MDPI

Article

Preserving Digital Privacy in e-Participation Environments: Towards GDPR Compliance

Vasiliki Diamantopoulou[1],*, Aggeliki Androutsopoulou[1], Stefanos Gritzalis[2] and Yannis Charalabidis[1]

[1] Department of Information and Communication Systems Engineering, School of Engineering, University of the Aegean, Samos, Greece; {vdiamant,ag.andr, yannisx}@aegean.gr
[2] Department of Digital Systems, University of Piraeus, Piraeus, Greece; sgritz@unipi.gr
* Correspondence: vdiamant@aegean.gr

Version September 9, 2019 submitted to Journal Not Specified

Abstract: The application of the GDPR 2016/679/EC, the Regulation for the protection of personal data, is a challenge and must be seen as an opportunity for the redesign of the systems that are used for the processing of personal data. An unexplored area where systems are used to collect and process personal data is the e-Participation environment. The latest generations of such environments refer to sociotechnical systems based on the exploitation of the increasing use of Social Media, by using them as valuable tools, able to provide answers and decision support in public policy formulation. This work aims at the analysis of such systems, by exploring the level of the satisfaction of the privacy requirements that GDPR imposes, contributing to the identification of challenges that e-participation approaches impose with regard to privacy protection.

Keywords: General Data Protection Regulation; e-Participation; crowdsourcing methods; privacy requirements; privacy enhancing technologies

1. Introduction

With the emergence of the Information Society, information has been transformed into a valuable asset and its management into a core economic activity [1]. At the same time, the administration of information gave rise to conflicts between its management bodies and exposed risks regarding individuals' rights, preservation of privacy and protection of personal data [1,2]. Such risks do not arise from external phenomena, but from human decisions and actions [3] related to the management and use of information according to the apparent interests of social groups, governments, businesses and individuals. Internet, as a leading technological infrastructure, has supported the realisation of a new field of communication between social entities, in the context of private life. The exponentially increasing use of the Internet and a variety of novel services based on it, especially social media, has gradually led to their adoption in areas of public life, such as politics. Digital channels of communication have introduced a new form of political interaction that seems to be of particular importance in restoring public confidence in politics and institutions that represent it. In an e-democracy environment, e-participation paradigm consists a key component, as it is the means to adapt government decisions to the real needs and expectations of citizens [4–6]. Thus, the almost continuous presence of people on social networks, through smart phones and tablets, consists a formidable chance for government entities to frequently collect opinions, preferences, evaluations, also considering that the demand of participation of citizens to the government has dramatically increased. Above all, however, the Internet and social media are important tools in decision making when designing public policies, supporting new models of interaction between governments, businesses,

citizens and experts, such as crowdsourcing [7], in the context of the need to tackle complex issues effectively in modern democratic societies.

Although Internet-mediated and social media interaction opens up new avenues of collaboration, it simultaneously generates new privacy and data protection risks, as often, users have zero or limited awareness of their personal disclosure risks. At the same time, they seem to be complacent by expressing implicit trust in the providers of services they use, in government and legislation, believing that they will protect them from the unlawful use of their personal data.

In the context of the Information Society, that recognises information as a source of knowledge and scope, but without the fact that the rights of information subjects are effectively guaranteed, the terms of privacy are again argued upon on a worldwide level and the right to privacy emerges as one of the most endangered [8]. Privacy is not considered as a new social issue, but it has been redefined as a topic within the Information Society since the "classical" concept of privacy has been significantly enriched [9,10], while its scope fluctuates significantly within various socio-cultural systems [11,12]. In addition, in post-modern society, the demarcation between the private and public sectors has become vaguer as the relationships between different information management bodies have become complex [13,14]. Privacy preservation has been recognised as a key principle in all modern democracies [15] and this preservation has been documented as a prerequisite for ensuring a sustainable development of our digital age [2,16].

Privacy, in the well-known advocacy of American judges S. Warren and L. Brandeis [17], was defined as "the right to be let alone". According to [18] it is the right of individuals to determine what information is accessible, to whom and when, while [19] is concerned with the selective control of individuals of access to them by others, thus constituting a dynamic process of setting boundaries in the context of social interactions. Data subjects often believe they can control the data they disclose, thereby protecting their privacy. However, this proves to be incorrect, as privacy is not controlled by individuals but by organisations that own and manage information [20]. In fact, the potential for privacy violations has greatly expanded due to the social media platforms [21] and the development of online participation methods. In this work the issue of privacy protection is being examined, in the context of actions being triggered by governments and public bodies in the context of e-participation, and in particular on crowdsourcing environments, applying new collaborative models, which obviously bring multiple benefits when developing public policies, ensuring that privacy requirements are met [22] and even by default [23].

The regulatory framework for privacy preservation is multidimensional. Although general principles of privacy have long been in place, states often have a different starting point for legal culture, making interpretations of privacy more and more indistinct [24]. In this context, the recently implemented General Data Protection Regulation (2016/697/EU) in the European Union is expected to make a positive contribution, ensuring a *"consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union"* (Recital 10, GDPR). Although privacy preservation is legally enshrined and theoretically self-evident in any form of modern democratic social practice [25], a multitude of incidents have been made public, such as the Snowden case or the notorious scandal of Cambridge Analytica, and others have not been made public. There are incidents, including a large number of affected individuals while others are limited. All these recorded incidents confirm that governments, organisations and businesses collect personal data, often without the knowledge of the data subjects, without disclosing the reasons for the collection to third parties or their retention period. At the same time, data subjects, although often voluntarily providing their personal data or conscientiously consenting to their collection, at a later time express concern or anxiety about protecting their privacy.

The rest of the paper is structured as follows: Section 2 presents the challenges that have arisen after GDPR came to existence. In this section we provide an overview of the readiness level of the organisations that process EU citizens' personal data. Section 3 presents the methodology that we

develop and follow in a project regarding the compliance of an organisation with the GDPR. Section 4 gives an overview of the e-Participation methods and the challenges that this domain faces regarding the protection of the personal identifiable information (PII) being exposed. Section 5 applies the proposed methodology into the e-Participation methods domain, in order to recognise the PII that are published in various platforms, to identify the privacy requirements that have to be satisfied in such environments, and using this information, to further conduct the required analysis. Finally, Section 6 concludes the paper by raising issues for further research.

2. Protection of personal data in the GDPR era

General Data Protection Regulation (hereafter, GDPR or Regulation) [26] entered into force in May 2018 aiming at the enhancement of user data protection. Despite that GDPR leads towards a radical change with many benefits for the individuals that provide their personal data in order to utilise a service, it turned out to be a significant challenge. Organisations that process personal data have to conduct long and complex changes for the personal data processing activities to become GDPR compliant. On the other hand, individuals, as data subjects, are empowered with new rights, of which they have to become aware and realise their importance in order to be able to exercise them. Finally, the role of data protection authorities changes along with their expectations from organisations.

The application of the GDPR entitled EU regulators to enforce momentous transformation on the way organisations process personal data of individuals. These changes were expected to have a positive impact on the latter. However, GDPR has turned into a significant challenge for organisations, which are enforced to conduct a series of adjustments, shifts and changes on their information technologies, their business processes, their culture, and on the way they operate overall. Some of these challenges have been documented by organisations, academic papers or by European Commission reports, shedding light on the particular aspects of the GDPR that appear troublesome, as we analyse below.

