access, rectification, erasure, restriction and data portability) and also article 25 (Data protection by design and by default). In Table 5 we summarized the different GDPR articles involved for each technical asset.

As expected, the Server is responsible for most of the article compliance, but is also noticeable that the whole Network and all of the workstations must be verified and assessed for compliance.

5.4. Per-asset policies

The last step of the proposed process aims at identifying the security controls that should be implemented by each of the assets of our system. Algorithm 1 describes the technique adopted to select all the controls, using the tables described in the previous sections. From the Table 5, referred as `AssetTable` we retrieved the list of the GDPR articles that each specific asset is responsible. Consequently, in the procedure, for each asset, we retrieved from the table 7 in Appendix, named `GDPRTable` in the pseudo-code, the full list of security controls (column 5) needed for each of the GDPR article (column 1) of the asset. We complete the procedure, removing the non-technical controls (that will be used for the administrative policies) and adding all the security control enhancements and (technical) related controls.

Executing the procedure for each of the assets in our system, we produced the Table 6, which is the (technical) security policy that should be assessed for each of the assets. It is worth noticing that we obtained a concrete security policy, that can be assessed by the university technicians and, at the same time, exposed to a third party to demonstrate adherence to GDPR procedures.

6. Conclusions and future work

Demonstrating accountability to GDPR principles places a significant burden on enterprises, especially SMEs, in terms of time and cost. Furthermore, it calls for specific knowledge, including but not restricted to technological expertise in privacy and security.

This article focuses on the identification of appropriate countermeasures for demonstrating GDPR compliance within the context of GDPR implementation. This technical issue involves developing a security policy that not only ensures regulatory compliance but is also feasibly assessable.

We proposed and demonstrated a concrete methodology that in a semi-automated way identifies security controls and demonstrates compliance with GDPR indicating, for each GDPR article, how it was addressed by the security controls.

Processes for certification and security evaluation usually use standard security measures. They offer enough technical details for technical staff to adequately verify their proper execution.

The mapping's effectiveness and the proposed approach were validated through its application in a real-world case study, specifically within our university infrastructure, where we successfully employed the technique.

This paper, starting from our previous work, a conceptual map of the GDPR and the relationships with the NIST standard security control framework introduced in [7], offers these concrete results:

Algorithm 1 Procedure to derive the technical security controls

```
1: procedure TECHNICAL SECURITY CONTROLS
2:     Initialize:
3:     AssetTable ← Table of the GDPR articles that applies for each Asset
4:     GDPRtable ← GDPR Mapping Table
5:     SCs[] ← Initial empty list of security controls for each asset
6:
7:     for each asset i in AssetTable do
8:         articles ← AssetTable(i)
9:         for each article i in column 1 of GDPRtable do
10:            tmpSCs ← Initial empty list of security controls
11:            tmpSCs ← all controls in column 5 of GDPRtable(i)
12:            for each sc i in tmpSCs do
13:                if sc is not technical then
14:                    Remove from tmpSCs
15:                end if
16:                for each enhance i in GDPRtable(i) do
17:                    add enhancement in tmpSCs
18:                end for
19:                for each related SC i in GDPRtable(i) for sc do
20:                    if sc is technical then
21:                        add related SC to tmpSCs
22:                    end if
23:                end for
24:            end for
25:        end for
26:        add all tmpSCs elements in SCs
27:    end for
28: end procedure
```

- a technique, with an algorithm and a tool to select and identify, in an almost automated way, security countermeasures needed to prove the compliance with GDPR;
- the actualization of mapping with the latest version of security control frameworks (namely NIST SP-800-53);
- the validation of the technique with a case study through a simple demonstrator.

This solution provides a valuable technical foundation for showcasing accountability and extends clear support to the Data Protection Officer (DPO), Data Controller, and Data Processor in verifying the proper implementation of security countermeasures.

One of the main limitations of this approach is the static mapping between the GDPR articles and the NIST SP-800-53 security controls. An update to the regulation or the release of new security controls would require the security expert to rework the mapping. A possible solution and further extension would be to leverage NLP (Natural Language Processing) techniques for dynamic construction. It would be interesting to develop an NLP technique in order to automatically map (or support the mapping) the GDPR articles and the NIST security controls.

A further extension would be to consider the organization controls included in the NIST SP-800-53 for accountability, as our methodology is currently focusing just on the technical controls.

