A Conceptual Model for the General Data Protection Regulation

Pasquale Cantiello[1(✉)], Michele Mastroianni[2], and Massimiliano Rak[2]

[1] Osservatorio Vesuviano, Istituto Nazionale di Geofisica e Vulcanologia, Napoli, Italy
pasquale.cantiello@ingv.it
[2] Dipartimento di Ingegneria, Università degli Studi della Campania, Aversa, Italy
{michele.mastroianni,massimiliano.rak}@unicampania.it
http://www.ingv.it, http://www.unicampania.it

Abstract. The widespread diffusion of Cloud paradigm and its approach based on delegation of resources to service providers, improved greatly the need of protecting personal data. Accordingly, in recent years, governments are going to define and apply new rules, that aims at protecting the personal space of each individual. From 2018, General Data protection Regulation (GDPR) applies in Europe, giving specific rights to each individual and imposing procedures to protect personal data. GDPR addresses a clear need of our social network-based society, but has the side effect of outlining the incapability of many actual enterprises, especially small and medium ones, to address such new requirements. In this paper the new Regulation is described with a conceptual map approach.

Keywords: GDPR · Privacy · Cloud

1 Introduction

In recent years, governments are going to define and apply new rules, that aims at protecting the personal space of each individual. In fact, from 2018, General Data protection Regulation (GDPR) [6] applies in Europe, it defines new rights for each European citizen, related to the control over their own personal data, as an example a citizen has the right to know who hosts his own personal data and ask for their deletion.

GDPR addresses a clear need of our *social network*-based society, but has the side effect of outlining the incapability of many actual enterprises, especially small and medium ones, to address such new requirements. As an example, GDPR imposes that service provider should perform a dedicated risk analysis (compiling a report named Data privacy Impact Assessment, DPIA) and select according the appropriate mechanisms. But the DPIA is not a simple analysis to carry out, and for proper evaluation of risks, is mandatory for data controllers to demonstrate that all security measures, both organisational and technical, are taken at state of the art level.

© Springer Nature Switzerland AG 2021
O. Gervasi et al. (Eds.): ICCSA 2021, LNCS 12956, pp. 60–77, 2021.
https://doi.org/10.1007/978-3-030-87010-2_5

The work proposed in this paper aims at addressing a very specific issue: the selection of countermeasures needed to demonstrate compliance to GDPR. We propose to address such an issue using standard security controls, in order to have a solution that can be transparently applied to different contexts. Accordingly, this paper proposes the following original and innovative results:

- A GDPR Conceptual map, that summarizes the main concepts of GDPR and will drive us in demonstrating compliances granted by security controls.
- A Mapping among standard security controls and GDPR concepts, in order to identify sets of security controls that grant compliances with GDPR requests.

The reminder of this paper is structured as follows. Section 2 describes the known issues related to GDPR adoption and to privacy management in general, outlining existing results. The following Sect. 3 describes the new Regulation and our innovative conceptual map over GDPR concepts, while Sect. 4 describes the relationship among the standard NIST security controls and GDPR articles. Section 5 summarizes our conclusions and a proposed set of future work.

2 Related Works

An interesting example that integrates semantic techniques for GDPR compliance was the approach proposed by [11,12]: they developed an integrated, semantically rich Knowledge Graph (or Ontology) to represent the rules mandated by both PCI DSS[1] and EU GDPR.

Another interesting research line is the one proposed in [7] which aims at semantically enrich BPMN (Business Process Model and Notation) with concepts related to GDPR, in order to support risk analysis and compliance verification.

An approach also based on ontologies may be found in [14]. In this paper is introduced PrOnto (Privacy Ontology for Legal Reasoning), which aims to provide a legal knowledge modelling of the privacy agents, data types, types of processing operations, rights and obligations, using a methodology used based on legal theory analysis joined with ontological patterns.

The results described in [1–3] (all produced by the same research team), focuses on the idea of Privacy Level Agreements (PLAs), proposed by CSA (Cloud Security alliance) [5]. The authors propose a PLA metamodel in [3], relating together the concepts of privacy, the security requirements and trying to understand how to address GDPR rules using such a metamodel to express both user needs and providers capabilities.

The idea of using standard security controls in order to address privacy requirements was explored by Rios et al. [15], trying to apply the concepts and results of the MUSA project, which suggests a development flow to address security requirements, involving Security Service Level Agreement all over the

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

development process. Such a research line differs from the approaches proposed in this paper because the compliance aspect is not the core of the technique, which, mainly, aims at relating Security SLAs and privacy.

The work in [10] proposes to use ISO27000 controls as a way to address GDPR compliance. The authors identify a set of controls in the ISO27000 framework and for each of them they suggest how to interpret/apply them in order to respect GDPR constraints. The approach proposed reminds our one, even if the procedure for the controls selection was not explained in detail (offering a limited grant about the completeness of the procedure), and there is no support for automating the process and its application when concretely applying the results in the process of GDPR compliance verification. The same team explored GDPR compliance in different contexts (public administration and crowdsourcing), even if experimenting different and less formal techniques in [9] and in [8].