The first official report regarding the implementation of the GDPR, provided by the European Data Protection Board [27] indicates that most organisations have put a lot of effort towards GDPR compliance, by increasing their financial budget allocated to personal data protection (30% - 50%), increasing the personnel allocated, while the authorities from 31 member states have dealt with a total of 206.326 legal cases related with complaints, data breaches, etc. A report by ISACA [28] presents research indicating that approximately 65% of organisations reported that they were not ready in terms of GDPR compliance in May 2018. The same report elaborates on technical, regulatory and legislative tools that should be implemented to assist organisations in their compliance efforts. In the same direction, Thomson Reuters [29] reports that organisations are still not ready in terms of GDPR compliance, many of them know very little about the Regulation and are still not fully aware of the GDPR's potential impact not being ready for the GDPR compliance. In a survey [30] conducted among privacy experts published by the International Association of Privacy Professionals (IAPP) in 2019, reported that less than 50% of respondents mentioned they are fully compliant with GDPR. Interestingly, nearly 20% of the privacy professionals who participated argues that full GDPR compliance is truly impossible.

However, after the enforcement of the GDPR, to the best of our knowledge, there is no recorded study regarding the readiness of the e-Participation platforms with regard to the requirements of the Regulation. There are only a few papers that deal with privacy problems in e-Participation methods. The authors in [31] brought together researchers from the crowdsourcing field and the human computation field, and among others, they raised issues related to privacy requirements in such environments, such as the preservation of anonymity. In [32] the authors focused on a privacy problem related with task instances in crowdsourcing. Next, the authors in [33] focus on privacy issues related with workers in crowdsourcing environments and they propose a crowdsourcing quality control method in order to estimate reliable provided results from low-quality ones. Our study provides a holistic approach of privacy preservation in e-Participation environments, by analysing the corresponding methods and identifying, through the PII that are provided by the users, the privacy

requirements that are compromised, providing also appropriate implementation techniques, following the PDCA model of a GDPR compliance project.

3. General Data Protection Regulation as a project

The current state, as the aforementioned analysis revealed, indicates the necessity for organisations that process personal data to systematically work in order to align their activities according to the requirements of the European Regulation. The compliance of an organisation with the GDPR can be seen as a project [34] that follows the fundamental steps of the Deming Plan-Do-Check-Act (PDCA) model [35]. The proposed approach for implementing a data protection compliance project is based on the guidelines of ISO standards ([36–38]) and on the recently released [39] which focuses on privacy information management, and on best practices published in various ISO standards ([36,37,40–43]) and various guidelines ([44,45]). For entities that process personal data (i.e. data controllers or data processors) the enforcement of GDPR requires the implementation of both technical and organisational measures, such as the appointment of Data Protection Officers, when necessary, the deployment of tools that allow demonstration of GDPR compliance, the conduction of data protection impact assessments, the training of staff, the implementation of data de-identification techniques, to name a few. All these actions towards the compliance of the Regulation have been emerged in the general PDCA model, which is divided in four phases and each phase has between two and seven steps. The proposed methodology is summarised in Figure 1 and analysed below. It is worth noting that each step is not presented in detail because they are specific for each project, depending mostly on the under examination organisation's context. Moreover, many processes might be iterative, because of the need for progressive development throughout the implementation project; for instance communication, training activities, or corrective actions.

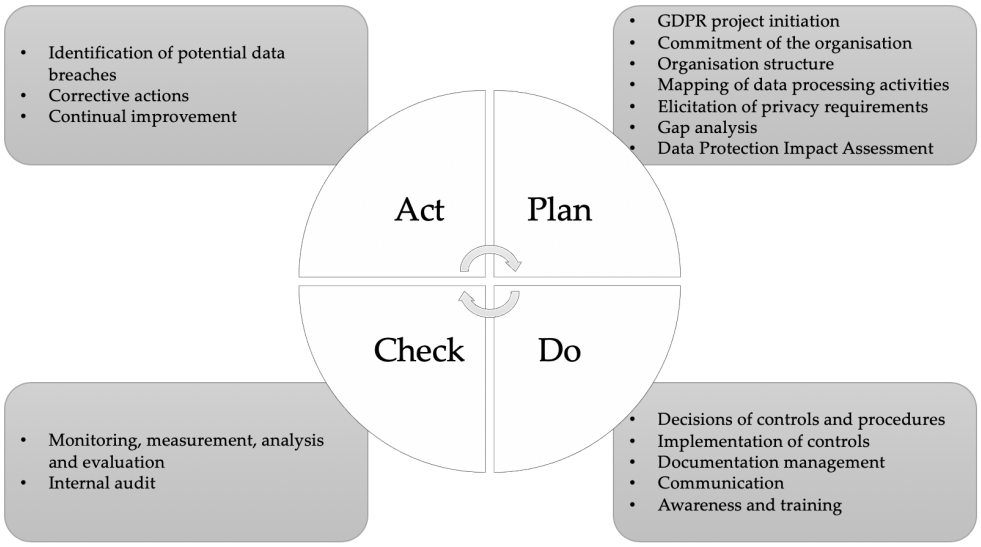

Figure 1. PDCA model of a GDPR compliance project

1. **Plan:** Practically, in this first step, we have the initiation of the project, which has the commitment of the management, being supported by the organisation as a whole. During this phase, the objectives of the project are set, as well as the identification of the corresponding employees that will be involved in the process is being conducted. This phase also contains the analysis of the existing system/systems, the identification of the organisation structure, as well as the mapping of the data the organisation processes in order to be able to conduct data classification. Next, the elicitation of the privacy requirements is conducted, since, according to ISO 27014:21013 [38], the desired state of an organisation *requires compliance with legislation, regulations and contracts*, i.e. external requirements. Since the following step is the gap analysis in relation to the requirements

of the Regulation, this has to be conducted based on the above *desired state*. Consequently, the elicitation of privacy requirements is mandatory in order to be able to proceed with the gap analysis and the data protection impact assessment that follow. Below, the steps of mapping of data processing activities, the gap analysis and the DPIA are analysed in detail:

- *Mapping of data processing activities:* This step aims at the depiction of the current status of the organisation regarding the personal data that it keeps. More specifically, this process starts with the identification of the various processing activities. These might be related with the administration of the organisation, the management of the users, the management of the customers, the human resources management, the sales, the procurement, the technical support, to name a few. In this initial phase, we should identify the role of the organisation regarding each process, i.e. acting as a data controller or as a data processor.According to the Greek Data Protection Authority[1], for each processing activity, the following data should be provided:
  (a) Basic characteristics of the processing: i) processing activity, ii) association with the file of joint controllers (if any), iii) categories of the data subjects, iv) categories of personal data being kept for each category of data subjects, v) sources of the data, vi) categories of the recipients, vii) retention period for each type of data.
  (b) Data related to the data processors: i) contact details of data processors, ii) provision of the corresponding contract.
  (c) Transfers of personal data to third countries or international organisations: i) third country (outside EU), ii) legal basis, iii) provision of information regarding the level of protection of data.
  (d) Technical and organisational measures: i) physical or electronic means of retention of personal data, ii) general description of technical and organisational security measures, iii) association with the file of analytical description of applied security controls.
  (e) Lawfulness of processing: i) legal basis of processing personal data (according to Art.6 of the GDPR), ii) legitimate interests, iii) legal basis of processing special categories of personal data.
  (f) Other information: i) Proof of provision of consent by the data subjects (as soon as the consent is the basis for the lawfulness of processing), ii) rights of data subjects being provided by the controller, iii) existence of automated individual decision-making, including profiling.
- *Elicitation of privacy requirements:* The vulnerability of information privacy has increased due to the intrusion of social media platforms [21] and the intensive development of new e-Participation methods on top of these. To a large extent, the raw material for most of interactions of individuals, with others, with well-established communities and with governmental authorities, include personal data of individuals. Alongside the benefits for the governmental decision making processes, which have been described in Section III, these developments are accompanied with privacy risks that can have negative impact on users' participation [46]. In view of the above, the GDPR is especially well timed. The basis for this study is the fundamental privacy requirements, as they have been defined and identified by the consensus of the literature of the area [43,47–49], namely, authentication, authorisation, anonymity, pseudonymity, unlinkability, undetectability, unobservability.
- *Gap analysis in relation to the requirements of the GDPR:* In this step the gap analysis for the organisation is presented, in relation to the requirements of the GDPR. In particular, compliance is examined per GDPR article, taking into account the required data protection policies, documentation, security measures, etc. the organisation has already implemented. The status of the compliance activities for each compliance requirement can be described using the following scale:

[1] https://www.dpa.gr/

(a) Implemented (highlighted with green colour): The organisation has taken all necessary steps to meet a specific compliance requirement.
(b) In progress (highlighted with orange colour): The organisation has taken part of the necessary steps to meet a specific compliance requirement.
(c) Not applicable (highlighted with grey colour): The organisation is not obliged to meet a specific compliance requirement.
(d) Not implemented (highlighted with red colour): The organisation has not taken any of the necessary steps to meet a specific compliance requirement.

The gap analysis is repeated for each organisation's processing activity.

- *Data protection impact assessment:* In order for an organisation to be compliant with the GDPR, they may need to conduct a data protection impact assessment (GDPR, Article 35) to extend the implemented countermeasures in a way that can demonstrate the appropriateness of the measures taken for each processing activity. Global platforms must assess the risks of individuals' fundamental rights and interests as part of the data protection impact assessment, in particular, when systematically monitoring users or using artificial intelligence algorithms and other new technologies, evaluating individuals or processing sensitive data at a large scale. Specifically, an organisation may be required to carry out an assessment of the impact of their processing activities in order to protect personal data during its processing, as well as to protect computer or other supporting resources that support processing. To this end, this step of the Plan phase aims to conduct a data protection impact assessment which is a risk assessment related to the impact that business operations or technologies associated with the processing of personal data, may have. According to Article 35 of the GDPR, data protection impact assessment is conducted when particular types of processing is likely to result in a high risk to the rights and freedoms of natural persons. In order for an organisation to satisfy the requirement for data protection impact assessment, the core actions they have to follow are i) to create a list of classified corporate information - including personal data, and ii) to implement an appropriate methodology, and to establish policies and procedures for carrying out an impact assessment. In the literature there are quite a few risk analysis methodologies [50–52], however, Working Party 29 has released criteria for acceptable data protection impact assessment [44] that an organisation can follow, where they also suggest EU generic frameworks as well as sector-specific ones.

2. **Do:** This step allows the plan set up in the previous step to be carried out. It includes the design of the necessary controls and procedures as well as their implementation. The documentation of key processes and security controls is also included in this step. Documentation facilitates the management of the aforementioned processes and controls, and it varies depending on the type, the size and the complexity of the organisation, their IS any other technologies available, as well as the requirements of the stakeholders and the relevant third parties (customers, suppliers). Furthermore, this step contains the establishment of a communication plan, as well as the set up of awareness and training sessions for the employees of the organisation. In particular, the step *Action plan for the conformance of the organisation with the GDPR* takes into consideration the outcomes of the previous steps namely *mapping of data processing activities*, *gap analysis in relation to the requirements of the GDPR*, and *data protection impact assessment* in order for the analyst to capture the appropriate technical and organisational controls appropriate for the under examination organisation. More specifically, the plan for the recommended actions related to the personal data processing is presented. Recommendations and guidelines should also be provided for choosing the appropriate controls for mitigating the risks identified from the data protection impact assessment step. In addition, suggestions for a long-term compliance strategy and ongoing improvement of the under examination organisation, regarding its compliance with the GDPR, are also provided.
3. **Check:** This step consists of two concrete actions. The first action contains the monitoring, measurement, analysis and evaluation of the process. In order to be sure that the suggested controls, set up in the second step, are implemented efficiently, the organisation shall determine

the controls that need to be measured and monitored, focusing on the activities that are linked to the organisation's critical processes. The second action refers to the internal audit that the organisation shall conduct. The objectives of the audit should be focused on the evaluation of the actions related with the GDPR requirements been implemented in the organisation.

4. **Act:** The final step of the process aims at maintaining the results of the project and identification of corrective action processes as well as the continuous improvement of the established framework. The corrective actions procedure is realised through the following steps:

- Identification of the non-conformity and analysis of its impacts on the organisation.
- Analysis of the situation, i.e. analysis of the root causes, assessment of the available options, selection of the most appropriate solution(s).
- Corrective actions, by implementing the chosen solutions and recording the actions taken.
- Continuous improvement, by evaluating and reviewing the actions taken.

4. e-Participation methods

Although the emergence of e-Participation is dated back to early 2000s as "the use of information and communication technologies to broaden and deepen political participation by enabling citizens to connect with one another and with their elected representatives" [53], a new stream of research challenges has recently emerged in the field, due to the advent of the new privacy protection regulations, described in the previous section. The e-Participation paradigm consists of a multitude of methods of participation in the democratic process, ranging from the simplest information provision by governmental bodies through open data platforms with the aim of enhancing transparency, to the straightforward measurement of public opinion through e-voting and e-polling systems. The most common form of e-Participation is the organisation of complex virtual, small and large-group discussions, allowing reflection and consideration of issues in e-Consultation platforms, discussion forums, allowing stakeholders to contribute their opinions on specific policy topics. Advanced deliberation tools also exist in order to target the discourse to specific public issues, such us spatial and urban planning [54]. Using GIS tools to support e-participation or participatory budgeting [55], allowing citizens to identify, discuss and prioritise public spending. Other e-Participation methods include collaboration environments, empowering individuals to shape and build communities, electronic surveying, electioneering and campaigning, that enable election campaigns, protesting, lobbying, petitioning and other forms of collective action, as per the categorisation within the DEMO-net project' [56]. In all of these various forms of civic engagement, users may consciously or unconsciously reveal different kind of personal/sensitive data, depending on the institutional framework of their operation thus imposing risks in their privacy preservation.

The first generation of e-Participation is characterised by dedicated platforms for public consultations were used, owned and controlled by government agencies, which are responsible for the data processing/storing [57,58], known mainly as electronic forums. However, the next generation of e-Participation, which entails the use of Web 2.0 and Social Media [59], brings plethora of content generated by a variety type of users (including citizens, experts, governmental agencies) and new forms of social interactions, thus diverse types of information disclosure. Moreover, in this Social Web enabled interaction, public participation is enabled through the utilisation of third-party applications, whose owners become the data controllers. In these paradigms, citizens may express political opinions, sentiments or stances against policy measures and prospective policies, even in general political beliefs. All the above constitute factors increasing the complexity of privacy requirements.