Table 6
Tool results

Component	Family	Controls	GDPR articles
Server	AC	AC-1, AC-3, AC-3(8), AC-3(11), AC-3(14), AC-16, AC-17, AC-17(2), AC-21	7, 25, 32
	AU	AU-1, AU-3, AU-3(3)	5, 18, 25
	CA	CA-1, CA-2	25
	MP	MP-1, MP-5, MP-6	15, 17
	PL	PL-8, PL-8(1), PL-8(2), PL-9	25
	PM	PM-1, PM-7, PM-9, PM-11, PM-23, PM-26, PM-20	5, 24, 25, 32
	SA	SA-8, SA-17	25
	SI	SI-1, SI-12, SI-12(1), SI-12(1), SI-12(2), SI-18, SI-19, SI-19(1), SI-20, SI-20(4)	5, 16, 17, 25, 32
	PT	PT-1, PT-4, PT-5, PT-6, PT-2, PT-3	5, 24
	PS	PS-8	24
Firewall	AC	AC-1, AC-17, AC-17(2)	32
	AU	AU-1, AU-3, AU-3(3)	5
	PM	PM-1, PM-9, PM-22, PM-23, PM-26	5, 24, 32
	SI	SI-1, SI-12, SI-12(1), SI-12(2), SI-18, SI-19, SI-20, SI-20(4)	5, 32
	PT	PT-4, PT-2, PT-3	5, 24
	PS	PS-8	24
Network	AC	AC-1, AC-17, AC-17(2)	32
	AU	AU-1, AU-3, AU-3(3)	5
	PM	PM-1, PM-9, PM-23, PM-26, PM-22	5, 24, 32
	SI	SI-1, SI-12, SI-12(1), SI-12(2), SI-18, SI-19, SI-20, SI-20(4)	5, 32
	PT	PT-4, PT-2, PT-3	5, 24
	PS	PS-8	24
Workstation	AC	AC-1, AC-17, AC-17(2)	32
	AU	AU-1, AU-3, AU-3(3)	5
	PM	PM-1, PM-9, PM-22, PM-23, PM-26	5, 24, 32
	SI	SI-1, SI-12, SI-12(1), SI-12(2), SI-18, SI-19, SI-20, SI-20(4)	5, 32
	PT	PT-4, PT-2, PT-3	5, 24
	PS	PS-8	24

We aim to extend the methodology in the future to support threat modelling [23,24] and risk analysis processes [26]. This task can be done by improving the tool that implements and automates the methodologies and integrating existing risk analysis tools, in order to relate the proposed countermeasures directly to the DPIA (Data Protection Impact Analysis) prescribed by the GDPR.

7. Acknowledgement

This work was partially supported by Project SSCeGov, funded by the University of Campania Luigi Vanvitelli, under Program VALERE.

Conflict of interest

The authors have no conflict of interest to report.

Appendix. Security controls and GDPR articles mapping

Table 7
NIST-GDPR mapping table

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
4	Definitions	O		MP-1					
				SI-12				SI-12(1)	
5	Principles relating to processing of personal data	T	Lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability	PT-3	Indicates the purpose for which the information is processed	The storage limitation of personal data is not managed	D	PT-3 (1)	CM-13 SC-43 SI-18
				AT-1	Provides information for organizational privacy and security roles		O		
				AT-2			O	AT-2(1) AT-2(2)	AT-4
				AT-3			O	AT-3(3) AT-3(5)	
				PM-23	Manages information's quality		D		SI-20
				SI-12	Minimizes personal data usage		D	SI-12(2)	
				PM-22	Ensures that information is correct and updated		S		
				SI-18			S		
				PM-26	Take steps to limit or minimize personal information		D		
				SI-19	Guarantees information accuracy		D		
				AU-3	Manages the limitation of personal information		D	AU-3(3)	
	Lawfulness of processing	O	Prescribes that personal data must be processed *in a lawful, correct and transparent way towards the data subject*	AC-1	Consent is managed		D		SI-12
				AC-3			D	AC-3(14)	
				PM-20			D		
				PT-5			D	PT-5(12)	PT-3
				PT-6			D	PT-6(1)	PT-2
								PT-6(2)	PT-3
				PT-3	Indicates the purpose for which information is managed		D		SI-18
							S	PT-3(1)	SC-43 CM-13