3 A Conceptual Model for GDPR

The GDPR (General Data Protection Regulation), has been adopted on April 27 of 2016 by the European Parliament and the Council *to protect the natural persons with regard to the processing of personal data and on the free movement of such data* [6]. Its birth has been mainly driven by the necessity to harmonize the different regulations about the privacy in the countries of the EU, by focusing on the rights of the european citizens to protect and control their personal data. At the same time it allows the circulation of the data in the current digital society in a protected way. Since the GDPR has the form of a regulation, it is adopted and has effects on each country of the EU with no further actions required, neither it can be modified by a single country.

In this paper the new Regulation is described with a conceptual map approach. The global conceptual map is shown in Fig. 6. Eight core concepts of the GDPR have been outlined and shown in Fig. 1a. They are described here along with their relationships with further topics.

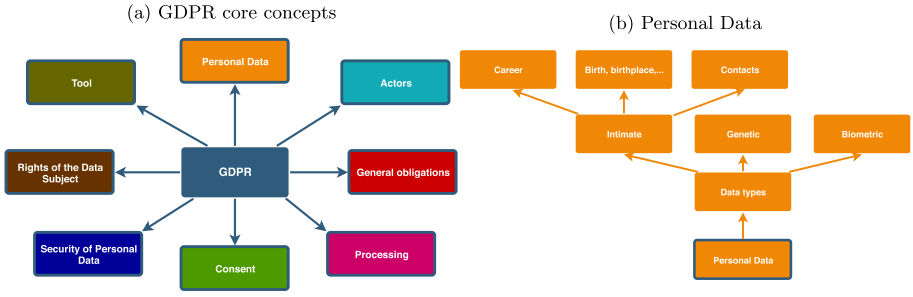

Fig. 1. GDPR core concepts and personal data

3.1 Personal Data

Personal Data, as defined in the article 4 of the Regulation, is any information relating to an identified or identifiable natural person *("Data subject")*. According to the Regulation, the identifiability of a natural person derives not only from common factors as names, identification numbers, locations or IP addresses, but also from factors specific to the *physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

A further classification of Personal Data, as shown in Fig. 1b, can lead to the following three sub-types:

- *Personal:* these are the data commonly known as personal, such as name, birth place and date, addresses, contacts (email, phone number), career and work experiences;
- *Genetic:* these are data relating to the characteristics (inherited or acquired genetic) of a natural person derived from the biological analysis (e.g.: DNA, RNA) which can give unique information about the physiology or the health of that natural person;
- *Biometric:* data resulting from specific technical processing (on physical, physiological or behavioural characteristics of a natural person), which can lead to the unique identification of that natural person;

3.2 Actors

Several actors are involved in the GDPR, each with his rights or obligations. In the conceptual model proposed here, as in Fig. 2a, we have identified the following:

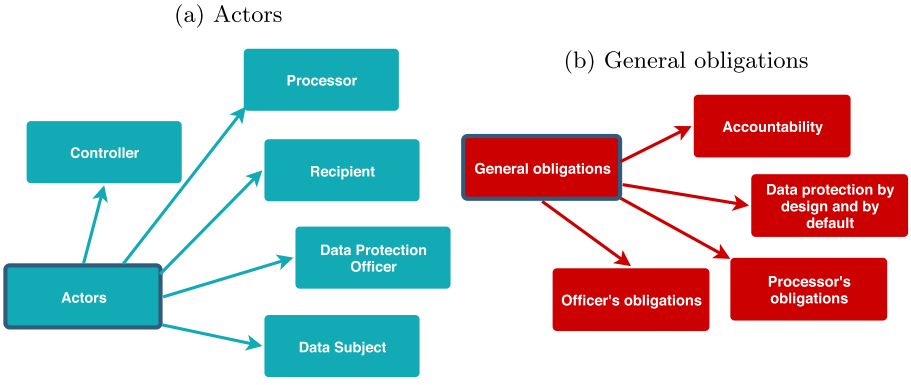

Fig. 2. Actors and General obligations

- *Controller:* A physical or legal person, a public authority, or any other service or organization that by itself, or in cooperation with others, defines the purposes and the methods of personal data processing.
- *Processor:* A physical or legal person, a public authority, or any other service or organization that processes personal data on behalf of a controller.
- *Recipient:* A physical or legal person, a public authority, or any other service or organization that receives communications with personal data.
- *Data Protection Officer (DPO):* A professional with specific knowledge about regulations and practice on personal data processing.
- *Data Subject:* A person to whom personal data is processed.

