information

MDPI

Article

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

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

[1] Department of Information and Communication Systems Engineering, School of Engineering, University of the Aegean, 83200 Samos, Greece; ag.andr@aegean.gr (A.A.); yannisx@aegean.gr (Y.C.)
[2] Department of Digital Systems, University of Piraeus, 18532 Piraeus, Greece; sgritz@unipi.gr
* Correspondence: vdiamant@aegean.gr

Received: 19 November 2019; Accepted: 18 February 2020; Published: 20 February 2020

Abstract: The application of the General Data Protection Regulation (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 being used for the processing of personal data. An unexplored area where systems are being used to collect and process personal data are 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 explores the privacy requirements that GDPR imposes in such environments, contributing to the identification of challenges that e-Participation approaches have to deal with, 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. The 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 all the above being widely accepted 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 is the means to adjust government decisions to the real needs and expectations of citizens [4–6]. Thus, the continuous presence of people on social networks, via smart phones and tablets, consists a formidable chance for government entities to frequently collect opinions, preferences, evaluations, also considering that the demand of citizens' participation in the governance 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], when tackling complex issues effectively in modern democratic societies.

Although Internet-mediated and social media interaction opens up new avenues for collaboration, at the same time, it generates new privacy and data protection risks, as often users have zero or limited awareness of their personal data disclosure risks. Additionally, 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, which 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 the post-modern society, the demarcation between private and public sector 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. Ref. [19] is concerned with the selective control of individuals of access to their personal data, 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 such information [20]. In fact, the potential for privacy violations has greatly expanded due to the use of social media platforms [21] and the development of online participation methods. In this work, the issue of privacy protection is being examined when actions are being triggered by governments and public bodies in the field 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] or, even better, ensured by default [23].

The regulatory framework for privacy preservation is multidimensional. Although generic principles of privacy have long been in place, states often have a different legal and cultural starting point, 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. There are incidents that affect a large number of individuals. All these recorded incidents confirm that governments, organisations and businesses collect personal data, often without the data subjects being aware thereof, 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 [26]. Despite the existence of historical incidents, there is still not a structured way to ensure the privacy protection in the social practices. The research question that arises is whether such method can be defined and applied in democratic contexts.

Taking into account that, in methods like e-Participation and crowdsourcing platforms, personal data and special categories of personal data can be revealed, such as subjective information, personal beliefs and political opinions, a data subject's protection of privacy is at stake. By examining digital privacy and e-Participation in a conceptual level under a unified perspective, we contribute both

to the theoretical and to the practical knowledge. More specifically, the contribution of this work is the provision of a method for GDPR compliance tailored to governmental environments exercising e-Participation. This paper extends the work presented in [27] since it provides the practitioners with a holistic approach of how to protect personally identifiable information (PII) in an e-Participation environment. The proposed method has been based on widely accepted methodologies, frameworks and standards, and, by identifying the special characteristics of an e-Participation environment (see Section 5), it includes an enhanced version of the Plan-Do-Check-Act (PDCA) model proposed in the previous work, for example, by including Data Protection Impact Assessment (DPIA), which is mandatory when specific conditions are met (Article 35 of the GDPR). Additionally, in this work, we have applied the proposed method in a crowdsourcing paradigm which gives us feedback and assessment opportunities on the application of this method in a governmental context. Finally, the provision of our results and outcomes on the examination of the topic from this perspective will save the future researcher from the effort of examining the implications on meeting the GDPR compliance requirements in such environments and will provide guidance to e-government practitioners.

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 method that we developed and followed in a project regarding the compliance of an organisation with the GDPR. Section 4 gives an overview of e-Participation methods and the challenges that this domain faces regarding the protection of PII being exposed. Section 5 applies the proposed method 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. Section 6 presents the application of the proposed method to a real case study from the e-Participation domain. Finally, Section 7 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) [28] entered into force in May 2018 aiming at the enhancement of user data protection. Although GDPR brings radical changes with many benefits for the individuals that provide their personal data when utilising 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 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 enabled 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, the 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 overall way they operate. 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 [29] 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 [30] 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 [31] 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. In a survey [32] conducted among privacy experts published by the International Association of Privacy Professionals (IAPP) in 2019, it was reported that less than 50% of respondents mentioned they are fully compliant with the GDPR. Interestingly, nearly 20% of the privacy professionals who participated argues that full GDPR compliance is truly impossible.

State of the Art

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 [33] brought together researchers from the crowdsourcing field and the human computation field and, among others, raised issues related to privacy requirements in such environments, such as the preservation of anonymity. In [34], the authors focused on a privacy problem related with task instances in crowdsourcing. Next, the authors in [35] 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.

In a more recent study [36], the authors provide guidance for the design of an e-Participation platform taking into account, among others, privacy requirements. There, the authors mention the GDPR as a future fundamental principle and they provide insights regarding data minimisation. In [37], the authors identify privacy functional requirements for crowdsourcing applications focusing on the requirements emerging by the smart cities paradigm. In [38], the authors propose a methodology for using crowdsourcing to evaluate privacy design decisions.

Our study goes beyond the state-of-the-art, by providing 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. In this way, practitioners can use the results of this work in order to comply an e-Participation platform with the GDPR.

3. General Data Protection Regulation Compliance 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 [27] that follows the fundamental steps of the Deming Plan-Do-Check-Act (PDCA) model [39]. We propose the use of this methodology because of its wide applicability, its easy adaptability to the requirements of each environment, as well as because of its iterative character. Taking the PDCA model as a basis, the proposed approach for implementing a data protection compliance project extends it, based on the guidelines of ISO standards [40–42] and on the recently released [43] which focuses on privacy information management, on best practices published in various ISO standards [40,41,44–47], and various guidelines [48,49]. All of these extensions are reflected in the specific steps of each phase.

More specifically, for entities that process personal data (i.e., data controllers or data processors), the enforcement of the GDPR requires the implementation of both technical and organisational measures. In each phase, the extensions are:

- Plan
  - The initiation of the project.
  - The commitment of the higher management regarding the required resources for this project.

- The revision of the organisation structure by the appointment of Data Protection Officers, when necessary.
- The mapping of data processing activities that will facilitate the identification of personal data the organisation processes.
- The elicitation of privacy requirements that vary in each organisation depending on their context.
- The gap analysis that highlights the gaps of the organisation with regard to its compliance with the GDPR.
- The conduction of data protection impact assessment.