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
	Conditions for consent	T	Consent from the data subject to personal data processing	AC-1	Consent		D	PT-4(1) PT-4(2) PT-4(3)	PT-5
				AC-3			D	AC-3(14)	
				PM-20			D		
				PT-5			D		
				PT-6			D		
				AC-21	Ensures that information sharing is authorized respecting the purpose		D		
				AC-3	Allows consent revocation		S	AC-3(8)	
				PM-26	Complaint Management		O		
				PT-2	Determines the authority that processes information		O		
	Transparent information, communication and modalities for the exercise of the rights of the data subject	O		PM-9	Privacy Authorization procedures exist		O		CA-7 CM-1 PM-12 PS-6
				PS-8			O		
				SI-12			O		
				PT-3			O	PT-3(1) PT-3(2)	
	Information to be provided where personal data are collected from the data subject	O		PT-3	Specifies the context	Management of personal and contact data of security officials; Management of the data retention period;	O		
				RA-2	Defines a categorization of the information that is processed				
	Information to be provided where personal data have not been obtained from the data subject	O		PT-3	Specifies the context	Management of personal and contact data of security officials	O	PT-3(1) PT-3(2)	
				RA-2	Defines a categorization of the information that is processed		O		

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
				AC-1	Right of access by the data subject	Criterion for determining the data retention period	O		SI-12
				MP-5			D		
				PT-3			D		
				PM-25			O		
				PM-22			S		
				SI-18			S		
				AC-3			S	AC-3(14)	
				RA-2			O		
				PM-21			O		
				PM-22	Right to rectification		S		
				SI-18			D		
				SI-19			D	SI-19(1)	
				SI-18	Right to erasure		D		MP-6
				AU-3	Right to restriction		D	AU-3(3)	
				PT-3			D	SC-43	
15	Right of access by the data subject	O	Obtaining access to personal data by the data subject	AC-1	Defines data access procedures		O		SI-12
				MP-5	Manages data transfer	Criterion for determining the data storage period	D		
				PT-3	Specifies the purpose		D	PT-3(1)	CM-13 SC-43 SI-18
				PM-27	Manages how individuals can access information		O		
				PM-22	Ensures that information is updated		S		
				SI-18			S		
				AC-3	Manages the right to access personal information		S	AC-3(14)	
				RA-2	Manages the categorization of information		O		
				PM-21	Indicates the mechanisms necessary to access information for authorized users		O		
16	Right to rectification	O	The data subject can correct his data	PM-22	Manages a process to keep information up to date		S		
				SI-18			S		

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
				SI-19	About techniques for correcting inaccurate information		D	SI-19(1)	
17	Right to erasure (*right to be forgotten*)	O	Possibility of deletion of personal data by the data subject	SI-18	Deals about techniques for deleting information		D		
18	Right to restriction of processing	O	Restriction of processing of the data subject	AU-3	Manages the restriction		D	AU-3(3)	
				PT-3	Restricts processing only to authorized purposes		D	PT-3(1)	CM-13 SC-43 SI-18
19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	O	Communication of rectification or erasure of personal data carried out	SI-18	Notifies that the information has been corrected	Management of notification of the cancellation and correction of data	S	SI-18(5)	
20	Right to data portability	O		SC-27		Right to data portability is missing	O		
21	Right to object	O		PT-3	Identifying and documenting the purpose for processing	A specific control to allow the data subject to assert their rights is missing	O S		
22	Automated individual decision-making, including profiling	O		PT-3	Automated mechanisms augment tracking of the processing purposes		S	PT-3(2)	
23	Restrictions	O		PT-3			O	AC-2 AC-3 CM-13	

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
24	Responsibility of the controller	O	Obligations of the controller	PM-26	Ensures that information about the processing is clear and understandable		O		
				PM-3	About a risk management strategy		O		CA-2 PM-32 RA-3 SI-12
				RA-8	Conducts a privacy impact assessment		O		RA-3
				CM-4	About a risk management strategy after changes		O		SA-5
25	Data protection by design and by default	T	Privacy by design and privacy by default	PL-8	About the development of security and privacy oriented architectures		S	PL-8(1) PL-8(2)	PL-9 PM-7 SA-8
				AC-3	Grants limited access to certain types of data		S	AC-3(11)	
				AC-1	Manages the consent to protect the natural person		D		
				AC-3			D	AC-3(14)	
				PM-20			D	PM-20(1)	
				PT-5			D		
				PT-6			D	PT-6(1)	PT-2
							D	PT-6(2)	PT-3
				PT-3	Takes into account the processing purpose		D		
				AC-3	About the user's access to their personal data		S	AC-3(14)	
				MP-2	Access restriction for certain types of data to certain types of roles		O		AU-9 SC-13