3.3 General Obligations

As described in Sect. 1 of Chapter IV of the GDPR, in order to guarantee the rights and freedoms of natural persons, several technical and organisational measures must be implemented, reviewed and updated where necessary. On our conceptual model, these obligations are classified, as shown in Fig. 2b, in the following four concepts:

- *Responsibility of the controller (Accountability):* As stated in the article 24 of the GDPR, the measures implemented by the controller serve to ensure (and to demonstrate) the compliance, according to the Regulation, of the processing on the data. Also any adherence to approved codes of conduct or to approved certification mechanisms, may be used to prove that compliance.
- *Data protection by design and by default:* The controller shall implement (article 25 of the Regulation) appropriate technical and organisational measures, since the planning stages of the data processing (*privacy by design*), to ensure data-protection principles and protect the rights of data subjects. These measures must be determined by taking into account the state of the art, their implementation costs, the nature and the related risks on the data processing. In the same way appropriate measures shall be implemented to ensure that, for each specific process, only personal data which are strictly necessary for the purpose are processed (*privacy by default*). This obligation applies also on the amount of data collected, the extent of processing and the time they are retained. Personal data must be not accessible to an indefinite number of natural persons.
- *Processor:* Where processing is made on behalf of a controller, only processors providing sufficient guarantees to meet the requirements of the GDPR should be chosen. As in the article 28, the controller must: i) process personal data on documented instruction from the controller and under a contract or legal act; ii) guarantee that persons authorised to process the data act with confidentiality or under an obligation of confidentiality; iii) take all security measures required.
- *Protection Officer:* The DPO has several obligations (Article 39) and in particular she/he must: i) inform and support the controller, the processor and the employees who process personal data about their obligations deriving from

the Regulation; ii) monitor compliance with the Regulation of the controller and the processor about protection of personal data; iii) provide advice, upon request, about DPIA (see Sect. 3.6) iv) have due regard to the risk associated with processing operations, considering the nature, scope, purposes and context of processing.

3.4 Processing

Personal Data Processing, as defined in the Article 4 of the Regulation generally means any operation or set of operations which is performed on personal data. In our model, shown in Fig. 3, we have identified two concepts: typology of personal data processing and principles applicable to them.

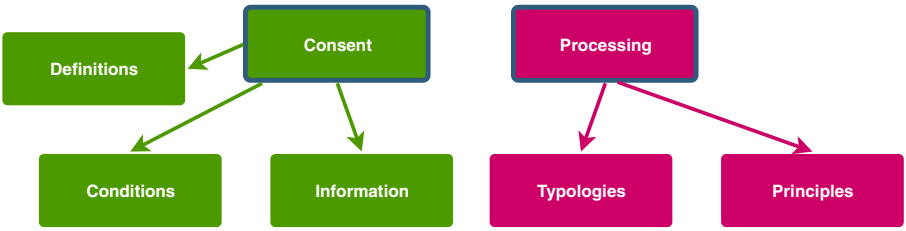

Fig. 3. Processing and consent

- *Typologies:* Several typologies of data processing operations are identified in the GDPR. In particular: i) *collection* is the starting point of the processing consisting in the acquisition of the data; ii) *recording* of the data on any kind of support for further processing; iii) *organisation* represents a classification of data in predefined way; iv) *structuring* consists in data distribution according to suitable schemas; v) *storage* of the data on any kind of support; vi) *adaptation* or *alteration* means any operation made on data to modify them in order to do a correlation with other data; vii) *retrieval* is the activity to find and retrieve any stored data; viii) *consultation* is the reading of the data, even in a simple form like visualisation; ix) *use* is a generic activity that involves any utilization of the data; x) *disclosure* is the transmission of data to different subjects; xi) *dissemination* regards the making available of the data as on public social networks; xii) *alignment* or *combination* of multiple data to get new structured information; xiii) *restriction* as partially hiding of entire classes or only parts of the personal data; xiv) *erasure* is data deletion using electronic tools; xv) *destruction* means the permanently deletion of that data.
- *Principles:* Every processing must be carried out in compliance with the principles of the Article 5 of the GDPR. These are: i) *lawfulness, fairness* and *transparency* of the processing in relation to the data subject; ii) *purpose*

limitation or that no further processing on the data is done other than the specified, explicit and legitimate purposes; iii) *data minimisation* is that the collected data must be adequate, relevant and limited to only what is strictly necessary to the specific purposes; iv) *accuracy* means the data must be accurate and kept up to date, and any personal data that are inaccurate are promptly erased or rectified; v) *storage limitation* of the data for no longer than what is necessary for the purposes of the processing; vi) *integrity* and *confidentiality* or that data must be processed to ensure appropriate security and protection against unauthorised processing and against accidental loss or modification by using appropriate technical or organisational measures; vii) *accountability* these principles must be followed by the controller, and he/she must be able to prove it (Article 24, par. 1).

3.5 Consent

Prior to data collection, the data subject must give his consent to processing. The consent can be defined as any *freely given*, *specific*, *informed* and *unambiguous* indication of the wishes of data subject by which he/she agrees to the processing of his/her personal data (Article 4). Consent can be given by a statement or by a clear affirmative action.

Conditions for consent (Article 7) require that: i) the controller shall be able to demonstrate that he has collected the consent of the data subject for the specific processing; ii) if the consent has been given in a written declaration with other matters, the request shall be presented in an easily accessible form, with clear and plain language; iii) the consent can be easily withdrawn by the data subject easily at any time and this shall stop any further processing on his/her data; iv) in order to assess if the consent is freely given, must be verified if the performance of a contract is conditional on consent to the processing of unnecessary personal data.