- Do
  - Decision of controls and procedures need to be implemented (for new ones), or transformed (for already existing) towards the data protection.
  - Implementation of appropriate controls.
  - Documentation management
  - Communication
  - Awareness and training, for the successful implementation of the controls. will reveal the

- Check
  - Monitoring, measurement, analysis and evaluation that need to be conducted periodically so the organisation will be able to assess their compliance with the GDPR
  - Internal audit on the evaluation of the actions related with the GDPR

- Act
  - Identification of potential data breaches.
  - Corrective actions that need to be taken after a realisation of an incident.
  - Continual improvement of the organisation.

All these actions towards compliance to the Regulation have emerged in the general PDCA model. The proposed method is summarised in Figure 1 and analysed in detail 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.

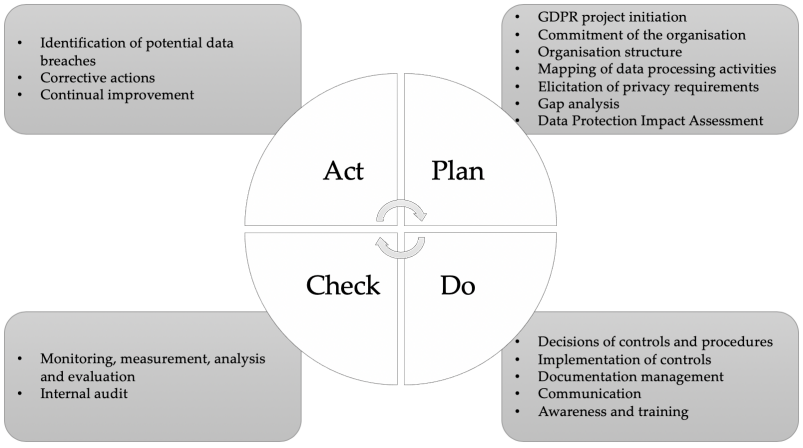

Figure 1. PDCA model of a GDPR compliance project.

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 27014:2013 [42], 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 users, the management of 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.
    - *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 individuals' interactions, 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 3, these developments are accompanied with privacy risks that can have negative impact on users' participation [50]. 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 [47,51–53], 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, gap analysis is conducted in three stages; first, we determine the current state of the organisation, by identifying the processes and controls being in place, second, we determine the level of maturity required for each control, and finally we assess the status of the organisation regarding their level of maturity.
      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 the processing, as well as to protect computer or other supporting resources that support processing. In this step of the Plan phase, a data protection impact assessment is conducted on business operations or

technologies associated with the processing of personal data. According to Article 35 of the GDPR, data protection impact assessment is conducted when particular types of processing are 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 classified list of 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 privacy impact assessment methods [54–57]; however, Working Party 29 has released criteria for acceptable data protection impact assessment [48] 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 and other technologies available, as well as the requirements of the stakeholders and relevant third parties (customers, suppliers). Furthermore, this step contains the establishment of a communication plan to make the established processes, procedures, methods and data sources available to all interested parties, as well as the set up of awareness and training sessions for the employees of the organisation which can greatly help the latter improve its capabilities and meet its data protection objectives. 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. Security experts, established methodologies and standards (such as [58]) will provide assistance on these selections. 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 ensure 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, being identified in Step 1. 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. Organisational Context of 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" [59], 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 with their opinions on specific policy topics. Advanced deliberation tools also exist in order to target the discourse to specific public issues, such as spatial and urban planning [60]. Using Geographic Information System (GIS) tools to support e-Participation or participatory budgeting [61], 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 [62]. 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 on their privacy preservation.

The first generation of e-Participation is characterised by dedicated platforms for public consultations that were used, owned and controlled by government agencies responsible for the data processing/storing [63,64], known mainly as electronic forums. However, the next generation of e-Participation, which entails the use of Web 2.0 and Social Media [65], 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 of the above constitute factors that increase the complexity of satisfying privacy requirements.

Since its advent, complementary methods for enabling and supporting e-Participation have also evolved, such as open innovation, social innovation, co-creation and crowdsourcing paradigms [66,67]. 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 [68–70]. Therefore, the interacted 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 feedback to government policy makers.

Crowdsourcing practices, originated in the private sector, are increasingly utilised by contemporary governments in order to engage citizens into participatory policy making [71]. Three methods of crowdsourcing are analysed in [7] in terms of privacy preservation. The first one, 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 via 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 given in textual form, so opinion mining methods are also applied. On the other hand, in the

second method, entitled passive crowdsourcing, a set of tools is used 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.), and people may be unaware of the purpose of processing. There exist 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 [72]. The aforementioned methods consist of citizen-sourcing, as they are targeted to citizens, as users of popular Social Media platforms. However, a third method is also analysed in [7], aiming at tapping into the knowledge and perspectives of experts (e.g., representatives of stakeholder groups, journalists, government employees, active citizens, etc.) as well, and as such is referred to as passive expert-sourcing. The method is based on the retrieval and processing of social media and web posts or documents authored by experts without any government stimulation. Opinion mining and sentiment classification methods are applied to the textual content in order to identify subjective information, extract opinions and assess their sentiment (positive, negative or neutral) and reputation management techniques to identify the authors with the highest expertise [73].

It is evident that such crowdsourcing methods produce large quantities of textual and non-textual contributions concerning policies and decisions under discussion. However, a considerable variety of underpinning technologies and tools are also 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 techniques 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 Information and Communications Technology (ICT) tools perform data processing oriented towards the collection and integration of public opinions and values in the democratic decision-making processes, and bring to the table additional concerns in the investigation of privacy requirements. The research contributes to the identification of challenges that both e-Participation methods and the ICT tools have to deal with, with regard to privacy protection and, especially, on the compliance of these methods with the GDPR, by focusing on a specific class of e-Participation methods, i.e., crowdsourcing.

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 starts, 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 privacy 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 [61,74,75], and, in some cases, by civil society organisations and policy makers, such as Members of the European Parliament (MEPs) [76]. 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 to 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 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 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 as 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; and (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 an example the crowdsourcing paradigms discussed in the previous section. As shown, the purpose of the three forms of crowdsourcing, like any e-Participation activity is to increase public engagement. However, there are cases that the initiatives are carried out as pilots, 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 in the Social Media platform used by the citizens and are then collected to estimate public opinion [7]. The most prominent data input in all e-Participation generations are comments provided by the participants of 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 be 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, policy makers also contribute (as they are the initiators of posts and provide content on a policy topic in order to stimulate the discussion). Processing of data are 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		

IT: Information Technology, SM: Social Media, ID: Identity Document, CV: Curriculum Vitae.