Since its advent, methods for enabling and supporting e-Participation, have been also evolved, such as open innovation, social innovation, co-creation and crowdsourcing paradigms [60,61]. Such paradigms are used for mining ideas and knowledge from citizens concerning possible solutions to social needs and policy related problems, for co-designing public sector innovations and for fostering collaboration between social actors [62–64]. Therefore, the interaction data collected undergoes various types of advanced processing (e.g., access analytics, opinion mining, simulation modelling) in order to extract synthetic conclusions from them and provide substantial support to government policy makers.

Three paradigms of crowdsourcing are analysed in [7] in terms of privacy preservation. Active crowdsourcing is based on a centralised automated publishing of policy-related content on multiple social media. The citizens are able to access this content, view it and interact with it through the capabilities offered by each of these social media. Then, data on citizens' interaction with them (e.g., views, comments, ratings, votes, etc.) are monitored and collected using the application programming interfaces (APIs) of the targeted social media. Part of this citizens-generated content is numeric (e.g., numbers of views, likes, retweets, comments, etc., or ratings), so it can be used for the calculation of various analytics following Social Media Monitoring practices. Furthermore, a large part of this content is in textual form, so opinion mining methods are also applied. On the other hand, in the paradigm of passive crowdsourcing, a set of tools for searching and analysing public policy related content that has been generated by citizens in numerous "external social media" (i.e. not belonging to government, such as various political blogs, fora, Facebook and Twitter accounts, etc.), people may be unaware of the purpose of processing their contributions. This paradigm also provides advanced tools for analysing this content in order to identify specific issues, ideas, concerns and other information hidden within the text of citizens' posting on the web [65].

It is evident that e-Participation produces large quantities of textual and non-textual contributions concerning policies and decisions under discussion. Yet, a considerable variety of underpinning technologies and tools are involved in order to address the overload of information produced by public participation methods. Data mining and analysis (including sentiment classification, argument extraction, topic identification), information visualisation and visual analytics are some of the methods utilised complementary to e-Participation initiatives in order to help the constructive extraction and aggregation of information and its transformation to useful insights within the decision-making process. These ICT tools performing data processing oriented towards the collection and integration of public opinions and values in the democratic decision-making processes, bring another dimension in the investigation of privacy requirements.

The research contributes to the identification of challenges that e-participation approaches impose with regard to privacy protection and especially on the compliance of these methods with the GDPR.

5. Applying PDCA model for GDPR compliance to e-Participation methods

Based on the analysis conducted in Sections 3 and 4, it appears that the e-Participation methods are an unexplored area regarding the preservation of privacy of the participants (i.e. data subjects), and thus, it is of utmost importance to set the foundation towards the compliance of such domain with the requirements of the GDPR. This section describes in detail the solid steps that an organisation needs to follow in order to deliver a compliant with the GDPR e-Participation service to citizens, taking care for the protection of their personal data being exposed to the public. To delimit the research scope, we focus on the crowdsourcing methods described in the previous section, as the most challenging ones in terms of data processing. The method that we propose to apply in the crowdsourcing paradigms is the one presented in Section 3, i.e. the PDCA model for GDPR compliance.

Stage 1: Plan

1. *GDPR project initiation:* When a GDPR project start, it is important for the participants to realise the benefits that the organisation gains. Specifically, the involved stakeholders should understand why the organisation's mission, objectives and values should be strategically aligned with data protection objectives. It is necessary to obtain an overview of the under examination organisation to understand the security challenges and the risk inherent in that market segment. E-participation initiatives are carried out mostly, by public institutions (at local, national or EU level) [55,66,67], and in some cases by civil society organisations and policy makers, such as MEPs [68]. Therefore the same principles apply, as within any GDPR compliance project they undergo, and therefore listing the implementation of e-Participation projects in their data processing activities is necessary. General information about the organisation should be collected in order to better appreciate its mission, strategies, main purpose, values, etc. Regardless of the

type of the e-participation carrier , the development of democracy and civic engagement shall be one of its strategic objectives. This helps ensure consistency and alignment between the strategic objectives for risk management and the organisation's mission.

The objectives of a GDPR compliance project are to indicate the intent of the public organisation to treat the risks identified and / or to comply with requirements of the Regulation. Initially, it is necessary to establish the objectives of a GDPR compliance project in consultation with the interested parties, such as other policy stakeholders, governmental and regulatory bodies.

2. *Commitment of the organisation:* When a GDPR compliance project starts, the higher management has to approve it and to communicate it to the lower levels of the organisation. The communication chain and commitment has to span the governmental structure and follow any bureaucratic processes established. Such a programme requires a lot of effort, both when the project starts, and when the analysis will have been completed and the results will have to be put in place. In the beginning of such a project, the employees should provide to the analysts the required information, since they are the ones who deeply know the processes and the data they handle. In the case of e-Participation activities, usually dedicated teams consisting of members of the public institution or inter-organisational committees are formed to carry out the activity. The commitment of the organisation and public servants is also required after the analysis will be completed and new measures, technical or organisational ones, will have to be applied in order to protect the personal data that the organisation processes.
3. *Organisation structure:* One of the most important elements in defining the GDPR compliance and its governance is the hierarchical setting in the organisation of the Data Protection Officer (DPO). Before the definition of the structure, the management of the organisation should consider factors such are its mission, potential business implications, organisational and functional structure, external entities (e.g., other public organisations, citizens or businesses acting as service consumers, suppliers), as well as the internal culture. The governance structure for data protection that will be developed should meet the following requirements: i) absence of conflicts, ii) strong support from senior management or upper governance level, iii) high influence ability, iv) integration of security concerns. Finally, the activities related to processing of personal data should be coordinated by a person in charge of information security and data protection, who establishes cooperation and collaboration with other departments of the organisation or other collaborating organisations.
4. *Mapping of data processing activities:* According to Article 30 of the GDPR, the data controller is obliged to demonstrate that the processing operations they are performing are in accordance with the requirements of the GDPR. To this end, organisations performing e-Participation initiatives should maintain a record of processing activities under its responsibility.

Table 1 summarises the data being processed in the area of e-Participation methods, taking as example the crowdsourcing paradigms discussed in the previous section. s shown, the purpose of the three forms of crowdsourcing likewise any e-Participation activity is to increase public engagement. However, there are cases that the initiatives are carried as piloting activities as part of research projects. Depending on their scope and if organised by international organisations, third countries can be involved. As identified in the assessment of the different methods, categories of personal data being processed are defined by the Social Media platform used by the citizens to contribute and which of them are then are collected to estimate public opinion [7]. The most prominent data input in all e-Participation generations are comments provided by the participants to the platforms, either these are electronic forums, consultations tools or social media. This increases the complexity of GDPR compliance projects, since textual contributions can reveal sensitive data of the data subject, such as political opinions and orientation, attitude against the policy under discussion, or profiling of voters. According to their privacy policy, Social Media can reveal additional personal data such as demographics.

The active crowdsourcing method relies on requests of users to provide content, while the passive crowdsourcing and the passive expert-sourcing do not require from individuals to create new content, instead they conduct selective passive crowdsourcing. This constitutes feasible for the authors of the content in the active crowdsourcing to be aware of the processing taking place. Regarding the passive approaches, any data that data subjects decide to disclose publicly in Social Media (i.e. without any restrictions on access rights to specific groups of people) might subject to processing without users being informed. Therefore legitimate crowdsourcing applications should acquire users' consent via the Social Media, with which citizens interact.