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
				PM-7	About the development of architectures considering security, privacy and risk		S		PM-11 SA-8 SA-17
				PM-9	About carrying out a risk strategy		O		CA-2 PM-32 RA-3
				PM-26	Minimization		D		
				PM-27	Protects the data subject's right of access to data		O		
				SI-12	About the management of information within the system		D	SI-12(1) SI-12(2)	AC-16 CA-2 PT-2 PM-9
				AU-3	Restricts information		S	AU-3(3)	
				PT-3	Restricts usage to authorized purposes only		D	PT-3(1)	CM-13 SC-43 SI-18
				AC-21	Manages the sharing of information protecting the rights of the data subject		D		AC-16
				PM-22	Ensures that the information is up to date		S		
				SI-18			D		
				SI-19	About techniques for correcting inaccurate information		D	SI-19(1)	
				PM-21	Indicates the procedures needed to access information by authorized users		O		

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
28	Processor	O	Data Processor	PL-9	About the management of controls and related processes		O		
				PM-2	Establishes the security officer and the related missions				
				PM-19	Concerns the roles involved in the security and privacy program		O		
				SI-20	Security measures pursuant to Article 32		D	SI-20(4)	
				SI-1			D/S		PM-9
				SI-6			O		SI-4
				IR-4			O		CP-2
									IR-8
				CA-7			O	CA-7(4)	CM-4
									PM-9
				PM-6			O		
				PM-14			O		SI-4
				PM-32			O		
				AT-2			O		
				AT-3			O		
				RA-3			O		PM-9
				RA-8			O		
				AC-17				AC-17(2)	
				PT-3					
				CP-10					CP-9
									IR-4
30	Records of processing activities	O	Proof of proper treatment management	PM-24	Determines a data management structure	Management of personal and contact information of the processor and, and, where applicable, the joint controller	D		PM-23 SI-20
				PM-25	Sets a data integrity sheet		D		AC-21
				PT-3	Specifies the purposes		D		PM-9
				RA-2	Defines a categorization of the information that is processed				PL-2

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
				SI-20	Security measures pursuant to article 32		D	SI-20(4)	
				SI-1			S		PM-9
				SI-6			O		
				CA-7			O		
				PM-6			O		
				PM-14			O		
				PM-32			O		
				AT-2			O		
				AT-3			O		
				RA-3			O		PM-9
				RA-8			O		
				AC-17				AC-17(2)	
				PT-3					
				CP-10					CP-9
									IR-4
				PM-18	Provides an overview of the structure of the privacy program		O		PM-9
									PM-19
				PM-29	Provides an inventory of the information		O		
32	Security of processing	T	Security of personal data	SI-20	Ensures the protection of information through encryption		D	SI-20(4)	
				SI-1	Sets procedures to guarantee the integrity of the system and information		D/S		PM-9
				SI-6	Sets the correctness of the security functions		O		SI-4
				IR-4	About incident management		O		CP-2
									IR-8
				CA-7	About management		O	CA-7(4)	CM-4
									PM-9
				PM-6	Manages the effectiveness of security measures		O		
				PM-14	Manages a testing procedure		O		SI-4

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
				PM-32	Takes into account the risk		O		
				AT-2	Guarantees education and training		O		
				AT-3			O		
				RA-3	Risk assessment		O		PM-9
				RA-8	Risk impact assessment		O		
				AC-17	Implements encryption mechanisms		S	AC-17(2)	
				PT-3	Specifies the purpose		D	PT-3(1)	CM-13 SC-43 SI-18
				CP-10	Manages system recovery after a failure		O		CP-9 IR-4
33	Notification of a personal data breach to the supervisory authority	O		IR-6	TBC	Time constraints for notification are missing		IR-6(2)	
34	Communication of a personal data breach to the data subject	O		IR-7	TBC				
35	Data protection impact assessment	T	Obligation of an analysis of processing risk and related planning of countermeasures	RA-3	Carries out a risk assessment		O		RA-7
				CA-2	About a security and privacy assessment		O		CA-7
				PT-3	Takes into account the context		D		RA-3
				RA-8	Carries out an impact assessment for privacy		O		RA-7
				PM-9	Develops a risk management strategy		O		CA-7
				PM-32	Deals about risk assessment		O		CA-7 RA-7
				IR-1					
				IR-8					
				IR-9					