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 [77] from the security requirements area, which has been extended [78,79] to meet the privacy requirements as well. The decision of choosing a security and privacy requirements methodology lies upon each organisation; however, we suggest that the use of Secure Tropos, as it is a methodology that supports both security and privacy requirements elicitation, is supported by a Computer-Aided Software Engineering (CASE) tool (i.e., SecTro tool) and, finally, the different views of the tool allow the designer to focus on a specific perspective, i.e., (i) on the organisational structure, (ii) on the security and privacy requirements, threats and appropriate countermeasures; and (iii) on the potential attacks a malicious user can conduct,

by exploiting system's vulnerabilities [80]. 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 represented 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].

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 in 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 personal information, concerning the name, demographics, etc., or sensitive information, such as religious or philosophical beliefs, political opinions, etc. 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 track the original source (e.g., a comment) and thus allow for 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 [49] methodology can be applied (Privacy Impact Assessment, Commission Nationale de l'Informatique et des Libertés), which is in accordance with the data protection impact assessment that has been described in ISO/IEC 29134 (2017) [57], Information technology—Security techniques—Guidelines for privacy impact assessment, and is one of the methodologies the

Working Party 29 proposes. It consists of concrete steps, as well as it is supported by a web-based tool. 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 an incident of *illegitimate access to data*, *unwanted modification of data*, or *data disappearance* can have. 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. Thus, 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, 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 risks that put the personal data the organisation processes in danger are different in every organisation, according to 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 [81,82].

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 records to provide objective evidence of compliance with the GDPR requirements. In the third level are 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 the 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 improve its capabilities and 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 [83], when training is selected as the solution to close the competency gap, training requirements should be specified and documented. Potential training methods are 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.

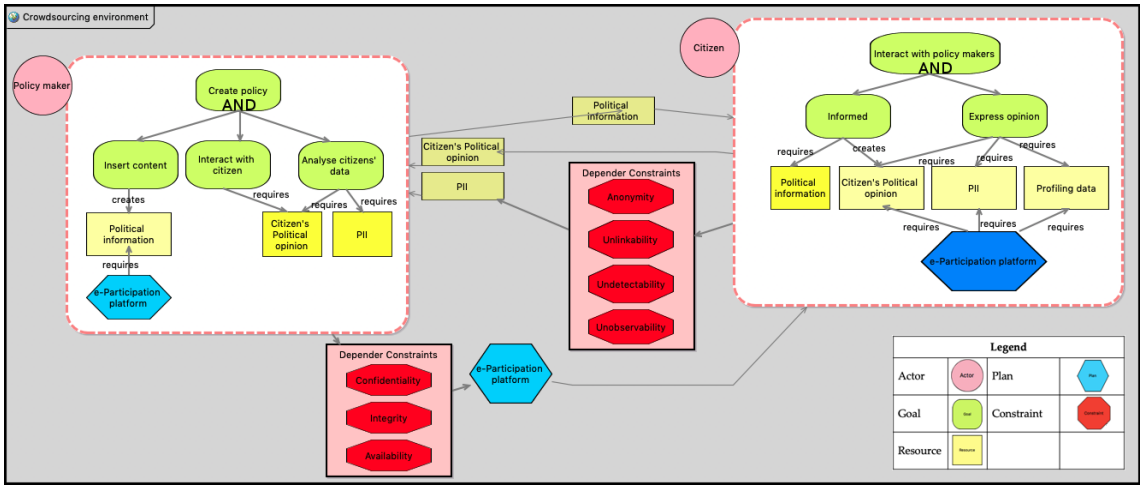

Figure 2. Crowdsourcing environment analysis.

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 employee. The best practice is to focus monitoring and measurement on the activities that are linked to the critical processes that enable the organisation 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 received 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 time required 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 the 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.

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 developed clear policies, they should have established 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. Case Study

This section presents a case study derived from the e-Participation domain, aiming at the understanding of the way the proposed method applies in such a paradigm. A pilot application of the passive crowdsourcing method, described above, was carried out, in collaboration with a governmental organisation, i.e., the Hellenic Parliament. A detailed scenario has been formed and executed in order to define how the organisation and its policy stakeholders will be able to use the method to collect knowledge and opinions on a topic of interest related with policy under formulation during the period of the pilot application. As already mentioned, the accumulated content has then undergone analysis by advanced tools in order to identify specific issues, ideas, arguments, concerns and other useful information related with the under discussion issue, contained in the citizens' text. Following the proposed method, described in Section 3, the steps have been shaped accordingly:

1. **Plan**

   - *GDPR project initiation*: All the stakeholders involved in the pilot application, including parliamentary officers, public servants, Members of the Hellenic Parliament, policy advisors

and scientific assistants of Members of the Parliament, representatives from Greek political parties have been informed, and as well as parliamentary employees responsible for the project understood and realised that the mission of the campaign should be aligned with data protection objectives. Dedicated meetings have been conducted with the aforementioned stakeholders and the privacy experts in order for the latter to understand the objectives and the way the pilot campaign should work, the responsible employees for the project, the data that will be collected, and the purpose of processing such data.

- *Commitment of the organisation*: After the initiation of the project, another meeting followed, dedicated to the discussion of the GDPR team with the higher management of the Parliament's European Programs Implementation Service (EPIS), which was the department responsible for the implementation. The aim of this meeting was to discuss any peculiarities regarding the project, the Organisation, the external third parties that have access to the Organisation's data, etc. The higher management realised the importance of the protection of citizens personal data and committed to contribute for the realisation of this project by allowing the personnel to provide to the GDPR team all the necessary information, to implement the proposed technical and organisational measures that the GDPR team will propose and to change the structure of the organisation according the to GDPR team's guidelines.
- *Organisation structure*: In order for the Parliament's European Programs Implementation Service to identify areas of concern, conduct gap analysis, implement the appropriate technical and organisational controls, the organisational structure must have already been defined, alongside the necessary changes. These changes include the appointment of the DPO, as an independent body, who directly reports to the head of the EPIS. The structure of the organisation will facilitate in assigning and communicating roles and responsibilities throughout the organisation regarding the GDPR requirements.
- *Mapping of data processing activities*: Following the template provided in Table 1, the identified processing activities are summarised below:
  - *Purpose of processing*: "Processing of data published in various Web 2.0 sources to increase Public Engagement in public policy formulation"
  - *Legal basis for processing*: User Consent to the data privacy policy of the Web 2.0 platforms (Terms and Conditions) used in the specific passive crowdsourcing application, i.e., Facebook, Twitter, blogs.
  - *Third countries*: 0 third countries were involved, as the selection of data sources was limited to Greek websites and Social Media communities
  - *Data source*: Greek Citizens
  - *Personal data categories*: 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)
  - *Receivers*: Members of the Hellenic Parliament, Policy Makers, Political Parties, NGOs
  - *Processing IT application*: Social Media platform, Third party applications
- *Elicitation of privacy requirements*: Articles around the topic of interest is published in various political sources, e.g., websites, fora, political blogs. The citizens are used to post content on the above Web 2.0 sites or the social media they interact with, and freely express their opinions on this topic. Therefore, during the pilot application, tools were used by the EPIS for searching the related content contributed by the citizens without any stimulation. Data relevant to the topic were collected, which at some times included the profiling data of the citizens who generated the content and, finally, EPIS use advanced tools to analyse the collected data in order to extract useful information, such as new ideas, concerns, directions,