In the case of active crowdsourcing, apart from citizens acting as Social Media users, also policy makers contribute (as they are the initiators of posts and provide content on a policy topic in order to stimulate the discussion). Processing of data is carried out by the Social Media platforms, but also third party applications are used for advanced data analysis, while the results are transmitted to the decision makers.

Table 1. Processing activities of e-Participation methods

Processing activity	**Active Crowdsourcing**	**Passive crowdsourcing**	**Passive Expert-sourcing**
Purpose of processing	i) Public Engagement, ii) Research Purposes		
Legal basis for processing	User Consent to the data privacy policy of the SM platform (Terms and Conditions)		
Third countries	According to the scope of the e-Participation initiative		
Data source	Data Subject		
Personal data categories	**Personal Data:** Social media users personal data provided to the SM platform (first name, last name, date of birth – age, gender, email address, login email, occupation), country (the ones submitting comments), social media user ID, Photos, social media activity (likes, retweets) **Sensitive Data:** Political opinions	**Personal Data:** Social media users personal data provided to the SM platform (first name, last name, social media user ID), comments, social media activity (in terms of frequency comments posted in SM/activity logs) **Sensitive Data:** Profiling data (personality-attitude towards)	**Personal Data:** Social media users personal data (first name, last name, email address, login email, educational Level, job title, organisation, position, professional experience, topics of expertise/ specialisation, CVs), photos **Sensitive Data:** Political opinions, profiling data (personality-attitude towards)
Data subjects	Citizens/Social Media Users, Policy Makers	Citizens/Social Media Users	Experts, Social Media Users
Receivers	Policy Makers, Public/Governmental organisations		
Processing IT application	Social Media platform, Third party applications		

5. *Elicitation of privacy requirements:* Since the mapping of the personal data being processed in e-Participation environments has been recorded, the organisation has to proceed with the privacy requirements elicitation, taking into account the environment of the under examination organisation. For capturing the ecosystem created between the policy makers and the citizens, we used Secure Tropos methodology [69] from the security requirements area, which has been extended [70,71] to meet the privacy requirements as well. Figure 2 illustrates the analysis of a crowdsourcing environment, where each component of the crowdsourcing ecosystem (cyber, physical, human) is represented as an *actor*, which has some *strategic goals* (aims or functionalities), relevant *plans* (tasks) for achieving those goals, and, finally, a set of *assets* (resources) required for carrying out the plans. Additionally, each actor may have a number of *dependencies* for goals/tasks that cannot achieve on their own. After we have captured all the dependencies between the two actors, according to Secure Tropos modelling language, we are able to elicit

the security and privacy requirements (in our work we focus only on privacy requirements elicitation) of the system, which are presented as *constraints*, which restrict the various goals and plans that each actor has.

Focusing on the crowdsourcing environment, a Policy Maker (actor) aims to analyse citizens' data in order to shape their policies. This functionality cannot be supported independently, but requires input from Citizens (actor). This input refers to the citizens' PIIs and their political opinions (resources), and this interaction is modelled as a dependency between the policy maker and the citizen. As we discussed in Section 3, the e-Participation methods are assessed against the list of seven privacy requirements, i.e. authentication, authorisation, anonymity, pseudonymity, unlinkability, undetectability, unobservability. In our example here, the requirements (constraints) that restrict the PII of citizens, being at risk at certain circumstances are anonymity, unlinkability, undetectability and unobservability [7].

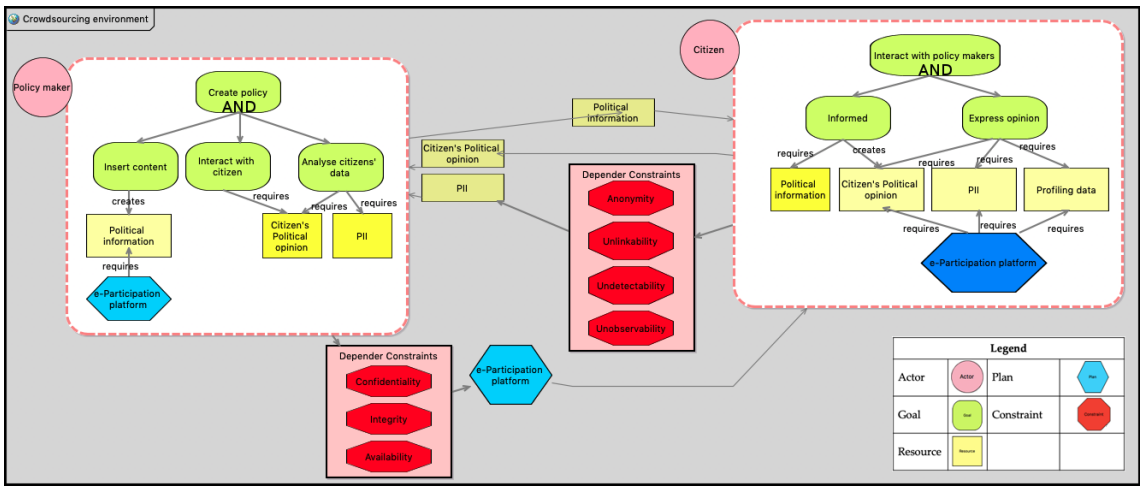

Figure 2. Crowdsourcing environment analysis

Based on the above privacy requirements elicitation process, we proceed with the analysis of the three different e-participation methods. The requirements "authentication" and "authorisation" are inherited by the privacy specifications of the Social media platforms and Web 2.0 sources, where users contribute with content only after they are registered and authenticated. Such platforms embed appropriate security mechanisms aiming to control access only by authorised users, therefore both authentication and authorisation are safeguarded in all methods. For this reason, the three approaches collect solely data that are open to the public. With respect to the reservation of the rest requirements in the two crowdsourcing approaches, a distinction among the concept of citizen-sourcing and expert-sourcing has to be made. The two first citizen-sourcing methods process only aggregated data resulting to automatically generated summaries. Although the results do not compromise the identity of authors, as discussed before it is possible that textual content (e.g., comments) may include sensitive information, concerning the name, demographics or the beliefs of the citizens authoring this content. Through this information, a third party can infer the identity of the author of this content. Moreover, the extraction of a textual segment can help to track the original source (e.g., a comment) and thus allow to a third party to link the user with the particular resource, distinguish the Social Media user, and observe that the specific user is using the relevant Social Media capability. All the above pose risks at the anonymity, unlinkability, undetectability and unobservability of individuals interacting through Social Media services within the active and passive crowdsourcing method. Finally, pseudonymity is satisfied as it can be retained as far as the Social Media platforms allow.

6. *Gap analysis:* Detailed information and guidelines concerning this step cannot be provided in a generic form, as all the steps involved in the gap analysis stage are determined by the structure

of each organisation, and of the actions and security and privacy countermeasures it has already implemented regarding the protection of its IS and the preservation of data subjects' privacy.