Table 7
(Continued)

Art.	Title	Type	Notes	Control	Motivation	Limits	T	En.	Rel.
36	Prior consultation	O				Prior consultation is missing			
37	Designation of the data protection officer	O	Technical figure representing an expert consultant	PL-9	It refers to the management and implementation at company level of selected security and privacy controls and related processes		O		
38	Position of the data protection officer			PM-2	Decides the security officer and related missions				
				PM-19	About the roles involved in the security and privacy program		O		
39	Tasks of the data protection officer	O	DPO obligations	RA-3	Carries out a risk assesment		O		RA-7
				CA-2	About an assessment of security and privacy		O		CA-7
				PT-3	It takes into account the context		D		
				RA-8	Carries out an impact assessment for privacy		O		RA-7
				PM-9	Develops a risk management strategy		O		CA-7
				PM-32	About a risk analysis		O		CA-7 RA-7

References

[1] A.S. Ahmadian, F. Coerschulte and J. Jürjens, Supporting the security certification and privacy level agreements in the context of clouds, in: *Conference of 5th International Symposium on Business Modeling and Software Design, BMSD 2015*, 6 July 2015 Through 8 July 2015, 2016, pp. 80–95. Conference Code: 176459. ISBN 978-3-319-40512-4. doi:10.1007/978-3-319-40512-4_5.

[2] A.S. Ahmadian and J. Jurjens, Supporting model-based privacy analysis by exploiting privacy level agreements, in: *Conference of 8th IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2016*, 12 December 2016 Through 15 December 2016, IEEE Computer Society, 2016, pp. 360–365. Conference Code: 126112. ISSN 23302194. ISBN 9781509014453.

[3] A.S. Ahmadian, D. Strüber, V. Riediger and J. Jürjens, Supporting privacy impact assessment by model-based privacy analysis, in: *Proceedings of the 33rd Annual ACM Symposium on Applied Computing, SAC '18*, Association for Computing Machinery, New York, NY, USA, 2018, pp. 1467–1474. ISBN 9781450351911. doi:10.1145/3167132.3167288.

[4] M. Barati and O. Rana, Tracking GDPR compliance in cloud-based service delivery, *IEEE Transactions on Services Computing* (2020), 1–1. doi:10.1109/TSC.2020.2999559.

[5] M. Barati, O. Rana, I. Petri and G. Theodorakopoulos, GDPR compliance verification in Internet of things, *IEEE Access* **8** (2020), 119697–119709. doi:10.1109/ACCESS.2020.3005509.

[6] M. Brodin, A framework for GDPR compliance for Small- and Medium-Sized Enterprises, *European Journal for Security Research* **4** (2019), 243–264. doi:10.1007/s41125-019-00042-z.

[7] P. Cantiello, M. Mastroianni and M. Rak, A conceptual model for the general data protection regulation, in: *Computational Science and Its Applications – ICCSA 2021*, Lecture Notes in Computer Science, Vol. 8285, Springer International Publishing, Cham, 2021, pp. 60–77. ISBN 978-3-030-87010-2. doi:10.1007/978-3-030-87010-2_5.

[8] Cloud Security Alliance (CSA), Privacy level agreement outline for the sale of cloud services in the European Union, 2013, 21, https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf.

[9] CODAU Working Group on privacy, Linee guida in materia di privacy e protezione dei dati personali in ambito universitario, 2017, 110.

[10] Council of European Union, General data protection regulation, European Commission, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[11] CSA, CCM v4.0 auditing guidelines, cloud security alliance, 2021, https://cloudsecurityalliance.org/artifacts/ccm-v4-0-auditing-guidelines/.

[12] Data Protection Commission, Ireland, Guidance note: Guidance on anonymisation and pseudonymisation, 2019, 17.

[13] M. D'Errico and S. Pearson, Towards a formalised representation for the technical enforcement of privacy level agreements, in: *2015 IEEE International Conference on Cloud Engineering*, 2015, pp. 422–427. doi:10.1109/IC2E.2015.72.

