Study on Online Collection Systems and technical specifications pursuant to ECI Regulation 211/2011 and Implementing Regulation 1179/2011

Final Assessment Report

everis
September 2017

EUROPEAN COMMISSION

European Commission
B-1049 Brussels

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The European Citizens' Initiative (ECI), as defined by both the ECI Regulation (EU) 211/2011 and the Implementing Regulation (EU) 1179/2011 for the Online Collection Systems in the context of the ECI, came into application on 1 April 2012. Since then, the procedure for collecting signatures online required organisers to put in place an online collection system that enables them to collect and store the statements of support (SoS) before sending them to the competent authorities in the verification phase. Furthermore, in order to be able to collect SoS online, organisers had also to obtain the certification of their system by the Member State in which the data will be stored.

In accordance with the ECI Regulation, the Commission has developed, maintains and improves an open source online collection software, offered free of charge to organisers of ECIs. This software provides a set of functionalities to securely collect statements of support online, store the signatories' data and export them for submission to the competent national authorities. The administration interface enables organisers to configure their system, monitor the number of statements of support received and request the export and transfer of data to competent authorities, while the public interface includes the electronic form of the statement of support to support an initiative. The organisers can use this software as a basis for their system or another one of their choice.

Bearing in mind the substantial difficulties faced by organizers, the Commission has provided a hosting environment in DIGIT data centre in Luxembourg. In the meantime, various challenges regarding online collection of SoS have been highlighted in a number of studies. Besides, the upcoming GDPR legislation (and its counterpart for EU Institutions) will also have some implications.

All these elements have been taken into consideration in this study, which aims at providing recommendations for the improvement of the ECI Regulation and related Implementing Regulation (EU) 1179/2011.

In the scope of the study, three possible scenarios have been identified for the improvement of the online collection process of SoS considering a potential revision of the ECI legislative framework and the evolution of the situation in regards to technology and security threats:

1. Update of the original scenario foreseen in the ECI Regulation, where the online collection of statements of support is done via individual online collection systems under the responsibility of the organisers (scenario 1);
2. A specific case of the online collection systems based on the Commission online collection software and the Commission hosting service (scenario 2);
3. A Commission-run centralised online collection platform (scenario 3).

The scenarios were analysed and assessed based on the criteria identified from everis suggested approach and methodology according to five aspects - legal, business, technical, security and costs. This study also focused on the potential benefits, weaknesses, opportunities and threats of the three scenarios for the online collection process.

A key feature of the online collection system is that it stores personal data and thus requires compliance with legal and technical requirements, including strict security and confidentiality measures. The administration and management of SoS in both the process of collection and submission to the competent national authorities also have to comply with security measures.

Taking into consideration the changes new data protection rules establish (General Data Protection regulation (EU) 2016/679 shall apply from 25 May 2018 and the Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies is also under revision), there are several implications for the processing of personal data in the context of the ECI.

The extension of liabilities to data processors in addition to data controllers under the new data protection rules introduces a shared responsibility between the two. This novelty offers the possibility to reduce the burden and the responsibility of ECI organisers for the personal data processed to a greater or lesser extent under each of the scenarios considered.

The certification of the online collection system and the verification of the collected SoS are the main aspects for organisational improvement. Both scenarios 2 and 3 would facilitate the suppression of the certification and provide significant improvement of the verification, benefiting from the EU File Sharing Service, which allows secure and efficient transmission of SoS directly to competent authorities. In addition to these features, scenario 3 could provide the integration of Central Authentication Service, providing a possibility to streamline the registration of a SoS once a signatory has fulfilled all required personal data.

From a technical point of view, scenario 3 provides the best technical performance and has various advantages over scenarios 1 and 2, especially by contributing to reducing the maintenance and operational efforts and by allowing faster and easier integration of technological evolutions.

Security-wise, the main advantages of scenario 3 are stability, compliance and better management of possible security breaches (physical or logical). This scenario would allow to transfer responsibilities from the organisers to the European Commission, making sure the online collection system is compliant with the Regulation, and the data collection and storage is done appropriately. However, although this solution will reduce the risk of security breaches, the impact of such risk if realised, would be potentially much higher in the case of scenario 3 in comparison to 1 and 2, as it may concern potentially data collected in support of several different initiatives.

Costs-wise, over a period of five years, only scenario 1 performs better than the AS IS situation and could be a viable option at short term. However, scenario 3 offers the most efficient use of the budget in a long term perspective as it offers several additional features such as the OCR reader and the integration with the Register and eIDAS, which are expected to contribute positively to the success of the new version of the online collection system.

In brief, everis has concluded that scenario 3 would be the best option, in particular for organisers of initiatives and citizens supporting ECIs. It represents the best value for money in terms of economy, efficiency and effectiveness. This scenario would contribute to the improvement and facilitation of the collection and verification of signatures for SoS, while simultaneously complying with necessary legal, organisation, technical and security requirements. It is the most promising scenario and the most-forward looking from the potential evolutions of the online collection system identified at the moment.

1 INTRODUCTION

The European Citizens' Initiative (ECI) is one of the major innovations introduced by the Lisbon Treaty[1] and aims at involving citizens more closely in agenda-setting at EU level. The rules and procedures concerning the European citizens' initiative are set out in Regulation (EU) No 211/2011 (the ECI Regulation, hereinafter: the Regulation)[2], which was adopted by the European Parliament and the Council in February 2011 and entered into application on 1 April 2012.

Both the ECI Regulation (EU) 211/2011 and the Implementing Regulation (EU) 1179/2011 set out the conditions, legal requirements and technical specifications for the online collection system in the context of the ECI. The online collection system is intrinsically linked to the collection of signatures as this is a prerequisite for organisers to collect the statements of support (SoS) online.

Once the registration of the initiative is confirmed, organisers have twelve months to collect one million signatures, both on paper and online, through an online collection system certified by the Member State where the data are stored.

In accordance with the ECI Regulation, the Commission has developed, maintains and improves an open source online collection software, offered free of charge to organisers of ECIs. This software provides a set of functionalities to securely collect statements of support online, store the signatories' data and export them for submission to the competent national authorities. The administration interface enables organisers to configure their system, monitor the number of statements of support received and request the export and transfer of data to competent authorities, while the public interface includes the electronic form of the statement of support to support an initiative. The organisers can use this software as a basis for their system or another one of their choice.

As organisers have been facing substantial difficulties to find appropriate hosting providers, the Commission provided servers of its own in Luxembourg, temporarily offered free of charge to the organisers. Later, the European Commission committed itself to continue its hosting practice for free as long as needed[3]. As the Commission’s data centres are located in Luxembourg, according to the ECI Regulation, organisers using the Commission's hosting offer have to request the certification of their online collection system (see sections 4.3.2, 5.3.2 and 6.3.2) to the Luxembourgish competent authority.

Some of the challenges regarding the online collection of statements of support, described and analysed in previous studies, are linked to a number of technical and security aspects. Article 6 of the Regulation states that the Online Collection System should have adequate security and technical features to guarantee data security and protection. It has to be ensured that personal data is securely collected and stored. Therefore, the improvements of the Technical Specification and, if necessary, the Regulation, are considered as potential options to improve, facilitate and simplify the online collection process.

This study assesses three different scenarios for the process of online collection of statements of support, considering a potential revision of the ECI legislative framework and the evolution of the situation in regards to technology and security threats:

[1] Article 11(4) of the Treaty on European Union and Article 24 of the Treaty on the Functioning of the European Union

[2] Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative (OJ L 65/1, 11.03.2011)

[3] http://ec.europa.eu/citizens-initiative/public/hosting

1. Update of the original scenario foreseen in the ECI Regulation, where the online collection of statements of support is done via individual online collection systems under the responsibility of the organisers (scenario 1);
2. A specific case of the online collection systems based on the Commission online collection software and the Commission hosting service (scenario 2);
3. A Commission-run centralised online collection platform (scenario 3).

This assessment also takes into consideration the provision of the new data protection Regulation (GDPR – Regulation (EU) 2016/679). The GDPR was approved on 14 April 2016 and shall enter into application on 25 May 2018. This Regulation replaces the Data Protection Directive 95/46/EC and aims at harmonising data privacy laws across Europe, protecting EU citizens' personal data, empowering them to take control of the use of their data, and reshaping the way organisations across the EU approach data privacy. Its objective is to protect the rights of the people who are sharing their personal data. In the scope of this study, it is about the protection of the signatories' rights.

From a technical point of view, the online collection system requires a number of specific features and characteristics. Those apply to the design of the application, the database and the infrastructure architecture, as well as to the business processes: certification of the online collection system software and hosting, extraction of the statements of support from the online collection system and transmission of those statements of support to the verifying authority.

Storing personal data in the online collection system has an impact not only from a legal perspective, but also from a technical requirements perspective, including strict requirements for security and confidentiality. Any online collection system should have adequate security features in order to ensure, inter alia, that the data are securely collected, stored, and processed. Moreover, those security measures are necessary to guarantee the identity of the signatory and prevent the risk of an intentioned attack (or fraud) from the outside or from the inside. It is also essential to meet the security needs in the administration and management of the statements of support collected by organisers and in the process of submission of those statements of support to the competent national authorities.

1.1 OBJECTIVES AND SCOPE

This analysis covers the assessment of the three above-mentioned scenarios:

- Scenario 1: update of the original scenario foreseen in the current ECI Regulation, where the online collection of statements of support is completed via individual online collection systems, under the responsibility of the organisers, based on the evolution of technology and security risks;
- Scenario 2: Specific case of the online collection systems where only the online collection software and hosting service provided by the Commission are used;
- Scenario 3: Setting up a centralised online collection platform provided and operated by the European Commission.

The study is carried out from a legal, organisation, technical, security and costs perspective for each scenario. Figure 1 illustrates the different layers of the scenario analysis.