7. *Data Protection Impact Assessment:* For fulfilling the objectives of this study, PIA-CNIL [45] methodology is applied (Privacy Impact Assessment, Commission Nationale de l'Informatique et des Libertés), which is in accordance with the data privacy impact assessment that has been described in ISO/IEC 29134 (2017) [72], Information technology – Security techniques – Guidelines for privacy impact assessment. PIA-CNIL methodology consists of the following stages:

   (a) Analysis of the context of processing of personal data under consideration.
   (b) Identification of the existing or under development controls, for the satisfaction of legal. requirements and the privacy risk assessment.
   (c) Assessment and evaluation of privacy risks.
   (d) Decision regarding the satisfaction of the principles related with the preservation of privacy and treatment of the identified risks.

   The main goal is the identification of the assets related to the Processing Activities of personal data of e-Participation methods, as well as the identification of risks against privacy protection and the impact that can have an incident of *illegitimate access to data*, *unwanted modification of data*, or *data disappearance*. In this task, risk identification and assessment is conducted, by evaluating the likelihood of risk occurrence and the potential impact, while recommendations on appropriate strategies for risk mitigation are provided.

   By applying PIA-CNIL in e-Participation methods, we have the following outcomes:

   (a) Context of personal data processing: This information has been provided in Step 4 *Mapping of data processing activities* of this Phase.
   (b) Controls: The objective of this step is to build a system that ensures compliance with privacy protection principles. So, existing controls have to be identified or determined. These controls can be organisational controls (such as organisation policy, risk management, project management, incident management, supervision, etc.), logical security controls (such as anonymisation, encryption, backups, data partitioning, logical access control, etc.), and physical security controls (such as physical access control, security of hardware, protection against non-human risk sources, etc.).
   (c) Risks: Potential privacy breaches: The objective of the third step of PIA-CNIL is to gain a good understanding of the causes of risks, the threats against privacy, as well as the impact of their potential realisation. In this step, for each of the three risk categories, i.e. illegitimate access to data, unwanted modification of data, data disappearance. Again, this part of DPIA cannot be provided as the risk that put the personal data the organisation processes in danger are different in every organisation, according its structure and the already applied security and privacy mechanisms.
   (d) Risk management decisions: The already existing controls are evaluated for the satisfaction of legal requirements and decisions are made whether existing controls are satisfactory. When not, an action plan is prepared and validated.

Stage 2: Do

1. *Decisions of controls and procedures:* The organisation should plan, implement and control the processes required to meet data protection and privacy requirements, as well as to implement actions determined from the results of the previous steps of risk assessment and data protection impact assessment. According to PIA-CNIL methodology, an organisation might respond to a risk that puts in danger the fundamental rights and freedoms of natural persons in one of the following ways: a) avoidance of the processing, b) confrontation of risk with the application of corresponding controls that minimise either the likelihood of appearance or the severity of the risk, and c) the acceptance of the risk.

2. *Implementation of controls:* The protection of personal data and privacy can be improved and enhanced by designing IT systems that reduce the degree of intrusion into the data subjects' privacy by focusing on the provision of efficient privacy process patterns [73,74].
3. *Documentation management:* The organisation should keep documented information to the extent that the processes have been carried out as planned. A four-level approach is proposed regarding the types of documents that should be kept. In the lower level the organisation keeps any records in order to provide objective evidence of compliance with the GDPR requirements. In the third level are any worksheets, forms, checklists, etc. that describe in detail how the tasks and activities are conducted. In the second level we have the description of the security process, controls and procedures and in the first level we have the governance framework description, such as policies, the scope of the organisation and other strategic documents.
4. *Communication:* The data protection objectives that the organisation sets can be used as a basis for an effective communication strategy. It is worth noting that when establishing the data protection communication objectives, they should be aligned with organisation's business communication policy, taking into account the view of internal and external interested parties, and that they are consistent with the communication principles. Indicative communication approaches and tools are the website of the organisation, newspaper articles, surveys, reports, press releases, brochures and newsletters, advertisements, workshops and conferences, posters, public meetings, media interviews, emails, focus groups, and presentations to groups.
5. *Awareness and training:* A planned and systematic training process can greatly help the organisation to improve its capabilities and to meet its data protection objectives. The appropriate involvement of personnel who are in the process of developing skills may result in personnel feeling a greater sense of ownership of the process, which makes them assume more responsibility for ensuring its success. The organisation's data protection and training policies, information security management requirements, resource management, and process design should be considered when initiating training to ensure that the required training will be directed towards satisfying the organisation's needs. According to [75], when training is selected as the solution to close the competency gap, training requirements should be specified and documented. Potential training methods are the workshops, distance learning, self-training, on-the-job coaching, apprenticeships, and course on-site or off-site.

   The awareness programme allows an organisation to raise awareness, to ensure consistency in information security and data protection practices, and to contribute to the dissemination and implementation of policies, guidelines and procedures.

Stage 3: Check

1. *Monitoring, measurement, analysis and evaluation:* In order to have confidence that the GDPR and the suggested controls are implemented efficiently, it is recommended that the organisation should determine the controls that have to be measured and monitored, as well as the responsible for this process. The best practice is to focus monitoring and measurement on the activities that are linked to the critical processes that enable the organisation to achieve its data protection objectives and targets. Examples of such objectives are measuring incidents (e.g., the percentage of false alarms through an event detection, the average cost of an incident), training activities (e.g., the percentage of staff who have receiving training and qualifications, the number of hours of training by employees), vulnerabilities (e.g., the percentage of systems tested for vulnerabilities in a period of time) and nonconformities (e.g., the percentage of nonconformity not corrected in the predetermined time, the average required time to fix a nonconformity).
2. *Internal audit:* Audit refers to the evaluation based on facts. This kind of evaluation is conducted to highlight the strengths and weaknesses of the audited organisation or system. Audit results are communicated to management who will then take the required and appropriate measures. In the context of the application of the GDPR, the objectives of the internal audit should be

focused on assessing and providing compliance on the best practices of the requirements of the Regulation. The outcome of the audit process should cover the following:

- Data governance and accountability of the organisation
- Privacy notices
- Potential breach notification
- Data processors and international transfers (if any)
- Lawfulness of processing and consent management
- Satisfaction of data subjects' rights
- Applied security measures appropriate to the risks involved with the processing of personal data
- Implementation of privacy by design and by default principles on systems and processes offered by the organisation

Stage 4: Act

1. *Identification of potential data breaches:* Organisations should establish procedures to ensure that no personal data breaches occur. Any potential breach should be reported to the corresponding Data Protection Authority (DPA). In order for an organisation to be able to report the breach *without undue delay and, where feasible, not later than 72 hours after having become aware of it* they should have already develop clear policies, they should have determine establish procedures and best practices and they should have developed procedures regarding the notification both of the DPA and the data subjects, if necessary (Article 34, GDPR).
2. *Corrective actions:* These actions should be taken to eliminate once and for all the root causes of a nonconforminty or of any other existing undesirable event and to prevent its reoccurence. The organisation should determine the actions necessary to eliminate the potential causes of nonconformity in accordance with the conditions of the GDPR.
3. *Continual improvement:* The GDPR programme needs to be maintained and updated periodically. During the continual improvement phase, the processes and procedures undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the process is reviewed and updated regularly as part of the organisation's change management process to ensure that new information is documented and appropriate controls are revised.