At the time when personal data are obtained from a data subject, and before performing any processing, the controller shall provide the data subject with all of the following information (Article 13): i) identity and contact details of the controller and possible representative; ii) contact details of the Data Protection Officer, where applicable; iii) the purposes and legal basis of the processing for which the personal data will be collected; iv) if the processing is related to the legitimate interests pursued by the controller or by a third party (Article 6(1)(f)); v) the recipients or categories of them that will receive personal data; vi) the reference to suitable safeguards if the collector means to transfer data in third part countries, along with the means by which the data subject can obtain a copy of them.

3.6 Security of Personal Data

In order to guarantee a level of security of the collected personal data (Article 32), the controller and the processor shall implement appropriate organisational and technical measures. These must be chosen taking into account: state of the

art, costs of implementation, nature, scope, context and purposes of processing, the risk related on the processing. In the conceptual model of this work, the related part is shown in Fig. 4.

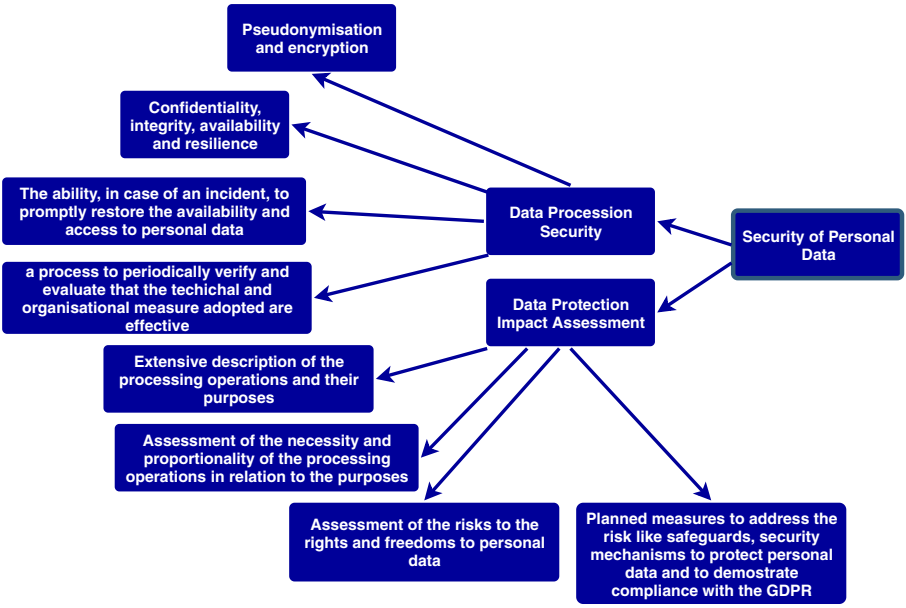

Fig. 4. Personal data security

We have done the following classification:

- *Data Processing Security:* the Article 32 of the Regulation identifies inter-alia the following measures: i) pseudonymisation and encryption of personal data, in order to delete or hide any reference to the data subject they belong; ii) the ability to ensure confidentiality, integrity, availability and resilience of all the systems and services involved in the personal data processing; iii) the ability, in case of an incident, to promptly restore the availability and access to personal data; iv) a process to periodically verify and evaluate that the technical and organisational measure adopted are effective.
- *Data Protection Impact Assessment:* Where a processing, especially when using new technology, may result in a high risk to the rights and freedoms of natural person, prior to that processing, an assessment of the impact of the processing on the protection of personal data must be carried out by the controller. This assesment is defined in Article 35 as *Data Protection Impact Assesment* (DPIA) and can be carried out on multiple similar processing operations that present similar risks. The decision to conduct a DPIA is leaved on risk evaluation by the controller, but is required in the case of

an evaluation of personal aspects relating to natural persons conducted systematically and extensively done by using exclusively automated processing, including profiling, and on which decision are based that can produce effects on or affect natural persons.
A DPIA must contain at last: i) an extensive description of the processing operations and their purposes, including the legitimate interest, if applicable, of the controller. ii) an assessment of the necessity and the proportionality of the processing operations in relation to the purposes; iii) an assessment of the risks to the rights and freedoms to personal data; iv) the planned measures to address the risks like safeguards, security mechanisms to protect personal data and to demonstrate compliance with the GDPR.

3.7 Rights of the Data Subject

The Regulation guarantees the Data Subject many rights regarding his/her personal data. In order to enforce his rights, he can directly contact the controller, even after given his consent and he must be able to revoke it.