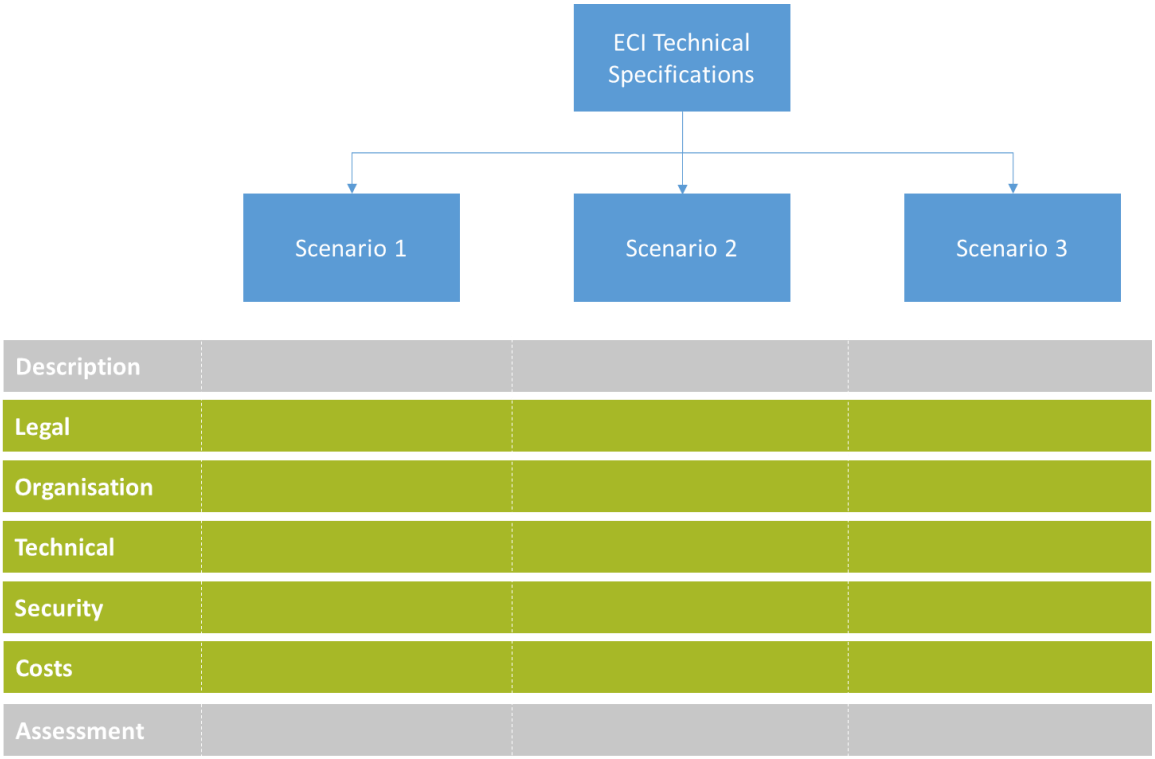


Figure 1: Breakdown of scenario analysis

Correspondingly, each scenario analysis breaks down into:

- A short description of the scenario;
- A summary of the main findings of the legal, organisation, technical, security and costs analysis.

Then, an evaluation and comparison of the three scenarios, based on the evaluation criteria, is performed in order to determine their main strengths and weaknesses.

Consequently, the objective of the study is twofold:

1. to assess the three identified scenarios, the impact of additional features such as the EU File Sharing Service and provide a high-level IT architecture;
2. to propose recommended changes or improvements to ECI Regulation (EU) 211/2011 and Implementing Regulation (EU) 1179/2011, which would make the online collection of statements of support easier, more efficient and fit for purpose.

1.2 STRUCTURE OF THE STUDY

The sequence of activities of the study is portrayed in Figure 2.

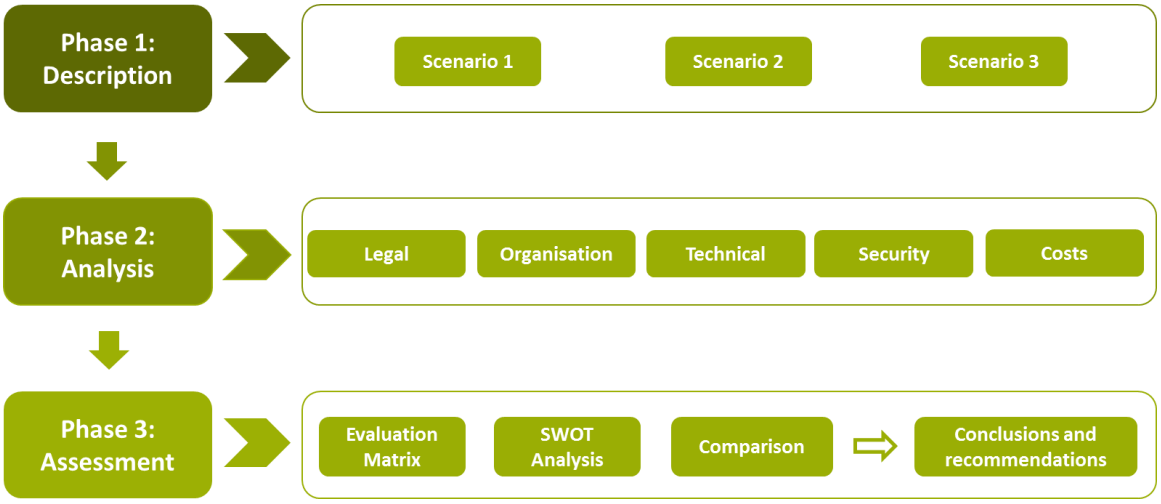


Figure 2: Sequence of the processes

Everis structured the report as follows:

- Chapter 2 states everis' approach to achieve the objectives following the three layers structure (Figure 2) and presents the methodology used throughout the study;
- Chapter 3 goes through the main components of the online collection systems that will be analysed in this study;
- Chapter 4 describes and assesses the scenario 1. In addition, it provides the proposed adaptations to the ECI legislation under this scenario;
- Chapter 5 describes and assesses the scenario 2. In addition, it provides the proposed adaptations to the ECI legislation under this scenario;
- Chapter 6 describes and assesses the scenario 3. In addition, it provides the proposed adaptations to the ECI legislation under this scenario;
- Chapter 7 evaluates and compares the three scenarios;
- Chapter 8 provides the main conclusions drawn by everis, based on the key findings;
- Chapter 9 lists all the references used in this report;
- Chapters 10 and beyond provides support material and supplementary information in appendix.

2 APPROACH AND METHODOLOGY

2.1 APPROACH

The first phase of the analysis consists of data collection by using various desk research techniques. The information collected during the study on the use of Electronic Identification (eID) for the European Citizens' Initiative is reused where relevant, in particular the information about the Commission' Online Collection Software requirements and architecture.

In the second phase, evaluation criteria are defined to guide the analysis of the three scenarios. Based on the findings of the analysis, the scenarios are then evaluated, and conclusions and recommendations are drawn. Finally, a summary of the adaptations required in the Implementing Regulation (EU) 1179/2011 and its Annex for each scenario was drafted in order to highlight the key technical aspects to take into consideration in the future.

Figure 3: Components of the study

To assess each scenario for the process of online collection of statements of support, the study consists of five main elements. Each scenario is analysed from (i) legal, (ii) organisation, (iii) technical, (iv) security, and (v) costs points of view. In the end, a comparative analysis based on identified scenarios' benefits, constraints (SWOT analysis) and the evaluation matrix of the three scenarios are presented, and final conclusions are drawn.

Legal analysis:

The legal analysis consists of a legal assessment of each scenario, based on the current ECI Regulation and Implementing Regulation (EU) 1179/2011, as well as on the new data protection

Regulation (Regulation (EU) 2016/679). The objective is to identify necessary or potential changes to ECI legislative framework.

In respect to the ECI Regulation, the particular emphasis is given to Article 6, paragraphs 1 to 4, providing implementation requirements of the online collection system.

Methods applied: desk research, legal analysis, analytical method, micro analysis of a legal rule, case analysis, qualitative analysis.

Organisation analysis:
The organisation analysis elaborates on key criteria that may lead to modifications of the business processes and are likely to impact the stakeholders: convenience for ECI organisers, certification of the online collection system and verification of the statements of support by verifying authorities.

Methods applied: desk research, analytical method, document analysis, qualitative analysis, use case.

Technical analysis:
The technical analysis is based on the assessment of two different criteria: implementation (ease of implementation of the online collection system application and infrastructure, scalability, and maintainability), and operations (ease of setting up an instance of the online collection system for a new ECI, system administration needs during the lifetime of an ECI and ease of transmission of the results to the verifying authorities).

Methods applied: desk research, analytical method, document analysis, qualitative and quantitative analysis, use case.

Security analysis:
This analysis provides a security assessment for each scenario, based on four main criteria: security architecture, software development security, data security & integrity and finally, identity and access management; based on IT security best practices and standards.

Methods applied: risk assessment and security standards & best practices (mainly ISO/IEC 27001 and 27002, OWASP, Cloud Security Alliance, etc.).

Costs analysis:
The cost impact of each scenario is assessed separately for other criteria. It focuses on the costs of the IT solutions as well as on the efforts that each scenario requires from the different stakeholders.

Methods applied: cost-benefit analysis, estimation techniques

Evaluation & conclusions
The scenarios are evaluated and compared, covering the main aspects of the SWOT analysis and the evaluation matrix. Then, final conclusions are drawn.

Methods applied: Evaluation matrix criteria, SWOT, analytical method, comparative analysis

2.2 METHODS AND TECHNIQUES

The identification of the methodology is strongly influenced by the multifaceted nature of the analysis, in order to cover the legal, organisation, technical, security and costs aspects of the three scenarios.

Document Analysis: The identification of relevant sources regarding the ECI is the main output of desk research. During this phase, documents, including the legal frameworks, are analysed to gather data and information related to the study.

Business process analysis: The business processes illustrate and describe the sequences of interactions between the various stakeholders along the process. To ease the understanding of the impact of each proposed scenario, business processes where the impact of each scenario differs are identified and described in detail.

Benchmarking: The evaluation of each scenario is structured along five dimensions: legal, organisation, technical, security and costs. In order to evaluate each scenario against these domains, a set of evaluation criteria is developed. Each criterion addresses a specific element that needs to be considered during the analysis. Then, the benchmarking analyses the various scenarios based on two methods: **Evaluation Matrix** and **SWOT analysis**.

Evaluation Matrix

To develop the Evaluation Matrix for each scenario, the following steps are followed:

1. Based on the five identified domains, a list of evaluation criteria, which allows to determine the level of fulfilment of each scenario, is developed.
2. A score is assigned to each evaluation criterion. A weakness is represented by a low score (1 or 2) while benefits or strengths are represented by a high score (4 or 5). A TO BE situation similar to the AS IS situation will usually get a median score of 3.
3. By summing the scores of all the criteria, the total resulting score of the scenario is obtained.

The score of each evaluation criterion can vary from 1 to 5. It is calculated based on a comparison between the ideal situation defined for each criteria and the current situation. The closer the situation in a scenario is from the ideal one, the better the score. The five different domains are equally important and therefore have the same weight when calculating the final score of each scenario.

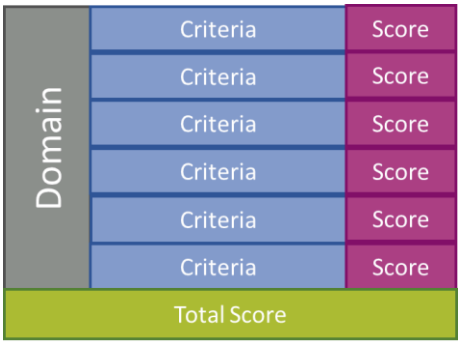


Figure 4: Evaluation Matrix

Figure 5: SWOT Analysis

SWOT Analysis

The SWOT analysis focuses on the strengths, weaknesses, opportunities and threats of each scenario. It aims at identifying the criteria influencing, in a helpful or harmful way, a scenario.

When conducting a SWOT analysis, the aim is to list, within the table, all the identified influencing factors. The final objective being to identify the impact of the different evaluation criteria on each scenario.