6. Conclusions

Successful completion of a GDPR project in any organisation is a challenging issue, demanding a lot of effort by the corresponding stakeholders. However, it is imperative for all organisations, public and private ones, to be compliant with the Regulation, in order to protect the personal information they process. In the algorithmic society, where services are personalised, where worldwide communication has become trivial, and decisions are taken based on processing outcomes, and with respect to the principles of fairness and transparency, it is of growing importance for organisations to, at least, inform data subjects regarding their processing activities. Furthermore, special attention should be paid to the legal ground of each processing activity. When it is based on consent, the user should be able to withdraw it easily at any time. This obliges the data controller to stop the processing if there is no other legal ground to justify this processing. The conditions for consent are strengthened as the consent will be valid only if it has been freely given, specific informed, affirmative and unambiguous (GDPR, Article 7).

The results of this paper provide new contributions for researchers and practitioners as follows. The main findings regard to organisations conducting e-participation activities. First of all, public administrations undergoing GDPR assessments, should include the organisation of the e-participation initiatives among their data processing activities and thus maintain this record. Next, the consent should be obtained to provide legitimate basis for processing citizens' data. The media or tool used for acquiring and processing citizens data determines the type of required consent. E-participation

practitioners can follow the steps that we propose and assess the readiness of their organisation, based on the processing activities they conduct to raise public engagement, the platform that they use to exchange content with citizens and the personal data they process. It is worth noting that the type of data each organisation processes determines the level of risk the organisation faces regarding the preservation of individuals' privacy.

Future directions of this work include the practical evaluation of indicative platforms from each of the three examined crowdsourcing methods, in order to reveal the peculiarities of each process. By engaging relevant stakeholders, we will be able to further examine any additional privacy requirements that these systems or in general e-participation platforms have. Moreover, we are planning to extend our work by analysing each ecosystem both from security and from privacy requirements perspective, in order to be able to identify potential threats that these systems have, any vulnerabilities that might have impact on the resources of the system, and finally be able to propose specific countermeasure in order to mitigate such risks.

Author Contributions:

Vasiliki Diamantopoulou and Aggeliki Androutsopoulou conceived of the presented idea and designed the study. Vasiliki Diamantopoulou investigated the General Data Protection Regulation and formulated the methodology to be followed in order for an organisation to reach compliance with the Regulation. Aggeliki Androutsopoulou developed the theoretical background regarding the e-Participation methods and investigated the exposed data that must be protected. Stefanos Gritzalis contributed to the design of the applied methodology. Stefanos Gritzalis and Yannis Charalabidis were involved in the planning and supervised the work.

Abbreviations

The following abbreviations are used in this manuscript:

EU	European Union
GDPR	General Data Protection Regulation
PDCA	Plan - Do - Check - Act
DPIA	Data Protection Impact Assessment
API	Application Programming Interface
DPO	Data Protection Officer
PIA-CNIL	Privacy Impact Assessment Methodology released by the French Data Protection Authority (CNIL)
DPA	Data Protection Authority

References

1. Spiekermann, S.; Acquisti, A.; Böhme, R.; Hui, K.L. The challenges of personal data markets and privacy. *Electronic markets* **2015**, *25*, 161–167.
2. Acquisti, A.; Gritzalis, S.; Lambrinoudakis, C.; di Vimercati, S. *Digital privacy: theory, technologies, and practices*; CRC Press, 2007.
3. Lash, S.; Szerszynski, B.; Wynne, B. *Risk, environment and modernity: towards a new ecology*; Vol. 40, Sage, 1996.
4. As-Saber, S.; Hossain, K.; Srivastava, A. Technology, society and e-government: in search of an eclectic framework. *Electronic Government, An International Journal* **2007**, *4*, 156–178.
5. Medaglia, R. eParticipation research: Moving characterization forward (2006–2011). *Government Information Quarterly* **2012**, *29*, 346–360.
6. Susha, I.; Grönlund, Å. eParticipation research: Systematizing the field. *Government Information Quarterly* **2012**, *29*, 373–382.
7. Diamantopoulou, V.; Androutsopoulou, A.; Gritzalis, S.; Charalabidis, Y. An assessment of privacy preservation in crowdsourcing approaches: Towards GDPR compliance. 2018 12th International Conference on Research Challenges in Information Science (RCIS). IEEE, 2018, pp. 1–9.

8. Beldad, A.; De Jong, M.; Steehouder, M. I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior* **2011**, *27*, 2233–2242.
9. Mitrou, L. *Law in the Information Society*; Sakkoula (in Greek), 2002.
10. Mitrou, L. *General Data Protection Regulation: New Law - New Obligations - New Rights*; Sakkoula (in Greek), 2017.
11. Solove, D.J. A taxonomy of privacy. *U. Pa. L. Rev.* **2005**, *154*, 477.
12. Islam, M.B.; Watson, J.; Iannella, R.; Geva, S. What I want for my Social Network privacy **2014**.
13. Newburn, T.; Jones, T. *Private security and public policing*; Clarendon Press, 1998.
14. Marx, G.T. Murky conceptual waters: The public and the private. *Ethics and Information technology* **2001**, *3*, 157–169.
15. Henderson, S.E. Expectations of privacy in social media. *Miss. CL Rev.* **2012**, *31*, 227.
16. Cohen, J.E. What privacy is for. *Harv. L. Rev.* **2012**, *126*, 1904.
17. Warren, S.D.; Brandeis, L.D. Right to privacy. *Harv. L. Rev.* **1890**, *4*, 193.
18. Westin, A.F. Privacy and freedom. *Washington and Lee Law Review* **1968**, *25*, 166.
19. Altman, I. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. **1975**.
20. Conger, S.; Pratt, J.H.; Loch, K.D. Personal information privacy and emerging technologies. *Information Systems Journal* **2013**, *23*, 401–417.
21. Mohamed, N.; Ahmad, I.H. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior* **2012**, *28*, 2366–2375.
22. Gritzalis, S. Enhancing web privacy and anonymity in the digital era. *Information Management & Computer Security* **2004**, *12*, 255–287.
23. Cavoukian, A.; others. Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada* **2009**, *5*.
24. Mitrou, L.; Gritzalis, D.; Katsikas, S.; Quirchmayr, G. Electronic voting: Constitutional and legal requirements, and their technical implications. In *Secure electronic voting*; Springer, 2003; pp. 43–60.
25. Sideri, M.; Kitsiou, A.; Kalloniatis, C.; Gritzalis, S. Sharing secrets, revealing thoughts and feelings: perceptions about disclosure practices and anonymity in a FB university students' community. *International Journal of Electronic Governance* **2017**, *9*, 361–384.
26. EU. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) **2016**.
27. EDPB. European Data Protection Board (2019). First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities. Technical report, 2019.
28. ISACA. GDPR: The end of the beginning. Technical report, 2018.
29. Thomson Reuters 2019. Study finds organizations are not ready for GDPR compliance issues. Technical report, 2019. https://legal.thomsonreuters.com/en/insights/articles/study-finds-organizations-not-ready-gdpr-compliance-issues, visited = 09-07-2019.
30. IAAP. Privacy Tech Vendor Report. Technical report, 2018.
31. Bernstein, M.; Chi, E.H.; Chilton, L.; Hartmann, B.; Kittur, A.; Miller, R.C. Crowdsourcing and human computation: systems, studies and platforms. CHI'11 Extended Abstracts on Human Factors in Computing Systems. ACM, 2011, pp. 53–56.
32. Varshney, L.R. Privacy and reliability in crowdsourcing service delivery. SRII Global Conference (SRII), 2012 Annual. IEEE, 2012, pp. 55–60.
33. Kajino, H.; Arai, H.; Kashima, H. Preserving worker privacy in crowdsourcing. *Data Mining and Knowledge Discovery* **2014**, *28*, 1314–1335.
34. Diamantopoulou, V.; Tsohou, A.; Karyda, M. General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance. tba. Springer, 2019, pp. –.
35. Moen, R.; Norman, C. Evolution of the PDCA cycle, 2006.
36. ISO/IEC. ISO 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements. Technical report, 2013.
37. ISO/IEC. ISO 27001:2013 Information Technology - Security Techniques - Code of practice for information security controls. Technical report, 2013.