[14] B. Di Martino, M. Mastroianni, M. Campaiola, G. Morelli and E. Sparaco, Semantic techniques for validation of GDPR compliance of business processes, in: *Conference of 13th International Conference on Complex, Intelligent, and Software Intensive Systems, CISIS 2019*, 3 July 2019 Through 5 July 2019, Advances in Intelligent Systems and Computing, Vol. 993, 2020, pp. 847–855. Conference Code: 227709, ISBN 9783030223533. doi:10.1007/978-3-030-22354-0_78.

[15] V. Diamantopoulou, A. Androutsopoulou, S. Gritzalis and Y. Charalabidis, An assessment of privacy preservation in crowdsourcing approaches: Towards GDPR compliance, *IEEE Computer Society* (2018), 1–9, ISSN 21511349. ISBN 9781538665176.

[16] V. Diamantopoulou, M. Pavlidis and H. Mouratidis, Privacy level agreements for public administration information systems, 8.

[17] V. Diamantopoulou, A. Tsohou and M. Karyda, From ISO/IEC 27002:2013 information security controls to personal data protection controls: Guidelines for GDPR compliance, in: *Computer Security*, S. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, C. Kalloniatis, J. Mylopoulos, A. Antón, S. Gritzalis, F. Pallas, J. Pohle, A. Sasse, W. Meng, S. Furnell and J. Garcia-Alfaro, eds, Springer International Publishing, Cham, 2020, pp. 238–257. ISBN 978-3-030-42048-2. doi:10.1007/978-3-030-42048-2_16.

[18] E.S. Dove, The EU general data protection regulation: Implications for international scientific research in the digital era, *The Journal of Law, Medicine & Ethics* **46**(4) (2018), 1013–1030. doi:10.1177/1073110518822003.

[19] L. Elluri and K.P. Joshi, A knowledge representation of cloud data controls for EU GDPR compliance, in: *2018 IEEE World Congress on Services (SERVICES)*, IEEE, San Francisco, CA, 2018, pp. 45–46, https://ieeexplore.ieee.org/document/8495788/. ISBN 978-1-5386-7374-4. doi:10.1109/SERVICES.2018.00036.

[20] L. Elluri, A. Nagar and K.P. Joshi, An integrated knowledge graph to automate GDPR and PCI DSS compliance, in: *2018 IEEE International Conference on Big Data (Big Data)*, IEEE, Seattle, WA, USA, 2018, pp. 1266–1271, https://ieeexplore.ieee.org/document/8622236/. ISBN 978-1-5386-5035-6. doi:10.1109/BigData.2018.8622236.

[21] European Parliamentary Research Service – Scientific Foresight Unit – (STOA), How the general data protection regulation changes the rules for scientific research, 2019, 104. doi:10.2861/17421.

[22] D. Granata and M. Rak, Design and development of a technique for the automation of the risk analysis process in IT security, in: *Proceedings of the 11th International Conference on Cloud Computing and Services Science – CLOSER*, SciTePress, 2021, pp. 87–98, INSTICC. ISBN 978-989-758-510-4. doi:10.5220/0010455200870098.

[23] D. Granata and M. Rak, Systematic analysis of automated threat modelling techniques: Comparison of open-source tools, *Software Quality Journal* (2023). doi:10.1007/s11219-023-09634-4.

[24] D. Granata, M. Rak and W. Mallouli, Automated generation of 5G fine-grained threat models: A systematic approach, *IEEE Access* **11** (2023), 129788–129804. doi:10.1109/ACCESS.2023.3333209.

[25] D. Granata, M. Rak and S. Petrillo, Automated threat modelling and risk analysis in e-government using BPMN, *Connection Science* **35**(1) (2023), 2284645. doi:10.1080/09540091.2023.2284645.

[26] D. Granata, M. Rak and G. Salzillo, Risk analysis automation process in IT security for cloud applications, in: *Cloud Computing and Services Science*, D. Ferguson, M. Helfert and C. Pahl, eds, Springer International Publishing, Cham, 2022, pp. 47–68. ISBN 978-3-031-21637-4. doi:10.1007/978-3-031-21637-4_3.

[27] D. Granata, M. Rak and G. Salzillo, MetaSEnD: A security enabled development life cycle meta-model, in: *Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22*, Association for Computing Machinery, New York, NY, USA, 2022. ISBN 9781450396707. doi:10.1145/3538969.3544463.