The above-mentioned evaluation criteria, selected for both the Evaluation Matrix and the SWOT Analysis methods, as well as their respective domains, are listed as follows:

Domain	Criteria	Description
Legal	Impact of GDPR	Assessment of GDPR impact on each stakeholder
	Impact on liabilities	Impact of the envisaged changes to the Regulation on the liabilities of each stakeholder
Organisation	Convenience	Convenience of each scenario, from a usability and administration perspective
	Certification	Impact of the implementation of each scenario on the certification process
	Verification	Impact of the implementation of each scenario on the verification process
Technical	Implementation	Assessment of the resources and infrastructure (hardware and software) needed to implement, certify and maintain the online collection system during its lifecycle under each scenario
	Operations	Impact of the scenario on the operational processes of each stakeholder
Security	Security Architecture	Assessment of the security of the systems infrastructure: security requirements for physical location, network infrastructure, security perimeter and server environment.
	Software development security	Assessment of the security requirements of the code involved in the collection of the statements of support to avoid security vulnerabilities.
	Data security & integrity	Assessment of the storage and protection security mechanisms that prevent the accidental destruction/alteration or unauthorised disclosure/access to personal data.
	Identity & Access Management	Assessment of the mechanisms ensuring a proper identification and authentication management of the different types of users (signatories and administrators)
Costs	Commission	Costs of infrastructure (capacity on (virtual) servers, operating systems and base software) and human resources (qualified professionals required to operate the online collection system) for the Commission
	Organisers	Costs of infrastructure and human resources for Organisers

Table 1: Description of the evaluation criteria

3 OVERVIEW OF THE MAIN COMPONENTS

3.1 LAYERS OF AN APPLICATION

Modern web-applications are usually built in three layers, taking advantage of the reusability of the modules of the same layer of other applications. Those layers are:

- **The presentation layer**, also called front-end, in charge of the user interface. It includes, on one hand, the screens and the visual elements that the user will see – header, footer, images, background, fonts, styles, etc. – and, on the other hand, the basic checks performed on the data entered by the user, such as dates or fields with a limited set of allowed values (i.e., gender (M/F), nationality, etc.).

  Some parts of this layer are often implemented in a "MVC" (Model, View, Controller) handler, such as Struts or Spring. This kind of framework also facilitates the management of the sessions, including the hibernation mechanism, temporarily storing session data and recovering them when they need to be activated.

- **The application layer**, also called business logic, determines the behaviour of the application; including the checks on the business rules. It also determines the data to be presented to the user.

- **The data layer**, including the Database Management System, and the accesses to it. This layer makes sure that the data is stored consistently and coherently; complying with the rules on the integrity of the data.

Although some grey areas may exist between the layers, the three above-mentioned are the most frequently implemented ones.

3.2 LAYERS OF A SYSTEM SOFTWARE

The system software of a server also uses a layered approach. Following the Unix architecture, most system software distinguish between:

- The **operating system** (or kernel): defining the structure of the file-system, the processes/threads and their priorities, the accesses to resources located on the system, the users and permissions and the inter-process communications.

- **Utilities and services**: enhancing the kernel with common services that are made available to the other applications running on the system, such as TCP/IP communications over network connections, domain-name resolution (DNS), printer services, remote access to/from other servers, etc.

- The **application server** (appserver): considering that the current Commission's online collection software is a Java application, the appserver is a process that launches a new thread for each new session, invoking the corresponding Java application for this specific thread. In case of existing sessions, together with the MVC handler, it reactivates the thread which was in charge of managing this session, recovering the contents of the memory which was assigned to it, as well as the connection with all the devices. For Java applications, the most common application servers are Tomcat, Glassfish, JBoss/WildFly, Weblogic and WebSphere.

- **Database Management System** (DBMS): this system software is in charge of storing consistent data, allowing applications to abstract the place and the way these data are stored and how they can be retrieved.

3.3 ORGANISATION OF EXPLOITATION

After the application has been built, it is deployed on a server and the operation phase begins. There is a number of ways to organise the exploitation of the application:

- The most well-known one is **in-house** exploitation: the server is installed in the data centre owned and maintained by the organisation itself.
- When the server is located in a data centre owned and maintained by another organisation, responsible for maintenance, this exploitation is called **housing**. This service normally includes the conditioning of its physical environment with measures against fire, water, excessive heat, access control, uninterrupted power supply, network connections, etc.
- When, additionally to the services included in the housing exploitation, the system software is also maintained by an external organisation, the exploitation is named **hosting**. Hosting services normally include the maintenance of the operating system, utilities and services, especially of the application server and database management system. The hosting organisation is responsible for keeping the software stack up-to-date, installing the new releases, configuring and maintaining an adequate configuration for all of the components (operating system, utilities, applications and DBMS), even in case of changes in the environment.

The last two services are considered as outsourced services. Outsourcing offers a possibility to agree on a predefined measurable level of service. Those **Service Level Agreements (SLAs)** establish the adequate levels of availability of the application that the housing or hosting provider shall meet.

3.4 EU FILE SHARING SERVICE

The EU File Sharing Service is an IT service provided by the European Commission to allow safe and secure transfer of messages and files between public entities, either at European level or within Member States. Under some conditions, it can also be used by private entities that needs to exchange files with public institutions.

This service, previously named e-TrustEx, had been created a few years ago initially to allow secure exchange of information, especially large files, in an eProcurement context. It is also heavily used for exchanging information between the Commission, the European Parliament and the European Council during the legislative process. It has been recently upgraded and rebranded as the EU File Sharing Service, as part of the efforts for providing reusable IT solutions under the CEF Digital programme.

The EU File Sharing Service is composed of two main elements:

- The **central system**, also named “open e-TrustEx”, which acts as an email server. It interfaces the external systems and stores the data and files sent by those systems so that they can be retrieved by any of the clients. It maintains the master version of the registry table.

- The **clients,** whose purpose is to access the information posted on the central system. Three types of clients are available and the choice between them depends on several criteria:
    - **e-TrustEx Web Client**: similarly to email web client, this web interface is accessible through the most common internet browsers and it accesses directly the central system. It is the most convenient option in case the frequency of data exchange is low since it only requires the configuration of the EU Login account of the user. The maximal combined size of the file(s) attached to a message is 100 MB. It should be noted that messages have an expiration date, set by default to six weeks. Once the expiration date is reached, the attachments are deleted in order to free up space on the central system.
    - **e-Delivery**: AS4 implementation of the CEF eDelivery Building Block. This is the recommended option for machine to machine data transfer and high frequency messages.
    - **SFTP Client**: this Secured File Transfer Protocol interface is the preferred option for transferring very large files whose size is above the threshold of the other clients (above 100 MB).

External Systems are any business applications operated by EU Institutions, national or local public entities of Member States, or any registered third parties that needs to share data or files with other registered public entities through the EU File Sharing Service. All external systems have to be registered prior to using the service in order to configure in the central registry table all the end points with whom they can exchange data (and create any new end points).

The Figure 6 below gives an overview of the main components of the central system and the way it interfaces with clients and external systems.

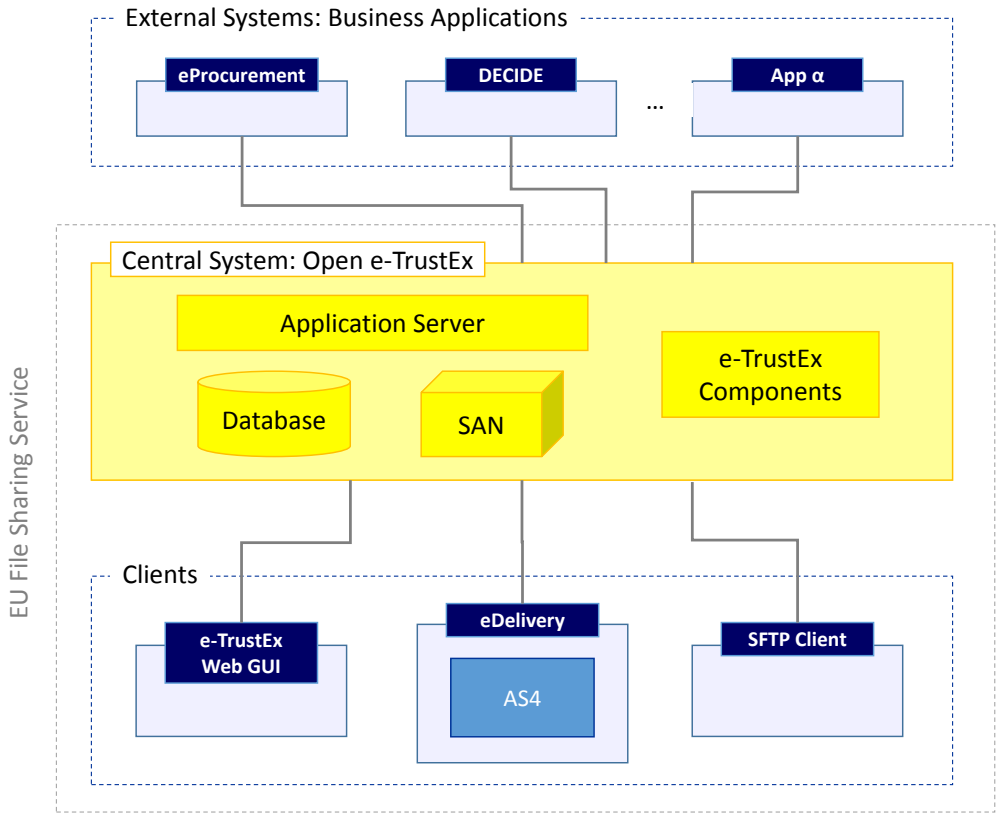


Figure 6: EU File Sharing Service High Level Architecture

In the context of the online collection system, the use of the EU File Sharing Service is considered in the verification step:

- By the Commission in all three scenarios for sending statements of support to the competent authorities in each Member State (when the Commission's online collection software is used) and for receiving their validation;
- By the Organisers in scenario 1 for sending statements of support to the competent authorities in each Member State.

3.5 BOTS SPAMMING PREVENTION

In the current online collection software provided by the Commission, the old CAPTCHA technology is used to prevent bots from creating fake statements of support. As highlighted in Kurt Salmon report, this feature generates quite some issues.

This section summarises in Table 2 the different types of bots that exist, categorised from the least to the most sophisticated ones.

Bot type	Complexity	Characteristics
I	-	• Requests from the same machine • Multiple request-response in a time window since the form submission • Multiple request-response in the same session
II		• Requests from the same machine • Closes the connection after submitting the form
III		• Requests from the same machine • Processes HTML when receiving it without rendering
IV		• Requests from the same machine • Non-human times • Renders HTML when processing
V		• Human times • Renders HTML when processing • Fills in all input fields of the form
VI		• Human times • Renders HTML when processing • Fills in only non-hidden input fields of the form
VII	++	• Human times • Renders HTML when processing • Fills in only not hidden input fields of the form • Requests are made using different machines • Requests are made with greater times than the window time

Table 2: Categorisation of bots

Several technologies and approaches allow to prevent most of the bots. In addition, it should be noted that most of the bots are from type I or II. The most complex ones are rarely used as they require much more development efforts. The next table summarises the different countermeasures that could be implemented. It is considered that applying the whole set of measures could prevent 99.9% of the most common types of bots spamming.