38. ISO/IEC. ISO 27014:2013 Information Technology - Security Techniques - Governance of information security. Technical report, 2013.
39. ISO/IEC. ISO 27701:2019 Security techniques - Extension to ISO/IEC27001 and ISO/IEC27002 for privacy information management - Requirements and guidelines. Technical report, 2019.
40. ISO/IEC. ISO 27004:2016 Information Technology - Security Techniques - Information security management - Monitoring, measurement, analysis and evaluation. Technical report, 2016.
41. ISO/IEC. ISO 27005:2018 Information Technology - Security Techniques - Information security risk management. Technical report, 2018.
42. ISO/IEC. ISO 31000:2018 Risk management - Guidelines. Technical report, 2018.
43. ISO/IEC. ISO 29100:2011 Information Technology - Security Techniques - Privacy framework. Technical report, 2011.
44. Working Party 29. Guidelines on Data Protection Impact Assessment. Technical report, 2019.
45. CNIL 2018. Privacy Impact Assessment (PIA) - Knowledge bases. Technical report, 2018.
46. Krasnova, H.; Kolesnikova, E.; Guenther, O. " It won't happen to me!": self-disclosure in online social networks **2009**.
47. Fischer-Hübner, S. *IT-security and privacy: design and use of privacy-enhancing security mechanisms*; Springer-Verlag, 2001.
48. Cannon, J. *Privacy: what developers and IT professionals should know*; Addison-Wesley Professional, 2004.
49. Pfitzmann, A.; Hansen, M. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management **2010**.
50. Alberts, C.; Dorofee, A.; Stevens, J.; Woody, C. Introduction to the OCTAVE Approach. Technical report, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2003.
51. Fredriksen, R.; Kristiansen, M.; Gran, B.A.; Stølen, K.; Opperud, T.A.; Dimitrakos, T. The CORAS framework for a model-based risk management process. International Conference on Computer Safety, Reliability, and Security. Springer, 2002, pp. 94–105.
52. Yazar, Z. A qualitative risk analysis and management tool–CRAMM. *SANS InfoSec Reading Room White Paper* **2002**, *11*, 12–32.
53. Macintosh, A. Characterizing e-participation in policy-making. 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the. IEEE, 2004, pp. 10–pp.
54. Loukis, E.; Xenakis, A.; Peters, R.; Charalabidis, Y. Using Gis Tools to Support E_Participation–A Systematic Evaluation. International Conference on Electronic Participation. Springer, 2010, pp. 197–210.
55. Society, T.D. Digital tools and Scotland's Participatory Budgeting programme: A report by the Democratic Society for the Scottish Government. Technical report, The Scottish Government-Riaghaltas na h-Alba, 2016.
56. Fraser, C.; Liotas, N.; Lippa, B.; Mach, M.; Macintosh, F.M.; Mentzas, G.; Tarabanis, K. DEMO-net: Deliverable 5.1 Report on current ICTs to enable Participation. Technical report, DEMO-net project, 2006.
57. Caddy, J.; Gramberger, M.; Vergez, C. *Citizens as partners: Information, consultation and public participation in policy-making*; Organisation for Economic Co-operation and Development PUMA Working Group on . . . , 2001.
58. Loukis, E.; Macintosh, A.; Charalabidis, Y. *E-Participation in Southern Europe and the Balkans: Issues of Democracy and Participation Via Electronic Media*; Routledge, 2013.
59. Charalabidis, Y.; Loukis, E. TRANSFORMING GOVERNMENT AGENCIES'APPROACH TO EPARTICIPATION THROUGH EFFICIENT EXPLOITATION OF SOCIAL MEDIA **2011**.
60. Desouza, K.C.; Smith, K.L. Big data for social innovation. *Stanford Social Innovation Review* **2014**, *12*, 38–43.
61. Charalabidis, Y.; Loukis, E.; Androutsopoulou, A. Fostering social innovation through multiple social media combinations. *Information Systems Management* **2014**, *31*, 225–239.
62. Brabham, D.C. *Crowdsourcing*; Mit Press, 2013.
63. Androutsopoulou, A.; Karacapilidis, N.; Loukis, E.; Charalabidis, Y. Towards an integrated and inclusive platform for open innovation in the public sector. International Conference on e-Democracy. Springer, 2017, pp. 228–243.
64. Hilgers, D.; Ihl, C. Citizensourcing: Applying the concept of open innovation to the public sector. *International Journal of Public Participation* **2010**, *4*.

65. Charalabidis, Y.; Karkaletsis, V.; Triantafillou, A.; Androutsopoulou, A.; Loukis, E. Requirements and Architecture of a Passive Crowdsourcing Environment. *Electronic Government and Electronic Participation-Joint Proceedings of Ongoing Research of IFIP EGOV and IFIP ePart 2035* **2013**.
66. Aitamurto, T. Crowdsourcing for democracy: A new era in policy-making. *Crowdsourcing for Democracy: A New Era In Policy-Making. Publications of the Committee for the Future, Parliament of Finland* **2012**, *1*.
67. Christensen, H.S.; Karjalainen, M.; Nurminen, L. What does crowdsourcing legislation entail for the participants? The Finnish case of Avoin Ministeriö. Internet, Policy and Politics Conferences, 2014.
68. Lironi, E. Potential and Challenges of E-participation in the European Union. *Study for the AFCO Committee, Director General of Internal Policies* **2016**.
69. Mouratidis, H. Secure software systems engineering: the Secure Tropos approach. *JSW* **2011**, *6*, 331–339.
70. Kalloniatis, C.; Mouratidis, H.; Vassilis, M.; Islam, S.; Gritzalis, S.; Kavakli, E. Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces* **2014**, *36*, 759–775.
71. Diamantopoulou, V.; Mouratidis, H. Applying the physics of notation to the evaluation of a security and privacy requirements engineering methodology. *Information & Computer Security* **2018**, *26*, 382–400.
72. ISO/IEC. 29100:2011(E) Information technology - Security techniques - Guidelines for privacy impact assessment. Technical report, 2017.
73. Diamantopoulou, V.; Kalloniatis, C.; Gritzalis, S.; Mouratidis, H. Supporting Privacy by Design Using Privacy Process Patterns. IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, 2017, pp. 491–505.
74. Diamantopoulou, V.; Argyropoulos, N.; Kalloniatis, C.; Gritzalis, S. Supporting the design of privacy-aware business processes via privacy process patterns. Research Challenges in Information Science (RCIS), 2017 11th International Conference on. IEEE, 2017, pp. 187–198.
75. ISO. 10015:1999 Quality management - Guidelines for training. Technical report, 1999.