alternatives, side effects, to name a few. However, data related to the ones who created that content were collected, and this information needs to be protected. By applying the Secure Tropos methodology in this case, as we see in Figure 3, we analyse the dependencies of the actors and we identify the privacy requirements. To this end, citizens' PII and citizens political opinion need to be protected, since the privacy requirements Anonymity, Unlinkability, Undetectability, and Unobservability are not satisfied.

- *Gap analysis*: This step presents a snapshot of the current state of affairs in the environment of the Parliament's European Programs Implementation Service as that existed before the implementation of the GDPR project, and serves primarily as a necessary methodological step for the rest of project's activities. After a series of interviews and discussions with the personnel responsible for the application, we were able to identify that the most important processing activity that is conducted is the "Processing of published data for Public Engagement". Regarding the current situation, we noticed that no specific security and data protection measures were taken by the organisation, especially for satisfying the identified privacy requirements. Additionally, no specific measures regarding the lawful, fair and transparent way of processing of personal data had been taken. However, these data were collected for a specified, explicit and legitimate purpose. All this information allowed us to assess that the under examination Organisation is at stage 1 (Initial stage), as they are aware of the existence of the problem, despite that they have not implemented any standardised approach towards data protection.
- *Data Protection Impact Assessment*: This step presents the risks that could be materialised by the data processing activities carried out by the Parliament's European Programs Implementation Service, regarding the processing activity carried out throughout this campaign, entitled "Processing of published data for Public Engagement", and could have an impact on the fundamental rights and freedoms of natural persons. The risks being examined are related with the *illegitimate access to data*, *unwanted modification of data* and *data disappearance*. The factors determining the risk level are the severity of the impact (which is the same as the severity of the data breach incident (feared event) that can be caused by the specific risk) and the likelihood (which is equal to the probability of occurrence of threats related to the particular feared event) of occurring. Next, each of these risks is examined.
  - Illegitimate access to data: The risk of unauthorised access to data that the organisation handles can appear in the examined processing activity due to various threats (i.e., masquerading of user identity, which can be conducted by insiders, by contracted service providers, or by outsiders, unauthorised use of an application, threats during data transmission (such as communication interception and accidental mis-routing), misuse of physical resources). The impact of this action would be the inappropriate use of citizens' personal and sensitive data for purposes other than the purpose originally set. For instance, these data can be sold to advertising companies or be used by political opponents for propaganda purposes, promoting their own directions for a topic, or using these data for the manipulation of the voters. For simplicity reasons, in Table 2, we present the aggregated table of the results of the risk assessment for this risk category.
  - Unwanted modification of data: The risk of unintended modification to the organisation's data can be realised in the examined processing activity based upon various threats. These threats are grouped according to their nature or according to the asset they exploit, including masquerading, damage to hardware, and damage to the organisation's software. The analysis of the impact of each threat takes into account the possible malfunction of the processing activities by data modification or the possible use of personal and sensitive data so that other processing activities can abuse them for their benefit. For instance, the masquerading of an Organisation user's

identity by internal or external users can lead to unwanted modification of citizens' data. If a malicious user masquerades as a legitimate user and alters the campaign's data, this action can lead to a maximum impact on the Organisation as the modification of such data can have as a result the Organisation publishing mistaken results for the public opinion. These results could guide decisions for the specific topic to an opposite direction. In Table 3, we present the aggregated table of the results of the risk assessment for this risk category.

– Data disappearance: The risk of data deletion in the passive crowdsourcing platform used during the pilot application can be realised after various threats have emerged. These threats are grouped according to their nature or according to the asset that they exploit and include masquerading, technical failure, application software failure, communication breaches, malfunction to physical resources of the Organisation. The analysis of the impact of each threat takes into account the possible malfunctioning processing and error causing through the processing of data or the possible loss of personal and sensitive data. For instance, software failure, and in particular in the Organisation's systems, can lead to the deletion of personal and sensitive data hosted on it. For example, possible errors when performing actions on the system (e.g., bugs) can lead to data being deleted. In such an incident, the Organisation will lose the data supporting their campaign, and this will cause damage to the reputation of the Organisation, making citizens loose their trust. Realisation of the above threat is expected to have a limited impact on data subjects since appropriate controls, like backup, are available. In Table 4, we present the aggregated table of the results of the risk assessment for this risk category.

Table 2. Risk category: Illegitimate access to data.

Threat	Severity	Likelihood
Masquerading	Maximum Level: 4	Negligible Level: 1
Unauthorised Use of an Application	Maximum Level: 3, 5 = 4	Negligible Level: 1
Threats during data transmission	Significant Level: 3	Negligible Level: 1
Misuse of physical resources	Significant Level: 3	Negligible Level: 1
MEAN ASSESSMENT	3, 3 = 3 Significant Level: 3	Negligible Level: 1

Table 3. Risk category: Unwanted modification of data.

Threat	Severity	Likelihood
Masquerading	Maximum Level: 4	Negligible Level: 1
Hardware Malfunction	Maximum Level: 2, 5 = 3	Negligible Level: 1
Software Malfunction	Limited Level: 2	Negligible Level: 1
MEAN ASSESSMENT	2, 8 = 3 Significant Level: 3	Negligible Level: 1

Table 4. Risk category: Data disappearance.