In our model the classification, as shown in Fig. 5a, includes the following:

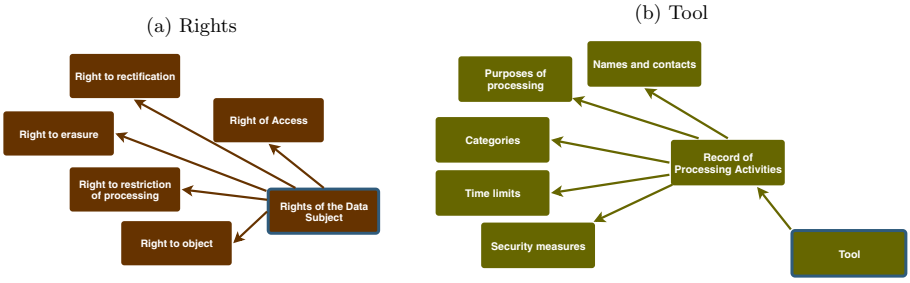

Fig. 5. Rights and tool

- *Right of access:* The Data Subject can ask the controller and has the right to obtain the confirmation about any personal data processing concerning him (Article 15 of GDPR). In that case, he has the right to access to the personal data, to know the purposes of the processing, to know the concerning categories of personal data and any recipients to whom this data will be disclosed. The Data Subjects can also have a copy of all his personal data processed.
- *Right to rectification:* The data subject has the right (Article 16) to obtain from the controller the rectification of any inaccurate personal data concerning him or her. The data subject has also to right to complete any personal data that is not complete regarding the purposes of the processing. The controller must comply without undue delay.

- *Right to erasure* or *right to be forgotten:* As guaranteed by the Article 17, the data subject can obtain by the controller that any data concerning him/her, that are no longer necessary for the reason they are collected and processed, must be erased. He/she can also obtain the erasure upon withdrawing of the consent, or if that data are unlawfully processed.
- *Right to restriction of processing:* The Article 18 guarantees the data subject that he/she can restrict the processing if, among the others: accuracy of personal data is contested by the data subject, or the process is unlawful and the subject opposes the erasure of the data, or the personal data are no longer necessary for the processing.
- *Right to object:* This right (Article 21 of GDPR), ensures that the data subject can object, at any time, to the processing of data concerning him or her, including profiling. This can be related to his or her particular situation. This right is different from the erasure one.

3.8 Tool

A fundamental tool required by the Regulation is the *Record of Processing Activities* described in the Article 30 of the GDPR. This is important to map all flows inside the organization, and is considered a best practice in data processing for the accountability of the controller. The record should be maintained by the controller and by any controller's representative, if present. The record is also useful for risk analysis and processing planning.

The representation is shown in Fig. 5b and the informations that should contained in the record, are:

- *Name and contacts* of controller, the joint controller (if present), the controller's representative and the Data Protection Officer.
- *Purposes of processing:* a description of the purposes of processing for each of the typologies and natures (e.g.: accounting, selling, payroll).
- *Categories:* a description of categories of data subject, personal data processing and categories of recipient.
- *Time limits:* where possible, the envisaged time limits for erasure of data, including any legal statement.
- *Security measures:* technical and organisational measures to enforce security on processing of personal data.

4 Compliance Verification Through Standard Security Control

Demonstrating compliance to GDPR is, nowadays, a complex issue that opens a lot of concerns, especially to SMEs. In this paper we focuses mainly on article 25 which imposes Data protection by design and by default (article 25) and that data processing should respect all the principles listed in article 5 (see Sect. 3 for

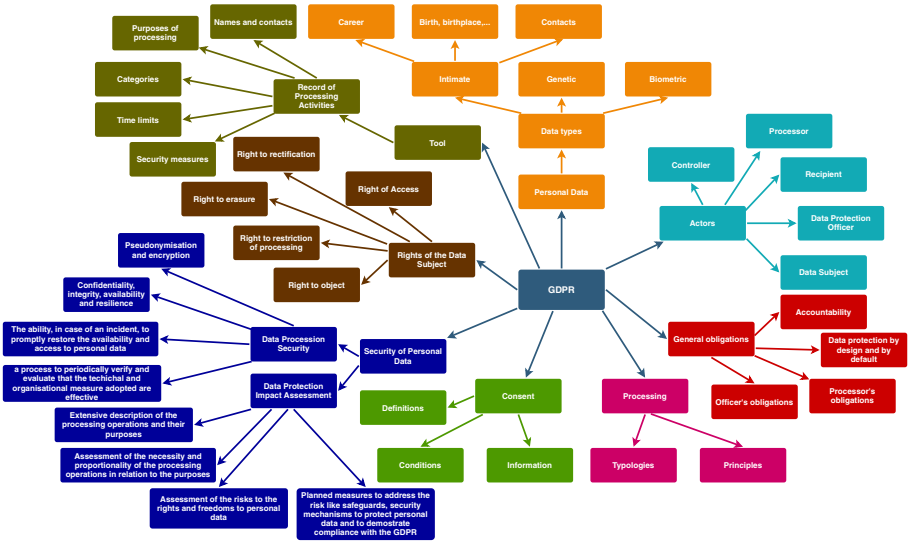

Fig. 6. GDPR global map

more details). GDPR, being a regulation, expresses the constraints (which are reasonable), but does not give a unique solution to implement them and gives freedom (and the duty) to Data Controller to identify the technical solutions. In any case, GDPR starts from the assumption that it is impossible to grant in absolute that a security breach will never happen, but imposes to Data Controller to implements all the countermeasures reasonably needed. In details, article 32 of the GDPR cites the criteria for processing security, while article 33 describes the behaviour to be followed in case of data breach [4]. As a drawback, it is up to Data Controller the role of demonstrating that he has applied all due diligence to grant correctness of behaviour. Section 2 outlined that, at best of authors' knowledge, no concrete solutions are available at state of the art.