Countermeasure	Characteristics	Objective
Session identification	• Identify open sessions • Assign session cookie to have control on the form connections • Check that only one form is received per session and at a specific time • Forms sent out of time or without session ID will be ignored	• Stop BOT #I activity: ○ The Bot cannot send more than one form in the same session ○ The Bot cannot send a form outside the time session window
Machine identification	• Identify the machine where the bot is running • Create a hash for the identification of the Bot machine • Block the Bot if it generates the same hashes over different sessions and windows	• Stop BOT #II activity: ○ The Bot will not be able to send answers because the same machine is detected; ○ The Bot machine is identified by the common hash of the sessions consisting of: ▪ IP ▪ TCP source port ▪ JavaScript element attribute window.navigator
Detection of HTML rendering	• Detect if HTML is rendered, meaning that the form is actually displayed in a browser • Inclusion of an AJAX script that performs request for rendering detection	• Stop BOT #III activity: ○ The Bot cannot send answers since the HTML has not been rendered ○ Filled form received without the AJAX request being received will be discarded
Detection of non-human times	• Measure the time since the form arrives to the user until the response of the filled form is received • Compare that time with a threshold considered non-human (1.5-2 seconds) • Block the session when detecting non-human times	• Stop BOT #IV activity: ○ The Bot cannot send forms if it fills the form too fast.
"Honey pot" on the form	• Add an hidden "input" field in the form • Use CSS to make this input field not visible by real users • Bots will enter data in this hidden because it cannot interpret the CSS while real users won't be able to enter any data	• Stop BOT #V & BOT #VI activity: ○ The Bot cannot send answers because it has entered data in the hidden field
Data validation	• Filter the input to confirm the correct entry of the data • All data validation must be done on server side, even if also implemented on client side • This measure further protects the system from attacks such as code injections	• Stop Bots activity: ○ The Bot cannot enter inconsistent or too large data.

Table 3: Countermeasures to prevent bots from filling forms

Enhancements to the Implementing Regulation (EU) 1179/2011 will be proposed in line with those measures. As already suggested in its current version, this Regulation should highlight what needs to be achieved (preventing bots spamming and automated submission of statements of support) while giving the flexibility to developers to select the most appropriate technical solution considering the evolution of the threats and the corresponding countermeasures.

4 SCENARIO 1

4.1 DESCRIPTION

The first scenario aims at formalizing the current situation, especially from a legal point of view, as it is not foreseen in the initial ECI Regulation that the European Commission is providing both the online collection software and the hosting.

From a technical point of view, it considers the scenario foreseen in the ECI Regulation with individual online collection systems, for which the organisers are being held responsible. The online collection system is stand-alone, under the responsibility of the organisers. Standalone instances of online collection software and infrastructure can be provided either by the Commission or by third party hosting organisations.

This scenario includes the update of the current technical specifications to cater for evolution and new threats in security as well as in application architecture. The technical specifications could be modified to simplify and adapt the requirements to technical progress.

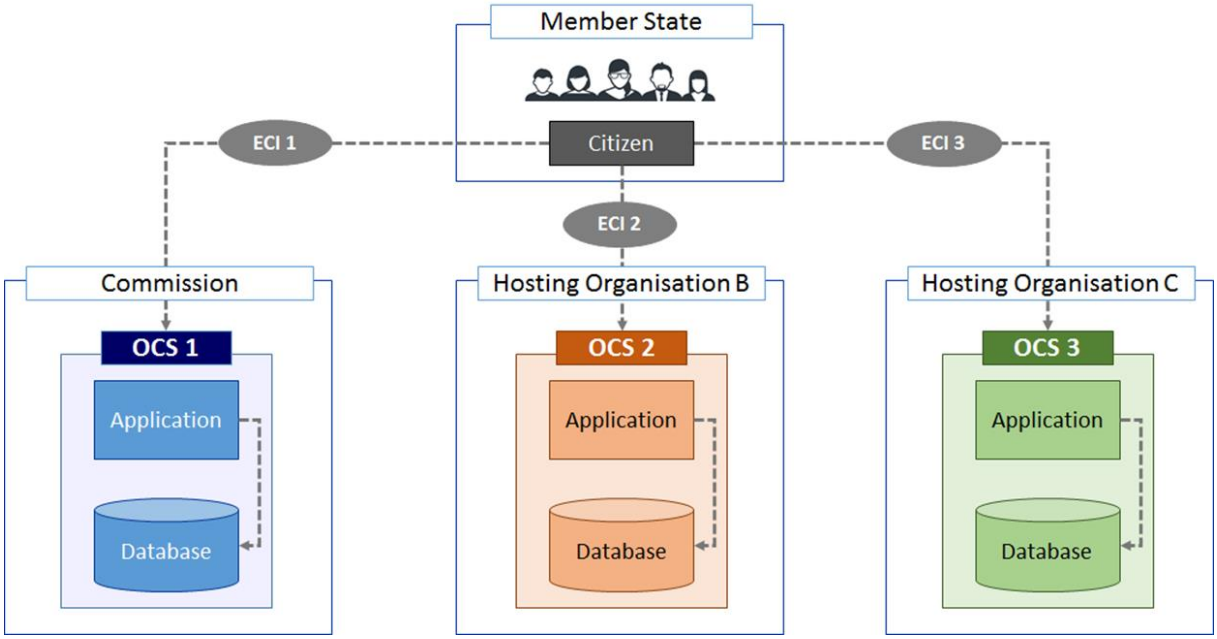


Figure 7: Architecture of scenario 1

Figure 7 shows the architecture of scenario 1 and its different standalone online collection systems, hosted either by the European Commission or by third party organisations.

4.2 LEGAL ANALYSIS

The legal analysis that follows focuses on the critical Articles of the ECI Regulation and the implementing Regulation, laying down the technical specifications for the online collection system that need to be adapted in the different scenarios considered in this study.

The changes or adaptations required concern in particular the updated EU rules for processing personal data, as laid down in the General Data Protection Regulation (EU) 2016/679 (GDPR), which contains the new EU rules for processing personal data and replaces former Directive 95/46/EC. This analysis highlights the changes with an impact on the substance. Other changes of a referring nature will be required in the revised ECI Regulation and its Implementing Regulation to ensure consistency with the new legislative instruments on data protection.

First, a word should be said about the material scope of the new data protection Regulation and its exclusions in order to justify its impact on the ECI. As indicated in Article 2(1) GDPR, it applies *"to the processing of personal data wholly or partially by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system"*. Paragraph 2 of this Article foresees a series of exceptions where the Regulation is not applicable. None of them are applicable to personal data processed in the case of an ECI.

Attention should be paid however to paragraph 3 of Article 2 GDPR, which recalls that where the processing of personal data is undertaken by the Union institutions, bodies, offices and agencies, the relevant applicable Regulation is **Regulation (EC) 45/2001** on the protection of individuals with regard to the processing of personal data. **This Regulation is currently being reviewed**[4] in order to ensure an approach to personal data processing that is consistent and coherent with the principles laid down in GDPR. This means that, in the scenarios described below, where the processing of personal data is carried out by the European Commission, the revised 45/2001 Regulation will apply and not the GDPR, even though the legal implications do not change in practice, since the revised Regulation will implement the principles of GDPR with regards to data protection.

The section below summarises some of the key novelties introduced by the GDPR and reflected also in the proposed revision of Regulation 45/2001 that are relevant to the analysis that follows. This part is common for all the scenarios considered in this study and will therefore not be repeated in the analysis of the other scenarios. The reader is invited to refer back to this section. It should be noted that due to the simplified nature of the chapter that follows, it is assumed that the reader is already familiar with the GDPR and with the different data protection roles that are foreseen in this Regulation. Should that not be the case, the reader is invited to consult chapter IV of GDPR.

4.2.1 Summary of key novelties introduced by the new data protection rules relevant for the ECI

The section below highlights some of the key novelties introduced by the new data protection rules with implications for the ECI legislative instruments.

More defined and new rights of the data subjects

The GDPR, which will become applicable in all EU Member States in May 2018, further specifies the **right of data subjects to obtain information** from the controller regarding the processing of their personal data, including the storage period, and the rights they may exercise as data subjects. The new Regulation also further develops the rights of data subjects to ask the data controller to **rectify and/or erase** their personal data whenever the collected data is no longer relevant or is inaccurate or incomplete, or if the data subject simply decides to withdraw his consent, and to lodge a complaint with a **single supervisory authority.**[5]

All these provisions are reflected in the currently under revision Regulation 45/2001.[6] Where the processing is carried out by the European Commission, the relevant body for dealing with the

[4] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (2017/0002(COD)), available at:
http://opac.oireachtas.ie/AWData/Library3/JUQdoclaid030217Inst_151002.pdf

[5] Articles 13(2)(b), 15, 16, 17 and 18 GDPR.

[6] Articles 14 to 22 of Proposed Regulation repealing Regulation (EC) No 45/2001, *op.cit.*

complaints submitted by data subjects in cases of infringement is the European Data Protection Supervisor (EDPS), in addition to the judicial remedy offered by the EU Court of Justice.

Clearer responsibilities and new liabilities for data processors and controllers

Another key novelty introduced by the new data protection rules relates to the **more defined role and responsibilities of the data processor vis-à-vis the data controller** and in particular the respective **liabilities** that they may incur in, either jointly or separately, in case of breach of their data protection obligations. With regard to their responsibilities, a clearer and detailed list of tasks for each of them is provided for in GDPR and is also reflected in the proposed revised Regulation 45/2001. New responsibilities assigned to the data controller and to the processor include their obligation to **maintain a record of processing activities** under their responsibility or carried out on behalf of the controller in the case of the processor.[7]

The data controller also has the obligation to provide the data subject with the personal data concerning him in a structured, commonly used and **machine-readable format**.[8] Under the new GDPR, data processors are expected to assist the controllers in implementing the appropriate **technical and organisational measures** to ensure an adequate processing of the personal data processed.[9] Data processors are further obliged to either **return or delete** all the personal data stored to the controller at the end of the provision of the processing services, at the choice of the controller.[10] Finally, both data controllers and processors have an **obligation to notify a data breach** as soon as they become aware of it. Data processors need to notify the data controller under whose instructions they are processing the data, and data controllers need to notify the relevant supervisory authority or the EDPS, where the processing is carried out by an EU institution or body.[11]

Under the previous Directive 95/46/EC[12] only data controllers were liable and could be subject to sanctions if data subject suffered a damage as a result of an unlawful processing operation or of any processing contrary to the provisions of the Directive. Under the new data protection rules, **both the controller and the processor may be held liable** for any damage caused by their processing, and the affected data subjects are entitled to receive compensation from it.[13] The GDPR also provides the relevant supervisory authority with the power to impose **administrative fines** for data protection infringements to both the data controller and the processor.[14] In addition, where the processing of personal data takes a **cross-border dimension**, the GDPR provides for a 'lead supervisory authority' that will coordinate the investigation.[15]