Threat	Severity	Likelihood
Masquerading	Maximum Level: 4	Negligible Level: 1
Technical failure	Significant Level: 3	Limited Level: 2
Application Software Failure	Limited Level: 2	Negligible Level: 1
Communications breaches	Maximum Level: 4	Limited Level: 2
Malfunction to physical resources	Significant Level: 3	Negligible Level: 1
MEAN	3, 2 = 3	1, 4 = 1
ASSESSMENT	Significant Level: 3	Negligible Level: 1

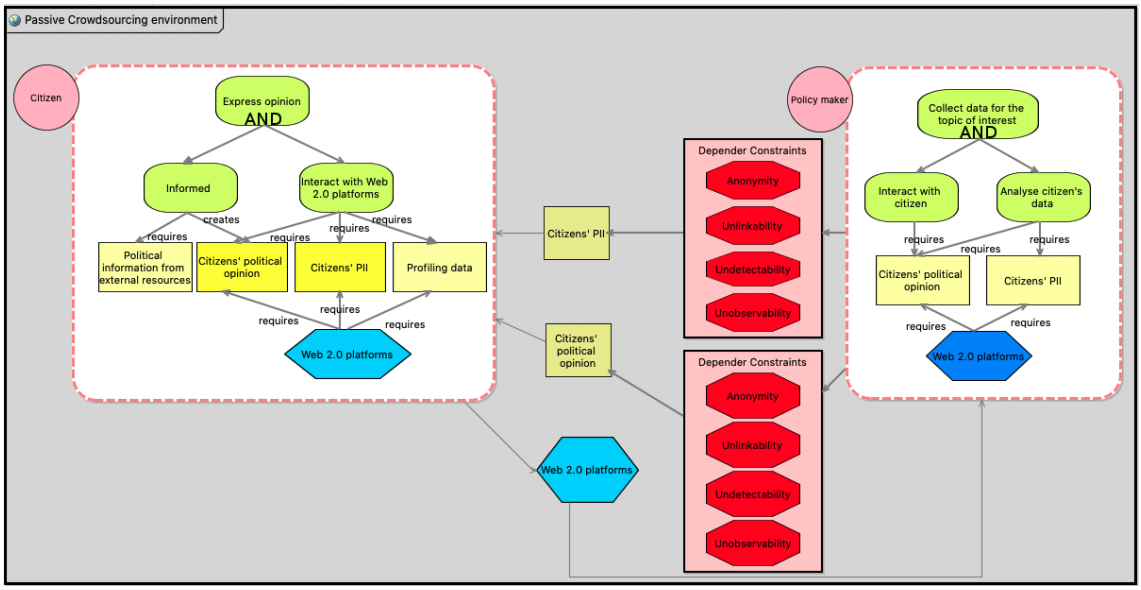

Figure 3. Passive Crowdsourcing environment analysis—privacy requirements.

2. **Do**

- *Decisions of controls and procedures*: Taking into account the results of the previous step regarding the severity and the likelihood of the three main treats that put personal data that the Organisation processes at risk, and following the recommendations of PIA-CNIL to address risks, the Organisation:
  - for the risk of the illegitimate access to data must avoid the processing activity or confront it with controls
  - for the risk of the unwanted modification of data must avoid the processing activity or confront it with controls
  - for the risk of the data disappearance must avoid the processing activity or confront it with controls

  Therefore, it is proposed that risk mitigation measures should be implemented, particularly for dealing with the masquerading of user identity. After the implementation of the proposed controls, it is expected that the risks will be minimised.
- *Implementation of controls*: The Organisation decided to confront the identified risks with appropriate controls. Hereby, in Tables 5–7, we present the data protection measures per threat per risk category.

- *Documentation management*: To keep documented information regarding the processes, the employees must follow when implementing a crowdsourcing paradigm, we developed a data protection policy that will be communicated to the employees of the Hellenic Parliament. This policy includes the purpose and the objectives set by the management with regard to the protection of personal data, as well as the instructions, procedures, rules, roles and responsibilities related to the protection of such data. Moreover, it provides strategic guidance to the organisation's management and staff for the protection of personal data when processing them.
- *Communication*: The Hellenic Parliament has decided to communicate their data protection goals by using their website, including a dedicated area for the data protection actions they follow that contains relevant educational material for their employees, as well as links to websites where internal and external users (employees, citizens, etc.) can provide feedback to the Organisation. The EPIS has further specified the data protection goals and actions targeted to such e-participation initiatives.
- *Awareness and training*: It has been decided that the Organisation must provide adequate and appropriate training to staff that use or manage the IT infrastructure or external tool such as the ones described in the current case study, in the topics of Personal Data Protection and Information Systems and Network Security, depending on the role of each employee.

3. **Check**

- *Monitoring, measurement, analysis and evaluation:* After the previous steps have been completed, we proceed in determining measurement objectives that enable Parliament's European Programs Implementation Service to achieve its data protection objectives. This process has been divided in four measurements: (i) incidents: % of false alarms through event detection, and average cost of an incident; (ii) training: % of employees who have received training, hours of training by employees; (iii) vulnerabilities: % of systems tested for vulnerabilities; and (iv) nonconformities: % of nonconformity not corrected in a specific amount of time, the time required to fix a nonconformity. Additionally, it has been decided to report the results of the analysis with the use of reports, where the employees of the organisation will have access, written in an easy-to-read format.
- *Internal audit*: The organisation shall conduct internal audit related to the GDPR. It has been decided by the higher management to adopt a continual internal audit programme. 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

4. **Act**

- *Identification of potential data breaches*: The Parliament's European Programs Implementation Service is deemed to be aware of a data breach when it is confirmed that an event that results in undermining of personal data has occurred. During the initial investigation of the incident, which must begin as soon as possible, they are not deemed to have knowledge

of the breach. Whether it is immediately clear that personal data are at stake or whether this conclusion takes some time to achieve, emphasis must be given to direct action to investigate the incident in order to determine whether there has actually been a violation of personal data. When a potential data breach occurs, and provided there is a risk for natural persons, the Organisation must inform the Greek Data Protection Authority (DPA), and if necessary, the data subjects (citizens). For timely notification, procedures that describe how the Organisation communicates with the Supervisory Authority and the information that will be communicated to them have been defined.

- *Corrective actions*: For establishing and implementing corrective actions, the Parliament's European Programs Implementation Service, should, amongst others:
  - Identify the actions for implementation
  - Attribute responsibilities to appropriate persons/roles in charge of the implementation
  - Determine the means (i.e., appropriate tools, employee training, appropriate controls and methods) for the evaluation of these actions.
- *Continual improvement*: After the GDPR compliance project is finished, the Parliament's European Programs Implementation Service is able to demonstrate that it has activated the appropriate mechanisms to continuously monitor its compliance level with the requirements of the law. Both the legal department of the organisation and the Information Systems' Lead Developer should monitor the policies and processes that have been developed and the technologies that allow continuous monitoring and assessment of security vulnerabilities.