The idea we propose relies on building a Security policy in terms of standard countermeasures that helps to systematically verify the compliance to GDPR, demonstrating the required *due diligence*. Accordingly, our solution relies on few key concepts:

- A **Security Policy** should describe all the organizational and technical procedures in order to demonstrate the correctness of systems behaviour
- The Security Policy should be expressed in terms of **standard security controls**, which are system and technology independent
- Security controls selection should be documented and clearly related to GDPR rules in order to both enable a basis for security assessment and offer a clear demonstration of compliance to the regulation

In order to grant the first point, we adopted the NIST security control framework [13], described in the following subsection. To address the second point,

instead, we systematically analysed the control framework, in order to create a detailed mapping of security controls and GDPR articles. The result is a pretty complex *mapping table* available on request to the authors and for which we report in this paper only some example rows. It is worth noticing that NIST security control framework contains (in the Appendix I) a table that relates each security control to controls in international standard (e.g. ISO 27000). Accordingly, our approach can be extended to such standard with a limited effort, this will be subject to a future work from our team. Last but no least, to document and assess the security policy for a specific infrastructure we defined a simple process to derive the security controls that each component of the infrastructure should respect, building a dedicated set of security controls for each of them.

4.1 NIST Security Controls

As outlined above, in order to grant well known, accepted and reusable security countermeasures, we adopted the NIST control framework, a catalogue of security controls. It is worth noticing that we adopted the revision 5 of the control framework, released in September 2020; this revision completely change the approach to privacy controls respect to the previous versions, adding new control families and outlining, for each control, if it affects or not privacy requirements. Alternative frameworks exist in literature, proposed by standardization bodies and/or by industry-oriented organizations, such as the ISO/IEC 27002 specification [10], CIS (Center for Internet security) security controls and the Cloud Security Alliance's (CSA) Cloud Control Matrix. Appendix I of NIST SP-800-53 outlines the relationship among the proposed controls and the international standards. Alternative mappings are offered by CIS and CSA among the controls they propose and NIST Framework. Being the NIST framework openly accessible, we choose to adopt it as a reference for our work.

A security control, according to NIST, can be defined as follows: *Security Controls are safeguards or countermeasures prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements*.

A system security policy can be expressed in the form of *capabilities*, which are themselves expressed in terms of a list of standard *security controls*. NIST lists several security controls, addressing different security domains and are related to both technical and organization aspects. As an example, the NIST Security Control Framework (currently supported by our process) lists more than 900 controls belonging to 18 different *control families*, including access control (AC), identification and authentication (IA), physical and environmental protection (PE) and awareness and training (AT).

Security controls are organized in Families, listed in Table 1 Each security control family has a name, that intuitively identify the capabilities addressed by the controls, and an acronym, used to identify the Family.

Table 1. NIST security controls families

ID	Name	ID	Name
AC	Access control	PE	Physical and environmental protection
AT	Awareness and training	PL	Planning
AU	Audit and accountability	PM	Program management
CA	Assessment, authorization, and monitoring	PS	Personnel security
CM	Configuration management	PT	PII processing and transparency
CP	Contingency planning	RA	Risk assessment
IA	Identification and authentication	SA	System and services acquisition
IR	Incident response	SC	System and communications protection
MA	Maintenance	SI	System and information integrity
MP	Media protection	SR	Supply chain risk management

NIST framework describes security controls in natural language, but adopting a fixed structure and with fixing naming rules. Each Security Control has a name, which summarize the control behaviour and an identifier, made of the family acronym followed by an incremental number (e.g. AC-1). The First security control of each family is always an organizational prescription, that requires the documentation and the description of the practice related to the family. It acts even as a description of the generic characteristics of the control family. The description of the control is offered in natural language and describes the prescription that should be done to correctly implement the countermeasure it refers to. A *supplemental guide* section describes additional actions and supports (human) operators that have the role of verifying the correct implementation of the control. The description of the control ends with a list of *Related controls* that directly impact or support the implementation of that control. Security Controls description may include *Control Enhancements*. Control Enhancements are themselves security controls that increase the strength of the base control. Their identifiers are formed by the ID of the security control they enhance, followed by an additional incremental value, commonly reported in parenthesis, e.g. AC-2(1).

As an example, the security control **IR-6**, named **INCIDENT REPORTING** has the following description[2]: *i) Require personnel to report suspected security and privacy incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and ii) Report security, privacy, and supply chain incident information to [Assignment: organization-defined authorities].* An example of enhancement is **IR-6 (1)** Automated Reporting, that imposes to automate the process of reporting. For brevity's sake we have not reported the full control and control enhancement descriptions, we invite the interested reader to check the NIST document for further details.

[2] The following text is directly extracted from NIST document.

4.2 How to Relate Security Controls and GDPR

NIST security control framework contains almost a thousand of security controls, considering even the enhancements, accordingly the control selection process (tailoring) can be very hard to perform. NIST suggests the adoption of their risk-based procedure and offers a referring baseline which outlines the level of risk for which each control should be considered.