The right of the data subject to **receive compensation** from the controller of processor for the damage suffered is also provided for the proposed Regulation replacing Regulation 45/2001, applicable to EU institutions when processing personal data.[16] Such right was not foreseen in the former Regulation 45/2001, which constitutes a key change. The new proposed Regulation concretely foresees sanctions for EU officials and civil servants who fail to comply with their data

[7] Article 30 of GDPR and Article 31 of the proposed revised Regulation 45/2001.
[8] Article 20 GDPR and Article 22 of the proposed revised Regulation 45/2001.
[9] Articles 28 and 32 GDPR, reflected in the proposed revised Regulation 45/2001 in Article 33.
[10] Article 28(3) (g) GDPR and Article 29(3) (g) of proposed revised Regulation 45/2001.
[11] Article 33 GDPR and Article 37 of the proposed revised Regulation 45/2001.
[12] Articles 23 and 24 Directive 95/46/EC.
[13] Article 82 GDPR.
[14] Article 83 GDPR.
[15] Article 56 of the proposed revised Regulation 45/2001.
[16] Article 65.

protection obligations. In addition, building on Article 83 GDPR, the proposed amending Regulation provides the EDPS with the power to impose **administrative fines** on Union institutions and bodies when they fail to comply with an order imposed by it regarding the processing or personal data.[17]

New roles: the Data Protection Officer and the Lead Supervisory Authority

The GDPR brings in an additional role to the data protection chain: the '**Data Protection Officer'** (DPO), which is defined in Article 37. This new role is compulsory whenever the processing is carried out by a public body or when the processing involves a large scale of special categories of data, such as data revealing political opinions, religious beliefs, trade union membership, or data concerning health or sexual orientation.[18] This person has to be jointly appointed by the controller and the processor and can be either a staff member of the controller or the processor, or fulfil the tasks on the basis of a service contract. The responsibilities of the DPO are essentially linked to monitoring compliance with the GDPR and to provide advice to the data controller and to the data processor. Within the remit of the ECI, the DPO will apply to the national authorities processing personal data and it may also apply to the organiser depending on the scope of the citizens' initiative and the type of information that is collected from data subjects.

The GDPR also establishes an additional role, the **'Lead Supervisory Authority'**, defined in Article 56 GDPR. In addition to the national supervisory authorities, whose main responsibility is to monitor and enforce the application of the data protection rules and handling complaints lodged by data subjects, this new body where the processing of personal data takes in a **cross-border dimension** in order to ensure that the role of the supervisory authority is centralised in one single entity in the EU. In this case, identifying the lead supervisory authority will depend on determining the location of the controller's 'main establishment' or 'single establishment' in the EU. This lead supervisory authority will serve for both controller and processor.[19] This has implications for the ECI, as the collection of statements of support genuinely implies a cross-border processing of personal data.

Where the processing of personal data is carried out by an EU institution or body, the role of the independent supervisory authority is filled by the **European Data Protection Supervisor**.[20]

Data protection impact assessment and prior consultation

As opposed to Directive 95/46/EC, which provided for a general indiscriminate obligation to notify the processing of personal data to the supervisory authorities, the new data protection rules focus on the processing operations that entail substantial risks in terms of the rights and freedoms of people because of their nature, scope, context and purposes.[21] Concretely, the data controller is required to carry out an impact assessment of the envisaged processing operations that may entail a "high risk" for the rights and freedoms of persons prior to their implementation, with the support of the data protection officer.[22] The controller has to consult the relevant supervisory authority prior to processing where the mentioned data protection impact assessment indicates that the processing would result in a "high risk" in the absence of measures taken by the controller to mitigate the risk.[23]

[17] Article 69 and Article 66 of proposed revised Regulation 45/2001, respectively.
[18] Article 37(1) a) and c) GDPR.
[19] For more information see Article 29 Data Protection Working Party (2016): *Guidelines for identifying a controller or processor's lead supervisory authority* (16/EN WP 244), available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf
[20] Article 41 of the proposed revised Regulation 45/2001.
[21] Recital 89 of GDPR.
[22] Article 35 GDPR.
[23] Article 36 GDPR.

These obligations are reflected in Articles 39 and 40 of the proposed revision of Regulation 45/2001, applicable to EU institutions and bodies when processing personal data.

4.2.2 Impact of the new data protection rules on ECI stakeholders and their responsibilities: General assessment

Generally speaking, the GDPR entails **more precise responsibilities for each ECI stakeholder involved in data protection matters**, namely the organiser, the European Commission and/or the third party acting as online collection system provider and the competent national authorities responsible for the verification of the statements of support. In addition, a brand new role is foreseen by the GDPR which did not previously exist: the '**lead supervisory authority'** centralising the tasks of the 28 national supervisory authorities, where the processing of personal data takes a **cross-border dimension**, as it is the case with the ECI. The role of the DPO is now applicable to national authorities processing personal data and may also concern the organiser depending on the scope of the ECI proposed and/or the type of information collected from the supporters.

Finally, the GDPR also substantially affects the **liabilities** that the different ECI stakeholders may incur if a damage is caused to the data subjects, either as data controllers, as data processors or as both. According to the previous Directive still in force,[24] the controller is the only one that can be held responsible whenever a person suffers a damage as a result of an unlawful data processing operation. Consequently, only ECI organisers and the competent national authorities, as data controllers, can theoretically undergo penalties in case of infringement[25]. Conversely**, in the new data protection rules the obligation to compensate the data subject in case of damage is foreseen for both controllers and processors** in case of infringement of the Regulation.[26] Concretely, the controller is liable for the damage caused by a processing which infringes the Regulation, unless he can prove that he is not responsible for the event causing the damage.[27] The processor´s liability is limited to the cases where he/she has not complied with the obligations arising from the Regulation that are specifically directed to processors or where he/she has acted outside or contrary to the instructions given by the controller.[28] In addition, the relevant supervisory authority may impose administrative fines in cases of data protection infringements.[29]

The right to compensation is also established in the proposed revised Regulation 45/2001, where the processing of personal data is carried out by an EU institution or body.[30] Sanctions can be imposed on EU officials that do not abide by their data protection obligations, whether intentionally or through negligence.[31] The proposed revised Regulation also empowers the EDPS to impose administrative fines to the EU institution or body that fails to comply with its orders regarding the processing of personal data.[32]

[24] Article 23(1) Directive 95/46/EC.
[25] In practice, Article 13 of the current ECI Regulation only foresees liabilities for ECI organisers, but not for the national competent authorities, even if the latter are also considered as ´data controllers´ as per Article 12(2) of the ECI Regulation. This should be amended in the revised text.
[26] Article 82 GDPR.
[27] Article 82(2) GDPR.
[28] Article 82(2) GDPR.
[29] Article 83 GDPR.
[30] Article 65 of the proposed revised Regulation 45/2001.
[31] Article 69 of the proposed revised Regulation 45/2001.
[32] Article 66 of the proposed revised Regulation 45/2001.

The section that follows highlights the key implications for scenario 1 of the changes referred to in section 4.2.2 in terms of data protection roles and liabilities of the ECI stakeholders. A separate analysis of the key implications for scenarios 2 and 3 is included further down, followed by a comparative analysis of the three scenarios (see section 5.2.1).

4.2.3 Specific implications for scenario 1

Impact on data protection roles

In scenario 1, **the organiser of an ECI and the competent authority in the Member State remain 'data controllers' under the GDPR**.[33] Both – the organiser and the competent authority – determine the purpose and means of the processing of personal data. Indeed, the organiser of an ECI takes the initiative to collect the statements of support and decides on the appropriate software for doing so when statements of support are collected online.[34] The organiser may choose a software developed by himself or by a third party, or the open source software made available by the Commission. The organiser is further able to choose the service provider for the hosting of the online collection software. When he/she uses the software made available by the Commission, he/she may choose that the statements of support are stored in the Commission´s data centre.

Furthermore, as data controllers, organisers remain ultimately responsible for the online collection system and, if still relevant, are in charge of getting the system certified with the competent national authorities in the Member States where the personal data is being stored by submitting the required security documents to the national authorities[35]. As regards the systems hosted by the Commission, organisers must also designate a minimum of three people from their citizens´ committee, who will have access to the personal data stored in the online collection system throughout the processing.[36] Finally, organisers are responsible for transferring the statements of support collected, either online or in paper or both, separately, to the competent authorities in the Member States for their verification, and for sending the certification issued by the Member States to the Commission, thereby acting as an intermediary throughout the process.

The so-called 'competent authorities'[37] in the Member States are responsible for checking and verifying the validity of the statements of support sent to them against their own databases and for issuing the corresponding certification to the organisers, which has ultimately an impact on the ECI success. In doing so, they are free to apply the methodology deemed appropriate in accordance with national law and practice.[38]

[33] For a definition of 'data controller' and 'data processor' see Article 4(7) and (8) GDPR and Article 3(2)(b) of the proposed revised Regulation 45/2001.
[34] It should be noted that statements of support can be collected both in paper and online, as per Article 5(2) of the ECI Regulation (211/2011). The focus of this study is the online collection, but the collection of statements of support in paper format should also be considered when revising the ECI Regulation.
[35] The future of the certification phase is discussed in the organisation analysis.
[36] European Commission, "Hosting of Online Collection Software Instances by the Commission", available online at: https://joinup.ec.europa.eu/sites/default/files/ocs_hosting_procedure_2014-12-08.pdf.

[37] As per term used in the ECI Regulation 211/2011.
[38] Article 8(2) of ECI Regulation.

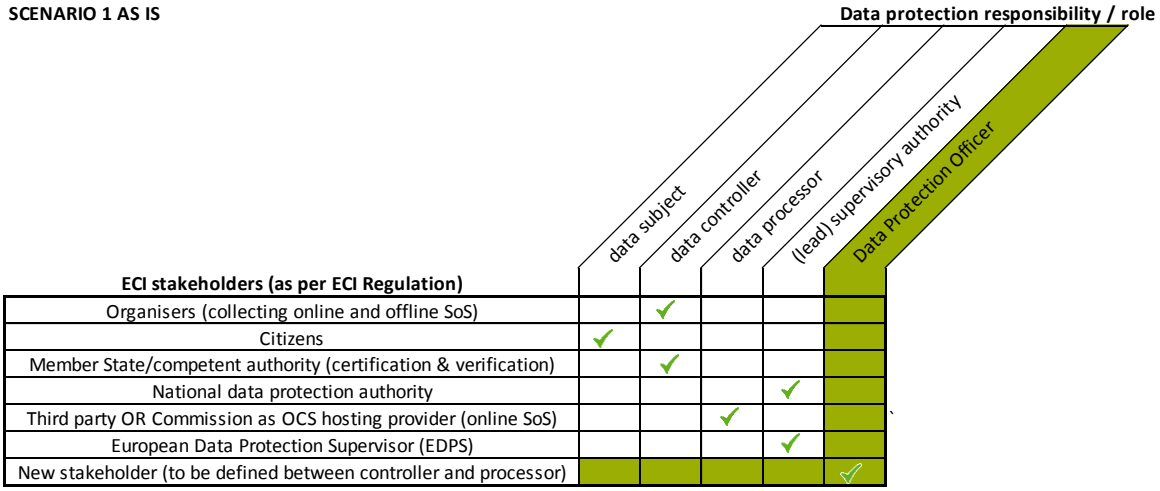


Figure 8: ECI stakeholders and responsibilities based on GDPR - scenario 1

In this scenario, the role of 'data processor' is exercised by the hosting provider of the online collection software, which can either be the Commission, where organisers choose its open source software, or a third party, if organisers opt for a third service provider. Either of the two are considered as data processors inasmuch as they process personal data on behalf of organisers.