[28] R.E. Hamdani, M. Mustapha, D.R. Amariles, A. Troussel, S. Meeùs and K. Krasnashchok, A combined rule-based and machine learning approach for automated GDPR compliance checking, in: *Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law*, Association for Computing Machinery, New York, NY, USA, 2021, pp. 40–49. ISBN 9781450385268. doi:10.1145/3462757.3466081.

[29] International Organization for Standardization ISO, ISO27000 – Information technology, security techniques, information security management systems, overview and vocabulary, 2018, 104.

[30] International Organization for Standardization ISO, ISO27701 – security techniques – extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – requirements and guidelines, 2019, 104.

[31] Joint Task Force Interagency Working Group, Security and privacy controls for information systems and organizations, Technical report, National Institute of Standards and Technology, 2020. Edition: Revision 5. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. doi:10.6028/NIST.SP.800-53r5.

[32] A. Mahindrakar and K.P. Joshi, Automating GDPR compliance using policy integrated blockchain, in: *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 2020, pp. 86–93. doi:10.1109/BigDataSecurity-HPSC-IDS49724.2020.00026.

[33] M.M. Merlec, Y.K. Lee, S.-P. Hong and H.P. In, A smart contract-based dynamic consent management system for personal data usage under GDPR, *Sensors* **21**(23) (2021), https://www.mdpi.com/1424-8220/21/23/7994. doi:10.3390/s21237994.

[34] M. Mourby, E. Mackey, M. Elliot, H. Gowans, S.E. Wallace, J. Bell, H. Smith, S. Aidinlis and J. Kaye, Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK, *Computer Law & Security Review* **34**(2) (2018), 222–233, http://www.sciencedirect.com/science/article/pii/S0267364918300153. doi:10.1016/j.clsr.2018.01.002.

[35] NIST, Framework for improving critical infrastructure cybersecurity, National Institute of Standards and Technology, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[36] P.-G. Noé, A. Nautsch, N. Evans, J. Patino, J.-F. Bonastre, N. Tomashenko and D. Matrouf, Towards a unified assessment framework of speech pseudonymisation, *Computer Speech & Language* **72** (2022), 101299, https://www.sciencedirect.com/science/article/pii/S0885230821001005. doi:10.1016/j.csl.2021.101299.

[37] M. Palmirani and G. Governatori, Modelling legal knowledge for GDPR compliance checking, in: *JURIX*, Vol. 313, 2018, pp. 101–110.

[38] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini and L. Robaldo, PrOnto: Privacy ontology for legal reasoning, in: *Electronic Government and the Information Systems Perspective*, A. Kő and E. Francesconi, eds, Springer International Publishing, Cham, 2018, pp. 139–152. ISBN 978-3-319-98349-3.

[39] M. Rak, D. Granata, B. Di Martino and L. Colucci Cante, A semantic methodology for security controls verification in public administration business processes, in: *Complex, Intelligent and Software Intensive Systems*, L. Barolli, ed., Springer International Publishing, Cham, 2022, pp. 456–466. ISBN 978-3-031-08812-4. doi:10.1007/978-3-031-08812-4_44.

[40] S. Ranise and H. Siswantoro, Automated legal compliance checking by security policy analysis, in: *International Conference on Computer Safety, Reliability, and Security*, Springer, 2017, pp. 361–372. doi:10.1007/978-3-319-66284-8_30.

[41] M. Rhahla, S. Allegue and T. Abdellatif, Guidelines for GDPR compliance in big data systems, *Journal of Information Security and Applications* **61** (2021), 102896, https://www.sciencedirect.com/science/article/pii/S221421262100123X arXiv:2021.102896. doi:10.1016/j.jisa.2021.102896.

[42] E. Rios, E. Iturbe, X. Larrucea, M. Rak, W. Mallouli, J. Dominiak, V. Muntés, P. Matthews and L. Gonzalez, Service level agreement-based GDPR compliance and security assurance in (multi)cloud-based systems, *IET Software* **13**(3) (2019), 213–222. doi:10.1049/iet-sen.2018.5293.

[43] E.-B. van Veen, Observational health research in Europe: Understanding the general data protection regulation and underlying debate, *European Journal of Cancer* **104** (2018), 70–80, http://www.sciencedirect.com/science/article/pii/S0959804918314023. doi:10.1016/j.ejca.2018.09.032.