For what regards privacy, NIST framework adopts, as a reference, the U.S laws (i.e. the FIPP standard) that differs from the EU regulation. In order to help tailoring process and identification of controls related to privacy, the latest version of the security control framework contains dedicated table that outlines: i) if a security control is privacy related and ii) if the security control is implemented by a system according to technical or organizational means.

It is worth noticing that we aim at adopting the control framework in an innovative way, suggesting a new process for security control tailoring, focused on EU legislation. Accordingly we had to make a dedicated analysis throughout all the framework, comparing it against the EU regulation. A detailed analysis of the full framework is a long and error-prone activity, so we proceeded in a systematic way, building a list of security controls, that we consider relevant for the GDPR. We built such a list following the procedure here described:

1. Starting from the Conceptual Map of the GDPR (illustrated in Sect. 3 and reported in Fig. 6) we assigned to each GDPR article a label to outline if it affects Technical (T) or Organizational (O) means
2. We selected all controls labeled as privacy-related, selected if they are Technical or Organizational ones and checked one by one against the GDPR articles of the same type. If we considered the control able to grant compliance to the regulation article, we:
   - describe how the security control grants compliance to the GDPR article;
   - describe the limit of such compliance, i.e. what the control, as it is, cannot grant respect to GDPR constraints;
   - outline if the control relates to System, Data or Organizational means;
   - outline the list of security control enhancement needed to grant compliance to the regulation.
3. Once the privacy-related controls (together with their enhancements) were analysed, we restarted the process for all the security controls that are listed in the *related controls* of the controls selected, and for each of them:
   - if we consider the security control relevant respect to the GDPR compliance, we applied the process in step 2
   - if we consider the security control an alternative and or a useful improvement, we added the id of the control in the description of the control that suggested this one
   - if we consider the security control useless respect to GDPR compliance, we simply neglect it
4. we analysed all the security controls that were not yet analysed and, if needed, we applied the process described in step 2, analysing consequently the related controls

5. we made a final review of the full framework

Note that, at end, we analysed the full framework, but the process adopted helped us in granting coherence in the analysis and limits the possible errors. Table 2 describes briefly each field of the final mapping table, in order to help the reader to correctly interpret the result.

Table 2. NIST-GDPR mapping table fields

Field	Values	Description
Art.	Number	Article number of GDPR
Title	Text	Title of GDPR Article
Type	T, O	**T**echnical or **O**rganizational prescription
Notes	Text	Notes about the article
Control	NIST ID	NIST Security Control Identification in the format <Family>-<Number>
Motivation	Text	Description of how the security control covers the article prescription
Limits	Text	Description of the article prescription that the security control cannot grant
Target	D, S, O	The article and the control are related to **D**ata, **S**ystem or **O**rganization
En.	NIST ID	The ID of security control enhancement needed to cover the article prescription, in the format <Family>-<Number>-<Number>
Related	NIST ID	Identification of the NIST security controls related to the one discussed, needed to cover article prescription, in the format <Family>-<Number>

In order to illustrate the result of the mapping process, offering a guide to its interpretation, we briefly illustrate it for the case of article 7 (related to the consent) and 33 (related to notification) of the GDPR. We cannot report a full description of each law article and mapping due to space constraints, the full map can be requested to the authors. A piece of the table was reported in Table 3. As outlined in Sect. 3, article 7 relates to the *Conditions for Consent*, which we consider a technical measure (consent must be collected, maintained in the system and must contain a clear set of data). Accordingly we identified six different standard security controls that regulates the consent management process: IP-2, PA-4, AC-3, IP.4, PA-2 and IP-5. 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 (IP-2) relates to data (and governates the conditions of the consent). In fact it is classified as *Data Oriented Target(D)*. Such control, moreover has two enhancements that we suggest to adopt (IP-2(1) and IP-2(2)) and a related security control IP-4, 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(8) enhancement, which is specific for consent revocation (needed by GDPR). The last three security controls (IP-4, PA-2 and IP-5) relate to the *Organization (O)*, so they do not affect directly our systems, but should be implemented through the internal procedures adopted in the organization. As illustrated, a detailed analysis of the table enables to identify the security controls to be implemented and, accordingly, it supports an internal self-assessment oriented to grant (and demonstrate) compliance to GDPR.

It is worth noting that not always a control exists that enables to correctly implement all the law prescriptions. As an example Article 33 imposes to notify to supervisory authority that a personal data breach has happened and imposes a time constraint (2 weeks) for such a notification. However, even if security control IR-6 (together with enhancement IR-6(2)) matches with the requirement of notification, there is no enhancement and/or additional control that imposes the two weeks limit. In such a case we report such a limitation of the suggested control in column 7. DPO should outline to Data Controller to apply an additional check.