The **role of the supervisory authority** as a "guardant" of the Regulation remains within the designated data protection authority at national level[39]. The new feature introduced by the GDPR is that this role **will now be centralised within one single national authority** called 'lead supervisory authority', corresponding to the one where the data controller is established, namely the country where the organiser is based. Where the European Commission acts as data processor by providing the hosting of the online collection software, the role of the independent supervisory authority is filled by the EDPS, in line with the provisions in Regulation 45/2001 currently under revision.[40]

The citizen who decides to support an ECI remains the data subject, namely the person whose personal information is being processed under both GDPR and Regulation 45/2001.

Finally, the new data protection rules include in certain circumstances a **new player** with data protection responsibilities: the DPO previously mentioned.

Impact on liabilities

Under the new data protection rules laid down in GDPR, both data controllers and data processors can be held liable whenever a person suffers a damage as a result of an unlawful data processing operation, whilst under the previous Directive the liability was limited to data controllers (see section 4.2.2).

The practical implication of the revised rules on liabilities for scenario 1 is that **in addition to ECI organisers and the competent authorities** who verify and certify the validity of the statements of support (acting as *data controllers*), **the service providers of the hosting of the online collection software** (acting as *data processors*) **may also incur liabilities for any damage caused by their processing to the data subject(s) if they failed to comply with the obligations specifically addressed**

[39] See list: http://ec.europa.eu/justice/data-protection/Article-29/structure/data-protection-authorities/index_en.htm

[40] Article 53(3) of the proposed revised Regulation 45/2001.

to them by the Regulation or if they acted outside or contrary to the instructions provided by the data controller. It is important to highlight that when the hosting of the online collection software is offered by a third party, the relevant provisions are found in GDPR.[41] When the hosting of the online collection software is offered by the European Commission, however, the applicable provisions are in Regulation 45/2001, currently under revision.[42]

Table 4 below summarises the results of the legal analysis for scenario 1.

Evaluation Criteria	Stakeholder	Score	Description
Impact of GDPR/Regulation (EC) No 45/2001 under revision on ECI stakeholders	European Commission/ Third party	●●●○○	• The online collection software hosting provider is considered as data processor only for the online statements of support.
	Competent Authorities (and data protection authorities in Member States)	●●●●○	• The competent authorities are considered as data controllers when verifying and certifying the paper and online statements of support. • The data protection authorities in the Member States are considered as the supervisory authorities • A lead supervisory authority is established by GDPR as a one-stop-shop in cases of cross-border processing of personal data
	Organisers	●●○○○	• Organisers are considered as data controllers concerning the processing of paper and online statements of support.
Impact on liabilities	European Commission/ Third party	●●●○○	• Under the previous data protection rules, only data controllers were liable in case of damages caused to the data subject when processing their data. • According with the new GDPR and Regulation 45/2001 under revision, both data controllers and data processors may face liabilities in proportion to their role. • The possibility for the supervisory authorities/EDPS to impose administrative fines to the controller and the processor, in case of non-respect of their data protection obligations, is now foreseen. • Consequently, the European Commission and the third party acting as online collection software hosting providers may now face liabilities as data processors.
	Competent Authorities		
	Organisers		

Table 4: overview of the legal analysis - scenario 1

4.3 ORGANISATION ANALYSIS

4.3.1 Convenience

According to this scenario:

- The European Commission provides an open source software incorporating the relevant technical and security features. Organisers can however decide to use the Online Collection System provided by third party hosting organisations.
- The online collection system provided by the European Commission is considered as de facto certified. Organisers would however need to accept a set of rules while using the Commission system, as they remain data controllers for the processing of the data through their systems. Consequently, the ECI process is shortened and there is no need to prepare the documentation for the certification anymore.

[41] Article 82(2) of GDPR.
[42] Article 65 of the proposed revised Regulation 45/2001.

- In case a third party online collection system is used, the organisers will need to request its certification by the Member State where the data is located.
- Throughout the whole ECI procedure, organisers and competent national authorities, considered as data controllers, are being held responsible for the protection of the data of the signatories. With the GDPR entering into force in 2018 and the revised Regulation 45/2001, this responsibility is extended to the data processor: the hosting provider, being respectively a third party organisation or the European Commission.
- The respective Member States are responsible for the verification of the personal data for the purpose of identifying the signatories and for the delivery of the certificate, certifying the number of valid statements of support (ECI Regulation, Articles 5.3 and 8.2) (see section 4.3.1).

4.3.2 Certification

The current version of the ECI Regulation requires the Member States to certify the system in which the data is stored, in order to verify that all technical specifications are fulfilled. The current certification process can be described as follows:

In order to collect statements of support online, organisers must set up an online collection system compliant with:

- *The data security collection and storage requirements and, more especially with the security and technical features, set out in Article 6.4 of the ECI Regulation;*
- *The technical specifications, set out in the Commission Implementing Regulation (EU) 1179/2011.*

The organisers must then request the certification of the system to the competent national authority of the Member State where the data will be stored. In case organisers make use of the Commission's hosting, the certification currently has to be requested to the Luxembourgish competent authority. This step is mandatory and a precondition for the collection of statements of support online. The certification procedure might vary from one Member State to the other, but also depends on the software and the hosting provider which are used. The competent authorities have then one month to verify whether the above-mentioned requirements are met. Once the system is certified, organisers receive a certificate from the national authority.

Organisers are required to provide appropriate documentation showing that they fulfil the requirements regarding the technical specifications to complete the certification. In case they take the opportunity to use the hosting and online collection software of the Commission, this process is simplified as the documentation related to the hosting environment and software are directly produced and sent by the Commission to the Luxembourgish authority[43].

4.3.3 Verification

The verification of the statements of support, in the original scenario foreseen in the ECI Regulation, works as follows:

- The organisers submit the statements of support to the relevant competent authorities for verification and certification;

43 http://ec.europa.eu/citizens-initiative/public/hosting

- The competent authorities, within a period not exceeding three months, verify the statements of support and deliver to the organisers a certificate, certifying the number of valid statements of support for the Member State concerned.

Table 5 below summarises the results of the legal analysis for scenario 1.

Evaluation Criteria	Stakeholder	Score	Description
Convenience	European Commission/ Third party	●●●○○	• The European Commission or the third party provides a stand-alone online collection software.
	Competent Authorities		• n/a
	Organisers	●●●○○	• The organisers are free to choose between the online collection software provided by the European Commission or by third party organisations.
Certification	European Commission/ Third party	●●●●○	• The online collection system provided by the Commission is considered as de facto certified, which shorten the setup process of a new initiative. • In case a third party system is used, organisers are responsible to request certification and competent authorities to certify it.
	Competent Authorities	●●●○○	
	Organisers	●●●○○	
Verification	European Commission	●○○○○	• The European Commission does not play any role in the verification of statements of support.
	Competent Authorities	●●●●○	• The national competent authorities verify the statements of support and deliver a certificate to the organisers.
	Organisers	●●○○○	• The organisers submit the statements of support to the relevant competent authorities.

Table 5: overview of the organisation analysis - scenario 1

4.4 TECHNICAL ANALYSIS

4.4.1 Implementation

The installation of the European Commission's online collection software is straightforward: the source code is delivered with the compilation directives in a pom.xml file, prepared to be used by the most widely used Java compilation environment: maven. The manual for the installation of the application under Weblogic and Glassfish application servers is clear and well developed. If organisers opt for an online collection software implemented by a third party, the installation might be more complicated. In both cases, this installation should be performed individually for each online collection software instance, corresponding to a single ECI.

The scalability of this scenario presents no major issue. The online collection software, deployed either in a physical or virtual server, should be sized accordingly to achieve its performance objectives. In the eID for ECI study, it was shown that a standard server is able to process 4 million statements of support in one day, which is sufficient given that each initiative requires a dedicated server.

The maintenance of the system is considered as normal and corresponds to 20-25% of the effort of the initial development. In the short term, changes are foreseen to integrate and deploy the new front-end. On the long term, other modifications can be anticipated, such as the integration of the eID.

4.4.2 Operations

The system administration consists first in the initial installation of the system, second in the daily operations (e.g.: verification of the log files) and regular updates of the software components and, finally, its disposal and/or migration to a newer environment.

The updates of the software imply that the system administrator should remain aware of any new flaws or issues, which are regularly detected. In this case, the system should be updated in order to avoid the flaw to be exploited. The verification of the system and application logs is intended to detect problems before they harm the system and its users. This will allow to detect bottlenecks before they cause performance problems, as well as to detect attacks before they succeed in corrupting the system. The disposal of the system covers the removal of the online collection software, its data and all logging and trace-files, in order to have the server ready to be used for other applications. Usually, this could be performed in a few hours.

Except for the possible improvement of the security features, no significant difference is currently observed on the technical side under scenario 1, compared to the AS IS situation. Nonetheless, it should be noted that some of the changes envisaged in scenarios 2 and 3 may be implemented in scenario 1, especially the use of the EU File Sharing Service (optionally or mandatorily).

Evaluation Criteria	Category	Score	Description
Implementation	Installation	●●●○○	• The installation of the source code is prepared to be used by the Java compilation environment: maven. • If organisers opt for an online collection software implemented by a third party, the installation might be more complicated.
	Scalability	●●●○○	• The online collection system should be sized accordingly to achieve its performance objectives.
	Maintenance	●●●○○	• In the short term, changes to integrate and deploy the new front-end are foreseen. • On the long term, other modifications can be anticipated, such as the integration of eID.
Operations	System administration	●●●○○	The following activities are covered: • Installation of the system; • Update of the software based on discovered flaws and security breaches, revision of log files during the life-cycle of the system; • Disposal/migration.
	Verification process	●●●○○	• This scenario offers no improvement of the verification process.

Table 6: overview of the technical analysis - scenario 1

4.5 SECURITY ANALYSIS

4.5.1 Security architecture

According to the ECI Regulation, it is the responsibility of the organisers to ensure that the system used for their registered initiative complies with the relevant requirements under the ECI Regulation (e.g. storage in the territory of an EU Member State, compliance with the technical and security features, certificate, etc.).

When organisers look for a hosting/housing service provider compliant with the Regulation, they may face some difficulties finding one that fully complies with the minimum security requirements, both on the logical and physical or availability levels.