Table 5. Data protection measures for risk category: Illegitimate access to data.

Threat	Data Protection Measures
Masquerading	Access control mechanisms: Personal Accounts, Password Use, Password Strength, Password Change Controls, Password Storage, Session ID Protection
	Data storage protection: encryption of citizens' names in databases
	Audit trails and event logs: Log and event management system
	Software/application integrity check: Implementation of an integrity checksum mechanism at file system level
	Protection of data during transmission: TLS, VPN, HSTS
Unauthorised use of an application	Access control mechanisms: Personal Accounts, Password Use, Password Strength, Password Use, Password Change Controls, Password Storage, Session ID Protection
	Secure system configuration and maintenance: webserver hardening
	Prevention mechanisms: web application firewall
Threats during data transmission	Protection of data during transmission: TLS, VPN, HSTS
Misuse of physical resources	Physical security:Perform a periodic audit for ensuring the completeness/ effectiveness/ applicability of all relevant procedures
	Deployment of an assets inventory

Table 6. Data protection measures for risk category: Unwanted modification of data.

Threat	Data Protection Measures
Masquerading	Access control mechanisms: Personal Accounts, Password Use, Password Strength, Password Change Controls, Password Storage, Session ID Protection
	Data storage protection: encryption of citizens' names in databases
	Audit trails and event logs: Log and event management system
	Software/application integrity check: Implementation of an integrity checksum mechanism at file system level
	Prevention mechanisms: antimalware software
	Secure system configuration and maintenance: webserver hardening
	Protection of data during transmission: TLS, VPN, HSTS
Hardware malfunction	Maintenance services by external partners
	Security and personal data protection training and awareness programmes
Software malfunction	Maintenance services by external partners
	Security and personal data protection training and awareness programmes
	Secure system configuration and maintenance: Webserver hardening partial; secure system and framework updates

Table 7. Data protection measures for risk category: Data disappearance.

Threat	Data Protection Measures
Masquerading	Access control mechanisms: Personal Accounts, Password Use, Password Strength, Password Change Controls, Password Storage, Session ID Protection
	Audit trails and event logs: Log and event management system
	Software/application integrity check: Implementation of an integrity checksum mechanism at file system level
	Prevention mechanisms: antimalware software
Technical failure	Maintenance services by external partners
Application software failure	Maintenance services by external partners
Communication breaches	Protection of data during transmission: VPN
Malfunction to physical resources breaches	Physical security
	Assets inventory

7. 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, and is specific, informed, affirmative and unambiguous (GDPR, Article 7).

This work aims to provide new knowledge to the ecosystem where e-Participation methods, and especially crowdsourcing environments are used. In such platforms, participants might reveal special categories of their personal data, putting their privacy at risk. Article 9 of the GDPR clearly states

that all organisations processing such data should protect it. The results of this paper provide new contributions for researchers and practitioners as follows. The main findings interest organisations conducting e-Participation activities. Public administrations undergoing GDPR assessments should choose a methodological framework in order to ensure that all the minimum requirements for the implementation of a compliance framework are covered. The proposed method is based on the well-established PDCA model, which should be adjusted to each organisation and its particular context, i.e., taking into account the corresponding requirements, the size of the organisation, its objectives, its business processes, and so on. The sequence of steps might change or merge according to the organisation's needs. Finally, due to the necessity for continuous development throughout the compliance project, many of the presented processes in the proposed method can be iterative, such as the communication plan and the training of the involved employees.

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 a privacy requirements' perspective, in order to identify potential threats that these systems have, any vulnerabilities that might have an impact on the resources of the system, and finally be able to propose specific countermeasures in order to mitigate such risks. Finally, this work can be further enhanced by providing technical aspects of the proposed solution aiming at providing a detailed architectural framework containing all required functionalities and procedures for addressing the various aspects of the PDCA model in crouwdsourcing environments.

Author Contributions: V.D. and A.A. conceived the presented idea and designed the study. V.D. investigated the General Data Protection Regulation and formulated the method to be followed in order for an organisation to reach compliance with the Regulation. A.A. developed the theoretical background regarding the e-Participation methods and investigated the exposed data that must be protected. S.G. contributed to the design of the applied method. S.G. and Y.C. were involved in the planning and supervised the work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

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
TLS	Transport Layer Security
VPN	Virtual Private Network
HSTS	HTTP Strict Transport Security
EPIS	Parliament's European Programs Implementation Service

References

1. Spiekermann, S.; Acquisti, A.; Böhme, R.; Hui, K.L. The challenges of personal data markets and privacy. *Electron. Mark.* **2015**, *25*, 161–167. [CrossRef]
2. Acquisti, A.; Gritzalis, S.; Lambrinoudakis, C.; di Vimercati, S. *Digital Privacy: Theory, Technologies, and Practices*; CRC Press: Boca Raton, FL, USA, 2007.
3. Lash, S.; Szerszynski, B.; Wynne, B. *Risk, Environment and Modernity: Towards a New Ecology*; Sage: Newcastle upon Tyne, UK, 1996; Volume 40.
4. As-Saber, S.; Hossain, K.; Srivastava, A. Technology, society and e-government: In search of an eclectic framework. *Electron. Gov. Int. J.* **2007**, *4*, 156–178.
5. Medaglia, R. eParticipation research: Moving characterization forward (2006–2011). *Gov. Inf. Q.* **2012**, *29*, 346–360. [CrossRef]
6. Susha, I.; Grönlund, Å. eParticipation research: Systematizing the field. *Gov. Inf. Q.* **2012**, *29*, 373–382. [CrossRef]
7. Diamantopoulou, V.; Androutsopoulou, A.; Gritzalis, S.; Charalabidis, Y. An assessment of privacy preservation in crowdsourcing approaches: Towards GDPR compliance. In Proceedings of the 2018 12th International Conference on Research Challenges in Information Science (RCIS), Nantes, France, 29–31 May 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. *Comput. Hum. Behav.* **2011**, *27*, 2233–2242. [CrossRef]
9. Mitrou, L. *Law in the Information Society*; Sakkoulas Publications: Athens, Greek, 2002.
10. Mitrou, L. *General Data Protection Regulation: New Law–New Obligations–New Rights*; Sakkoulas Publications: Athens, Greek, 2017.
11. Solove, D.J. A taxonomy of privacy. *Univ. Pa. Law Rev.* **2005**, *154*, 477. [CrossRef]
12. Islam, M.B.; Watson, J.; Iannella, R.; Geva, S. *What I Want for My Social Network Privacy*; NICTA: Sydney, Australia, 2014.
13. Newburn, T.; Jones, T. *Private Security and Public Policing*; Clarendon Press: Oxford, UK, 1998.
14. Marx, G.T. Murky conceptual waters: The public and the private. *Ethics Inf. Technol.* **2001**, *3*, 157–169. [CrossRef]
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. Law Rev.* **2012**, *126*, 1904.
17. Warren, S.D.; Brandeis, L.D. Right to privacy. *Harv. Law Rev.* **1890**, *4*, 193. [CrossRef]
18. Westin, A.F. Privacy and freedom. *Wash. Lee Law Rev.* **1968**, *25*, 166.
19. Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*; Cole Publishing Company: Monterey, CA, USA, 1975.
20. Conger, S.; Pratt, J.H.; Loch, K.D. Personal information privacy and emerging technologies. *Inf. Syst. J.* **2013**, *23*, 401–417. [CrossRef]
21. Mohamed, N.; Ahmad, I.H. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Comput. Hum. Behav.* **2012**, *28*, 2366–2375. [CrossRef]
22. Gritzalis, S. Enhancing web privacy and anonymity in the digital era. *Inf. Manag. Comput. Secur.* **2004**, *12*, 255–287. [CrossRef]
23. Cavoukian, A. *Privacy by Design: The 7 Foundational Principles*; Information and Privacy Commissioner of Ontario: Toronto, ON, Canada, 2009; Volume 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: Boston, MA, USA, 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. *Int. J. Electron. Gov.* **2017**, *9*, 361–384. [CrossRef]
26. Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. [CrossRef]