Table 3. 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	IP-2	Consent		D	IP-2(1)	IP-4
								IP-2(2)	
				PA-4	Ensures that information sharing is authorized respecting the purpose		D		PA-1
				AC-3	Allows consent revocation		S	AC-3(8)	
				IP-4	Notifies privacy authorization		O	IP-4(1)	
				PA-2	Determines the authority that allows data collection		O		
				IP-5	Helps understanding the actions to be performed on the data collected from the user		O		
33	Notification of a personal data breach to the supervisory authority	O		IR-6	TBC	Time constraints for notification are missing		IR-6(2)	

5 Conclusions and Future Work

The effort needed by Enterprises, in particular SMEs, to grant compliance to GDPR is time- and cost- expensive. Moreover it involves specialized competences, including, but not limited to, the technical skills on security and privacy.

Among the issues opened by GDPR implementation, this paper focuses on the selection of countermeasures needed to demonstrate compliance to GDPR. As we outlined in the paper, this technical problem implies the definition of a security policy that grants compliance to the regulation on one side and that could be concretely assessed on the other side.

We proposed a concrete technique that helps the security administrator to define a security policy in terms of standard countermeasures and outline how such policy addresses GDPR constraints, offering a simple way to support GDPR compliance verification.

Standard security controls are commonly adopted in certification processes and in security assessment procedures, offering enough technical details to enable the technical personnel to verify their correct implementation with an acceptable effort. This paper offers two concrete results: (i) a conceptual map of the GDPR, and (ii) the mapping among GDPR articles and the security controls.

The solution has the great advantage of offering a technical base to demonstrate compliance and offer a clear support to DPO, Data Controller and Data Processor to verify the correct implementation of security countermeasures.

We aims at extending the methodology in the near future, fully automating the process of countermeasures selection and comparison and generating a report that outlines how countermeasures addresses GDPR requirements. Moreover, we aims at integrating existing risk analysis tools, in order to relate the proposed countermeasures directly to the DPIA (Data Protection Impact Analysis) prescribed by the GDPR.

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

References

1. Ahmadian, A.S., Coerschulte, F., Jürjens, J.: 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, Conference Code: 176459, pp. 80–95 (2016). https://doi.org/10.1007/978-3-319-40512-4_5
2. Ahmadian, A.S., Strüber, D., Riediger, V., Jürjens, J.: Supporting privacy impact assessment by model-based privacy analysis. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, New York, NY, USA, pp. 1467–1474, SAC 2018. Association for Computing Machinery (2018). https://doi.org/10.1145/3167132.3167288

3. Ahmadian, A., Jurjens, J.: Supporting model-based privacy analysis by exploiting privacy level agreements, Conference of 8th IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2016, pp. 360–365. IEEE Computer Society (2016). https://doi.org/10.1109/CloudCom.2016.0063. 12 December 2016 Through 15 December 2016; Conference Code: 126112
4. Article 29 Working Party: guidelines on personal data breach notification under Regulation 2016/679 (wp250rev.01) (2018). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
5. Cloud Security Alliance (CSA): Privacy level agreement outline for the sale of cloud services in the European union, p. 21 (2013). https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf
6. Council of European Union: General Data Protection Regulation (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj
7. Di Martino, B., Mastroianni, M., Campaiola, M., Morelli, G., Sparaco, E.: Semantic techniques for validation of GDPR compliance of business processes. In: Barolli, L., Hussain, F.K., Ikeda, M. (eds.) CISIS 2019. AISC, vol. 993, pp. 847–855. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-22354-0_78
8. Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S., Charalabidis, Y.: An assessment of privacy preservation in crowdsourcing approaches: towards GDPR compliance, vol. 2018, pp. 1–9 (2018). IEEE Computer Society (2018). https://doi.org/10.1109/RCIS.2018.8406643
9. Diamantopoulou, V., Pavlidis, M., Mouratidis, H.: Privacy level agreements for public administration information systems, p. 8 (2017)
10. 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., et al. (eds.) CyberICPS/SECPRE/SPOSE/ADIoT -2019. LNCS, vol. 11980, pp. 238–257. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-42048-2_16
11. Elluri, L., Joshi, K.P.: A knowledge representation of cloud data controls for EU GDPR compliance. In: 2018 IEEE World Congress on Services (SERVICES), pp. 45–46. IEEE, July 2018. https://doi.org/10.1109/SERVICES.2018.00036, https://ieeexplore.ieee.org/document/8495788/
12. Elluri, L., Nagar, A., Joshi, K.P.: An integrated knowledge graph to automate GDPR and PCI DSS compliance. In: 2018 IEEE International Conference on Big Data (Big Data), pp. 1266–1271. IEEE, December 2018. https://doi.org/10.1109/BigData.2018.8622236, https://ieeexplore.ieee.org/document/8622236/
13. Joint Task Force Interagency Working Group: Security and Privacy Controls for Information Systems and Organizations. Technical report, National Institute of Standards and Technology, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Edition: Revision 5
14. Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., Robaldo, L.: PrOnto: privacy ontology for legal reasoning. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2018. LNCS, vol. 11032, pp. 139–152. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98349-3_11
15. Rios, E.: Service level agreement-based GDPR compliance and security assurance in (multi)cloud-based systems. IET Softw. **13**(3), 213–222 (2019). https://doi.org/10.1049/iet-sen.2018.5293