Furthermore, the requirements on a technical level regarding the isolation of the online collection software, within the physical or virtual server hosting the application, are not clear. Consequently, it

entails a potential risk for the applications of other clients, which could have a vulnerability affecting the data or the application of the organiser.

With regards to section 2.13 of the Annex of the Implementing Regulation (EU) 1179/2011, it is recommended to set up a backup process outside the system hosting the online collection software, either on a different disk belonging to another server within the hosting/housing, or on an alternate site (such as the Commission's recovery site).

According to section 2.16, further actions should be taken into consideration and registered/audited, especially with regard to the data access and maintenance tasks of both the system administrator and the organiser.

Following section 2.18.1, only the presentation layer should be deployed in the DMZ. Other layers shall be protected at a higher level in the internal zone and with another firewall.

It is worth mentioning that, for administrative tasks, only robust protocols should be allowed, relying on encryption such as SSH, TLS, etc.

With regard to section 2.17 pertaining physical security, further controls may be included, such as physical security perimeter protecting against external and environmental threats, and cabling security.

As an improvement on the security architecture, an Intrusion Detector/Protection System (IDS/IPS) could be added to monitor and block potential attack attempts, including brute force and denial of service. For prevention purposes, a web application firewall (WAF) might also be helpful to filter the requests. It is however important to highlight that such validations must be conducted by the application on all the layers instead of relying on an external element.

4.5.2 Software development security

According to the ECI Regulation, the certification of the Online Collections System must be done by the competent authorities in the Member States where the data are stored. Consequently, the national competent authority should certify the online collection system to ensure that it complies with the technical and security requirements established in the ECI Regulation and Implementing Regulation. A potential risk lies on the fact that the competent authorities may certify the compliance of a specific online collection system without noticing a security breach in the code application, having therefore an impact on the entire security.

This risk entails a serious issue, as the certification is only conducted once and no further security tests are performed. Instead of a one-shot certification exercise, it is recommended to conduct regular audits of the whole system, ensuring not only compliance with the technical and security requirements, but also running further ethical hacking tests or penetration testing activities, as well as a code audit to detect eventual failures in the software. This approach represents an additional cost, but advantageously it can be outsourced to a competent third party provider that will have all the necessary skills.

In case organisers opt for at a third party hosting provider, they shall take all the security measures throughout the software development lifecycle.

Some additional security aspects should be clarified and taken into consideration in the Implementing Regulation, especially in its Annex:

- Section 2.7 should state that data validation is always conducted on server side (although functional validation could also be done on the client) ;
- It should also be noted that, if APIs are used, they should be tested and protected from the different types of injection, authentication, access control, encryption, configuration, and other issues that can exist, similarly to traditional applications;
- As regards section 2.7.6 (d), a generic error webpage should be used for all exceptions, without displaying confidential data. Confidential information should never be exposed in error notices. Information such as system access routes to local files or any internal information of the system should be hidden;
- Properly parameterized flags should be added to section 2.7.9 (b): “Secure”, “HttpOnly”, “Domain” and “Path”, “Expire” and “Max-Age”;
- As a general rule, during the entire software development lifecycle (SDLC), security measures should be applied. The framework OWASP Software Assurance Maturity Model (SAMM) framework is recommended. It should be applied to any online collection software, whether provided by third party or by the European Commission, and focuses on integrating security concerns into each part of the software development process, such as code security analysis.

4.5.3 Data security & integrity

Regarding data security and integrity, the ECI Regulation foresees the following:

- The secure storage of the signatories’ data;
- The possibility to export the data in order to submit it to the national competent authorities. In the AS IS situation, the submission is done by the organisers, outside of the system;
- The administration and management, by organisers, of the statements of support collected for their initiative;
- The secure collection and storage of the statements of support, taking into account the need for data integrity, reducing the risk of possible fraudulent data input or input validation mechanisms tweaks.

Article 6.4(b) of the ECI Regulation states that “*the data provided online are securely collected and stored, in order to ensure, inter alia, that they may not be modified or used for any purpose other than their indicated support of the given citizens’ initiative and to protect personal data against accidental or unlawful destruction or accidental loss, alteration or unauthorised disclosure or access*”. As personal data are stored through the Online Collection System, this system is required to have strong security and technical features, as well specified in the GDPR.

In addition, the following aspects of the Implementing Regulation should be taken into consideration, especially in its Annex:

- Section 2.7.7(a)(d) does not specify how encryption keys should be managed, leading to confusion or potentially bad practices. It is recommended to store them on a keystore, considering the following elements:
    - Keys must be protected on both volatile and persistent memory, ideally processed within secure cryptographic modules;
    - Keys should never be stored in plaintext format;

- All keys should be stored in cryptographic vault, such as a Hardware Security Module (HSM) or isolated cryptographic service.

- It is essential that the application incorporates a secure key backup capability, especially for applications that support data at rest[44] encryption, for long-term data stores. When backing up keys, it is important to ensure that the database used to store the keys is encrypted.
- Section 2.10 should clarify that data should only be accessible to organisers, citizens and competent authorities. For example, the "DB admin" (the technical role responsible for the maintenance of the HW/SW) should not have access to the data stored (principle of necessity).
- Section 2.11 should specify that unencrypted data should also be protected in read-only mode.
- Section 2.16 should specify that all system activity logs shall be in place, if possible in other systems with adequate protection.
- Section 3.1 should also specify that the reports shall be provided in read-only mode, with an integrity verification by means of a hash function (message digest).
- In regards to section 3.4, in the process of sending, reception and storage of the data collected from the online collection system (exported data), for the verification in accordance with Article 8(2), for the purpose of validation, valid protocols should be applied for the secure transmission of the communication between the online collection system and the national competent authorities.

4.5.4 Identity and access management

The objective of setting identity and access management procedures is to ensure:

- The necessary and adequate permissions of each stakeholder to manage the information collected in the online collection system;
- The process of identification and authentication meets the security requirements.

According to Article 8 of the ECI Regulation, the organisers shall submit the statements of support, collected in paper or electronic form via the online collection system, to the relevant competent authorities for verification and certification.

Under scenario 1, the competent authorities do not need to have a direct access to the online collection system. The same is also applicable to the Commission. Whenever the Commission's online collection system is used, the system administrators of the Commission need the correct access to perform their tasks, but do not need an access to the personal data collected by the online collection system. Only organisers will be granted a role allowing them to perform their duties, including the export of the data of the statements of support in order to send them to competent authorities. Their obligations are laid down in section 2.7.3(h) of the Annex of the Implementing Regulation (EU) 1179/2011.

[44] inactive data that is stored physically in any digital form

Evaluation criteria	Stakeholder	Score	Description
Security architecture	European Commission	●●●○○	• Even if the hosting service is compliant with the Regulation, it may have some security breaches (physical or logical) not covered.
	Competent Authorities	●●●○○	• Communications with each organiser's platform may vary in the security configurations but it should meet the requirements laid down in the ECI Regulation.
	Organisers	●●●○○	• Even if the hosting service is compliant with the Regulation, it may have some security breaches not covered.
Software development security	European Commission	●●●○○	• The Commission guarantees that the Commission's online collection software follows the ECI technical specifications and publishes it as open source code for external verification.
	Competent Authorities	●●●○○	• The competent authorities may certify the compliance of a specific online collection system without noticing a security breach in the code application.
	Organisers	●●○○○	• Organisers need to ensure that the system used for their registered initiative complies with the relevant requirements under the Regulation development of their own online collection software.
Data security & integrity	European Commission	●●●○○	• The sending and storage of the data collected in the online collection system, for the verification by the Member States, is made in accordance with Article 8(2).
	Competent Authorities	●●●○○	• The reception and storage of the data collected from the online collection system of each initiative (exported data), for the verification by the Member States, is done in accordance with Article 8(2).
	Organisers	●●○○○	• The sending and storage of the data collected in the online collection system, for the verification by the Member States, is done in accordance with Article 8(2).
	External user	●●○○○	• A malicious user (outsider) could try to hack the online collection system by exploiting a possible vulnerability.
Identity and access management	European Commission	n/a	• The European Commission does not have direct access to the online collection system.
	Organisers	●●●○○	• The organisers' access, as an admin role, has several security requisites in the Technical Specifications Article 2.7.3 h.

Table 7: overview of the security analysis - scenario 1

4.6 COSTS ANALYSIS

Estimates of the costs incurred by the Commission and the organisers in the AS IS situation and in the three scenarios have been made in order to analyse the financial impact of each scenario. Costs for the competent authorities couldn't be estimated due to lack of data.

4.6.1 European Commission

The first step of the costs analysis consisted in calculating the costs of the AS IS situation for the Commission. The Kurt Salmon report[45] provided the basis for these estimates. In addition, the following assumptions were made for the estimation of the costs for the European Commission and are applicable to all situations, including the AS IS:

- 20 ECI per year are expected. This is in line with the observations of this year (10 ECI registered or under registration in the first 6 months of the year);
- Hosting costs of development, test and acceptance environments are 30,000 euros;

[45] http://ec.europa.eu/citizens-initiative/files/Final-report-ICT-impacts.pdf

- The maintenance of the online collection software is estimated to 360 days per year (198,000 euros). On top of that, 40 days per year are foreseen for the upgrade of the tools, software and frameworks used by the solution (system administrator activities);
- STIS IV daily rates for "Normal" on-site profiles have been used to estimate the development and maintenance costs.

Moreover, the following assumptions only apply to the AS IS situation:

- Out of the 20 ECIs, it is assumed that 15 are implemented with the Commission's online collection software and hosted by the Commission;
- The average yearly hosting cost is 20,000 euros per ECI;
- The configuration of a new ECI requires on average 3 days of a system administrator and 1 day of a developer;
- Certification costs are equal to 10,000 euros per ECI for the online collection software instances hosted in DIGIT data centre.

As a result, the costs for the Commission for the AS IS are estimated as follows:

		AS IS				
		Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**
European Commission	**Infrastructure**	**€ 330,000**	**€ 330,000**	**€ 330,000**	**€ 330,000**	**€ 330,000**
	Hosting	€ 330,000	€ 330,000	€ 330,000	€ 330,000	€ 330,000
	Fees/Licenses	€ -	€ -	€ -	€ -	€ -
	Development	***€ -***	***€ -***	***€ -***	***€ -***	***€ -***
	OCS Back-end					
	OCS Front-end					
	EU File Sharing Service interface					
	OCR Reader integration					
	eIDAS integration					
	Register integration					
	Maintenance	***€ 224,000***	***€ 224,000***	***€ 422,000***	***€ 422,000***	***€ 422,000***
	OCS	€ 198,000	€ 198,000	€ 198,000	€ 198,000	€ 198,000
	Register			€ 198,000	€ 198,000	€ 198,000
	Tools & frameworks	€ 26,000	€ 26,000	€ 26,000	€ 26,000	€ 26,000
	Support & Operations	***€ 70,500***	***€ 70,500***	***€ 70,500***	***€ 70,500***	***€ 70,500***
	ECI Instance Configuration	€ 42,000	€ 42,000	€ 42,000	€ 42,000	€ 42,000
	Helpdesk	€ 28,500	€ 28,500	€ 28,500	€ 28,500	€ 28,500
	Certification	***€ 150,000***	***€ 150,000***	***€ 150,000***	***€ 150,000***	***€ 150,000***
	TOTAL	**€ 774,500**	**€ 774,500**	**€ 972,500**	**€ 972,500**	**€ 972,500**
	TOTAL ACCRUED	**€ 774,500**	**€1,549,000**	**€2,521,500**	**€3,494,000**	**€4,466,500**

Table 8: Costs estimates for the Commission – AS IS[46]

The total cost of the AS IS situation over a period of 5 years is 4,466,500 euros.