27. Diamantopoulou, V.; Tsohou, A.; Karyda, M. General Data Protection Regulation and ISO/IEC 27001: 2013: Synergies of Activities Towards Organisations' Compliance. In Proceedings of the International Conference on Trust and Privacy in Digital Business, Linz, Austria, 26–29 August 2019; Springer: Cham, Switzerland, 2019; pp. 94–109.
28. 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)*; Publications Office of the European Union: Luxembourg, 2016.
29. 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; European Data Protection Board: Brussels, Belgium, 2019.
30. ISACA. *GDPR: The end of the Beginning*; Technical Report; ISACA: Rolling Meadows, IL, USA, 2018.
31. Thomson Reuters 2019. *Study Finds Organizations Are Not Ready for GDPR Compliance Issues*; Technical Report; 2019. Available online: https://legal.thomsonreuters.com/en/insights/articles/study-finds-organizations-not-ready-gdpr-compliance-issues (accessed on 9 July 2019).
32. IAAP. *Privacy Tech Vendor Report*; Technical Report; IAPP: Portsmouth, NH, USA, 2018.
33. Bernstein, M.; Chi, E.H.; Chilton, L.; Hartmann, B.; Kittur, A.; Miller, R.C. Crowdsourcing and human computation: Systems, studies and platforms. In Proceedings of the CHI'11 Extended Abstracts on Human Factors in Computing Systems, Vancouver, BC, ACM: New York, NY, USA, 2011; pp. 53–56.
34. Varshney, L.R. Privacy and reliability in crowdsourcing service delivery. In Proceedings of the 2012 Annual SRII Global Conference (SRII), San Jose, CA, USA, 24–27 July 2012; pp. 55–60.
35. Kajino, H.; Arai, H.; Kashima, H. Preserving worker privacy in crowdsourcing. *Data Mini. Knowl. Discov.* **2014**, *28*, 1314–1335. [CrossRef]
36. Schoßböck, J.; Terbu, O.; Sachs, M.; Leitner, M.; Heussler, V.; Wenda, G.; Bonitz, A.; Hötzendorfer, W.; Parycek, P.; Vogl, S.; et al. Inclusion and privacy in E-participation platform design. *Innov. Public Sector. Electron. Gov. Electron. Particip.* **2016**, *23*, 51–58.
37. da Silva, M.; Viterbo, J.; Bernardini, F.; Maciel, C. Identifying Privacy Functional Requirements for Crowdsourcing Applications in Smart Cities. In Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 9–11 November 2018; pp. 106–111.
38. Ayalon, O.; Toch, E. Crowdsourcing privacy design critique: An empirical evaluation of framing effects. In Proceedings of the 51st Hawaii International Conference on System Sciences, Waikoloa Village, HI, USA, 2–6 January 2018.
39. Moen, R.; Norman, C. Evolution of the PDCA cycle, 2006. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.5465&rep=rep1&type=pdf (accessed on 9 July 2019).
40. ISO/IEC. *ISO 27001:2013 Information Technology–Security Techniques–Information Security Management Systems–Requirements*; Technical Report ISO: Cham, Switzerland, 2013.
41. ISO/IEC. *ISO 27002:2013 Information Technology–Security Techniques–Code of Practice for Information Security Controls*; Technical Report ISO: Cham, Switzerland, 2013.
42. ISO/IEC. *ISO 27014:2013 Information Technology–Security Techniques–Governance of Information Security*; Technical Report ISO: Cham, Switzerland, 2013.
43. ISO/IEC. *ISO 27701:2019 Security Techniques–Extension to ISO/IEC27001 and ISO/IEC27002 for Privacy Information Management–Requirements and Guidelines*; Technical Report ISO: Cham, Switzerland, 2019.
44. ISO/IEC. *ISO 27004:2016 Information Technology–Security Techniques–Information Security Management–Monitoring, Measurement, Analysis and Evaluation*; Technical Report ISO: Cham, Switzerland, 2016.
45. ISO/IEC. *ISO 27005:2018 Information Technology–Security Techniques–Information Security Risk Management*; Technical Report ISO: Cham, Switzerland, 2018.
46. ISO/IEC. *ISO 31000:2018 Risk Management—Guidelines*; Technical Report ISO: Cham, Switzerland, 2018.
47. ISO/IEC. *ISO 29100:2011 Information Technology–Security Techniques–Privacy Framework*; Technical Report ISO: Cham, Switzerland, 2011.
48. Working Party 29. *Guidelines on Data Protection Impact Assessment*; Technical Report ISO: Cham, Switzerland, 2019.
49. CNIL 2018. *Privacy Impact Assessment (PIA)–Knowledge Bases*; Technical Report CNIL: Paris, France 2018.

50. Krasnova, H.; Kolesnikova, E.; Guenther, O. "It won't happen to me!": Self-disclosure in online social networks. *AMCIS 2009 Proc.* **2009**, 343.
51. Fischer-Hübner, S. *IT-security and Privacy: Design and Use of Privacy-enhancing Security Mechanisms*; Springer: Berlin/Heidelberg, Germany, 2001.
52. Cannon, J. *Privacy: What Developers and IT Professionals Should Know*; Addison-Wesley Professional: Boston, MA, USA, 2004.
53. Pfitzmann, A.; Hansen, M. A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. 2010. Avalable online: http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf (accessed on 17 February 2020).
54. Wright, D.; De Hert, P. Introduction to privacy impact assessment. In *Privacy Impact Assessment*; Springer: Dordrecht, The Netherlands, 2012; pp. 3–32.
55. ICO. *Privacy Impact Assessment Handbook, Wilmslow, Cheshire, UK, Version 1.0*; Trilateral Research and Consulting, Technical Report; ICO: Wilmslow, UK, 2007.
56. European Commission *A Privacy Impact Assessment Framework for Data Protection and Privacy Rights*; Technical Report ISO: Cham, Switzerland, 2012.
57. ISO/IEC. *ISO FDIS 29134 Information Technology–Security Techniques–Privacy Impact Assessment–Guidelines*; Technical Report ISO: Cham, Switzerland, 2017.
58. ISO/IEC. *ISO/IEC 29151 Information Technology–Security Techniques–Code of Practice for Personally Identifiable Information Protection*; Technical Report ISO: Cham, Switzerland, 2017.
59. Macintosh, A. Characterizing e-participation in policy-making. In Proceedings of the IEEE, 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2004; p. 10.
60. Loukis, E.; Xenakis, A.; Peters, R.; Charalabidis, Y. Using Gis Tools to Support E_Participation–A Systematic Evaluation. In Proceedings of the International Conference on Electronic Participation, Lausanne, Switzerland, 29 August–2 September 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 197–210.
61. 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: Edinburgh, UK, 2016.
62. 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; European Commission: Brussels, Belgium, 2006.
63. Caddy, J.; Gramberger, M.; Vergez, C. *Citizens as Partners: Information, Consultation and Public Participation in Policy-making*; OECD: Paris, France, 2001.
64. Loukis, E.; Macintosh, A.; Charalabidis, Y. *E-Participation in Southern Europe and the Balkans: Issues of Democracy and Participation Via Electronic Media*; Routledge: Abingdon, UK, 2013.
65. Charalabidis, Y.; Loukis, E. Transforming government agencies'approach to eparticipation through efficient exploitation of social media. In Proceedings of the Conference: 19th European Conference on Information Systems, ECIS 2011, Helsinki, Finland, 9–11 June 2011.
66. Desouza, K.C.; Smith, K.L. Big data for social innovation. *Stanf. Soc. Innov. Rev.* **2014**, *12*, 38–43.
67. Charalabidis, Y.; Loukis, E.; Androutsopoulou, A. Fostering social innovation through multiple social media combinations. *Inf. Syst. Manag.* **2014**, *31*, 225–239. [CrossRef]
68. Brabham, D.C. *Crowdsourcing*; Mit Press: Cambridge, MA, USA, 2013.
69. Androutsopoulou, A.; Karacapilidis, N.; Loukis, E.; Charalabidis, Y. Towards an integrated and inclusive platform for open innovation in the public sector. In Proceedings of the International Conference on e-Democracy, Athens, Greece, 14–15 December 2017; Springer: Cham, Switzerland, 2017; pp. 228–243.
70. Hilgers, D.; Ihl, C. Citizensourcing: Applying the concept of open innovation to the public sector. *Int. J. Public Particip.* **2010**, *4*, 67–88.
71. Clark, B.Y.; Zingale, N.; Logan, J.; Brudney, J. A framework for using crowdsourcing in government. In *Social Entrepreneurship: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 405–425.

72. Charalabidis, Y.; Karkaletsis, V.; Triantafillou, A.; Androutsopoulou, A.; Loukis, E. Requirements and Architecture of a Passive Crowdsourcing Environment. In *Electronic Government and Electronic Participation-Joint Proceedings of Ongoing Research of IFIP EGOV and IFIP ePart 2035*, Gesellschaft für Informatik e.V.: Bonn, Germany, 2013.
73. Androutsopoulou, A.; Mureddu, F.; Loukis, E.; Charalabidis, Y. Passive expert-sourcing for policy making in the European Union. In Proceedings of the International Conference on Electronic Participation, Guimarães, Portugal, 5–8 September 2016; Springer: Cham, Switzerland, 2016, pp. 162–175.
74. Aitamurto, T. *Crowdsourcing for Democracy: A New era in Policy-making*; Publications of the Committee for the Future, Parliament of Finland 1/2012: Helsinki, Finland, 2012; Volume 1.
75. Christensen, H.S.; Karjalainen, M.; Nurminen, L. What does crowdsourcing legislation entail for the participants? The Finnish case of Avoin Ministeriö. In Proceedings of the Internet, Policy and Politics Conferences, University of Oxford, Oxford, UK, 25–26 September 2014.
76. Lironi, E. Potential and Challenges of E-participation in the European Union. In *Study for the AFCO Committee, Director General of Internal Policies*; European Parliament: Brussels, Belgium, 2016.
77. Mouratidis, H. Secure software systems engineering: The Secure Tropos approach. *JSW* **2011**, *6*, 331–339. [CrossRef]
78. 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. *Comput. Stand. Interfaces* **2014**, *36*, 759–775. [CrossRef]
79. Diamantopoulou, V.; Mouratidis, H. Applying the physics of notation to the evaluation of a security and privacy requirements engineering methodology. *Inf. Comput. Secur.* **2018**, *26*, 382–400. [CrossRef]
80. Pattakou, A.; Kalloniatis, C.; Gritzalis, S. Security and privacy requirements engineering methods for traditional and cloud-based systems: A review. *CLOUD COMPUTING 2017* **2017**, *155*, 145–151.
81. Diamantopoulou, V.; Kalloniatis, C.; Gritzalis, S.; Mouratidis, H. Supporting Privacy by Design Using Privacy Process Patterns. In Proceedings of the IFIP International Conference on ICT Systems Security and Privacy Protection, Rome, Italy, 29–31 May 2017; Springer: Cham, Switzerland, 2017; pp. 491–505.
82. Diamantopoulou, V.; Argyropoulos, N.; Kalloniatis, C.; Gritzalis, S. Supporting the design of privacy-aware business processes via privacy process patterns. In Proceedings of the 2017 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, UK, 10–12 May 2017; pp. 187–198.
83. ISO. *10015:1999 Quality Management–Guidelines for Training*; Technical Report ISO: Cham, Switzerland, 1999.