Then, the costs of the first scenario were estimated. The following assumptions were made and apply to all three scenarios under assessment:

[46] In all costs table, OCS is to be understood as online collection software.

- Several developments are common to all scenarios:
    - e-TrustEx interface (for using the EU File Sharing Service): the necessary set-up per ECI is taken into account in the operational costs (although its costs may slightly differ depending on the architecture chosen for each scenario);
    - eIDAS integration: the online collection software will access the eIDAS network through EU Login, which implements the eIDAS interface for the Commission;
- The full-fledged option for the licensing costs of EU File Sharing Service is chosen (GUI User + Access Point):
    - GUI User: 28 MS * € 490 = € 13,720 per year
    - eDelivery Access Point: 28 MS * € 4,400 = € 123,200 per year
- Certification costs are no longer considered (for systems hosted by the Commission).

The following assumptions apply only to scenario 1:

- Out of the 20 ECIs, it is assumed that 15 are implemented with the Commission's online collection software and hosted by the Commission;
- The average yearly hosting cost is 15,000 euros per ECI;
- The configuration of a new ECI requires on average 5 days of a system administrator and 2 days of a developer;
- Register integration: this is limited to the improvement of the navigation between the Register and each ECI by adding a link between the entry in the Register to their corresponding support website as well as the dissemination towards social networks;
- No integration with an OCR reader tool is foreseen.
- Maintenance costs of the online collection software is expected to be reduced by 50% compared to the AS IS and a small amount is also foreseen for the maintenance of the Register.
- Helpdesk costs are unchanged compared to the AS IS.

As a result, the costs for the Commission of the scenario 1 are estimated as follows:

		Scenario 1				
		Year 1 (2019)	Year 2	Year 3	Year 4	Year 5
European Commission	**Infrastructure**	**€ 470,000**	**€ 535,000**	**€ 535,000**	**€ 535,000**	**€ 535,000**
	Hosting	€ 330,000	€ 255,000	€ 255,000	€ 255,000	€ 255,000
	Fees/Licenses	€ 140,000	€ 280,000	€ 280,000	€ 280,000	€ 280,000
	Development	***€ 246,100***	***€ -***	***€ -***	***€ -***	***€ -***
	OCS Back-end					
	OCS Front-end					
	EU File Sharing Service interface	€ 98,440				
	OCR Reader integration					
	eIDAS integration	€ 98,440				
	Register integration	€ 49,220				
	Maintenance	***€ 224,000***	***€ 144,800***	***€ 144,800***	***€ 144,800***	***€ 144,800***
	OCS	€ 198,000	€ 99,000	€ 99,000	€ 99,000	€ 99,000
	Register		€ 19,800	€ 19,800	€ 19,800	€ 19,800
	Tools & frameworks	€ 26,000	€ 26,000	€ 26,000	€ 26,000	€ 26,000
	Support & Operations	***€ 70,500***	***€ 101,580***	***€ 101,580***	***€ 101,580***	***€ 101,580***
	ECI Instance Configuration	€ 42,000	€ 73,080	€ 73,080	€ 73,080	€ 73,080
	Helpdesk	€ 28,500	€ 28,500	€ 28,500	€ 28,500	€ 28,500
	Certification	***€ -***	***€ -***	***€ -***	***€ -***	***€ -***
	TOTAL	**€ 1,010,600**	**€ 781,380**	**€ 781,380**	**€ 781,380**	**€ 781,380**
	TOTAL ACCRUED	**€ 1,010,600**	**€1,791,980**	**€2,573,360**	**€3,354,740**	**€4,136,120**

Table 9: Costs estimates for the Commission- scenario 1

The total cost of scenario 1 for the European Commission over a period of 5 years is 4,136,120 euros.

4.6.2 Organisers

In the AS IS situation, some costs are incurred by organisers whenever they choose not to use the online collection software provided by the Commission or not to host their online collection software in DIGIT data centre.

The following assumptions were made for the AS IS situation based on the data collected by Kurt Salmon:

- Out of the 20 ECIs, it is assumed that 5 are implemented by the organisers without using the Commission's online collection software and the hosting provided by the Commission;
- The average yearly hosting costs are 10,000 euros per ECI;
- No development costs are considered as an alternative software is already available (besides the one of the Commission);
- Maintenance represents 15% of the initial development costs of the more expensive solution (130,000 euros);
- Support costs were estimated by the organisers;
- Certification costs range from 5,000 to 10,000 euros depending on the countries. Thus, an average of 7,500 euros was considered.

The table below summarises the estimates of those costs

		AS IS				
		Year 1	Year 2	Year 3	Year 4	Year 5
Organisers	Infrastructure	€ 50,000	€ 50,000	€ 50,000	€ 50,000	€ 50,000
	Development	€ -	€ -	€ -	€ -	€ -
	Maintenance	€ 19,500	€ 19,500	€ 19,500	€ 19,500	€ 19,500
	Support & Operations	*€ 20,000*	*€ 20,000*	*€ 20,000*	*€ 20,000*	*€ 20,000*
	Certification	*€ 37,500*	*€ 37,500*	*€ 37,500*	*€ 37,500*	*€ 37,500*
	TOTAL	€ 127,000	€ 127,000	€ 127,000	€ 127,000	€ 127,000

Table 10: Costs estimates for organisers (for 5 initiatives) – AS IS

For scenario 1, the assumptions are identical to the AS IS and certification costs are still borne by organisers for the ECIs hosted at third party providers.

		Scenario 1				
		Year 1	Year 2	Year 3	Year 4	Year 5
Organisers	Infrastructure	€ 50,000	€ 50,000	€ 50,000	€ 50,000	€ 50,000
	Development	€ -	€ -	€ -	€ -	€ -
	Maintenance	€ 19,500	€ 19,500	€ 19,500	€ 19,500	€ 19,500
	Support & Operations	*€ 20,000*	*€ 20,000*	*€ 20,000*	*€ 20,000*	*€ 20,000*
	Certification	*€ 37,500*	*€ 37,500*	*€ 37,500*	*€ 37,500*	*€ 37,500*
	TOTAL	€ 127,000	€ 127,000	€ 127,000	€ 127,000	€ 127,000

Table 11: Costs estimates for organisers (for 5 initiatives) – scenario 1

Table 12 summarises the scores of the costs analysis.

Evaluation Criteria	Category	Score	Description
Costs Commission	Infrastructure	●●●○○	• Lower ECI unit hosting cost but some additional costs, such as the EU File Sharing Service fees
	Development	●●●○○	• Investment of 250,000 € should be made to configure the online collection software for a permanent hosting in DIGIT data centre and to add new functionalities.
	Maintenance	●●●●●	• Savings both in online collection software and Register
	Support	●●●○○	• Slightly higher than the AS IS as some additional configuration should be done for each ECI due to the new functionalities
Costs Organisers	Infrastructure	●●●○○	• Similar to AS IS situation
	Development	●●●○○	• Similar to AS IS situation
	Maintenance	●●●○○	• Similar to AS IS situation
	Support	●●●○○	• Similar to AS IS situation

Table 12: Overview of the costs analysis - scenario 1

4.7 SUMMARY OF ADAPTATIONS REQUIRED IN THE IMPLEMENTING REGULATION 1179/2011

To implement scenario 1, the following sections should be modified in Implementing Regulation (EU) 1179/2011:

- In recital 5, any reference to Directive 95/46/EC shall be replaced by a reference to Regulation (EU) 2016/679. It is also suggested to mention the responsibility of the third party or the European Commission, as online collection software hosting providers in ensuring the implementation of the requirements laid down in the technical specifications.
- In the Annex – section 1, in addition to the use of 'Captcha', it is recommended to state that extra measures against the automated submission of statements of support should be implemented, such as session identification, detection of html rendering, honeypot on the form, detection of non-human times and machine identification and/or input validation.
- In section 2.7.6(d), it is recommended to include the implementation of a generic error webpage for all exceptions. It should be done without displaying confidential data, to prevent the exposure of confidential information such as system access routes to local files or any internal information of the system should be hidden.
- Section 2.7.7 should specify how encryption keys should be managed and stored. Also it is necessary to mention that keys must be protected in both volatile and persistent memory (ideally processed in cryptographic modules). Keys shall never be stored in plain text format and should be stored in a cryptographic vault (HSM or isolated service).
- In section 2.7.9(b), it is advised to include properly parameterised flags such "HttpOnly", "Domain" and "Path", "Expire" and "Max-Age".
- In section 2.10, it is recommended to clarify that the data provided is only accessible to the organisers, the citizen concerned and the Member States competent authorities.
- In section 2.11, it is advised to mention that the integrity of the information must also be guaranteed for the mechanisms detailed in sections 3.1 and 3.2.
- In section 2.12, it is advised to specify the signatories' right to access to their information, in accordance to Articles 16 and 17 of the GDPR. Signatories can, after submitting the data during the session in which they complete the statement of support form, request the organisers, considered as data controllers, to rectify or erase inaccurate their personal data.
- In section 2.13, it is suggested to indicate an additional backup outside of the system hosting the online collection software, either on a different disk belonging to another server within the hosting/housing or in an alternate site such as the Commission disaster recovery site.
- In section 2.17, it is advised to include further controls concerning physical security such as physical parameters (against external threats) and cabling security.
- In section 2.18.1, it is recommended to clarify that only the presentation layer is intended to be deployed on the demilitarised zone (DMZ). Other layers shall be protected at a higher level in the militarised zone.
- Section 2.18.5 (a) & (d) may not be necessary as they depends on the network configuration and may not be applicable to all hosting providers.

- In section 2.20.2, it is advised to clarify that the organisers shall have an antimalware solution.
- In section 3.2, it is recommended to include a data integrity control check with a hash function.
- In section 3.4, it is recommended to detail the valid secure options such as VPN with TLS, Ipsec or FTPS.

5 SCENARIO 2

5.1 DESCRIPTION

In scenario 2, the online collection software and hosting is only provided by the European Commission. This scenario evaluates the feasibility and impact of allowing only the current European Commission's online collection software and infrastructure for collecting statements of support, from a legal, organisation, technical, security and costs perspective. Such as in scenario 1, each online collection system is provided as a standalone instance, although sharing of some internal resources and processes is envisaged at infrastructure and operational levels.

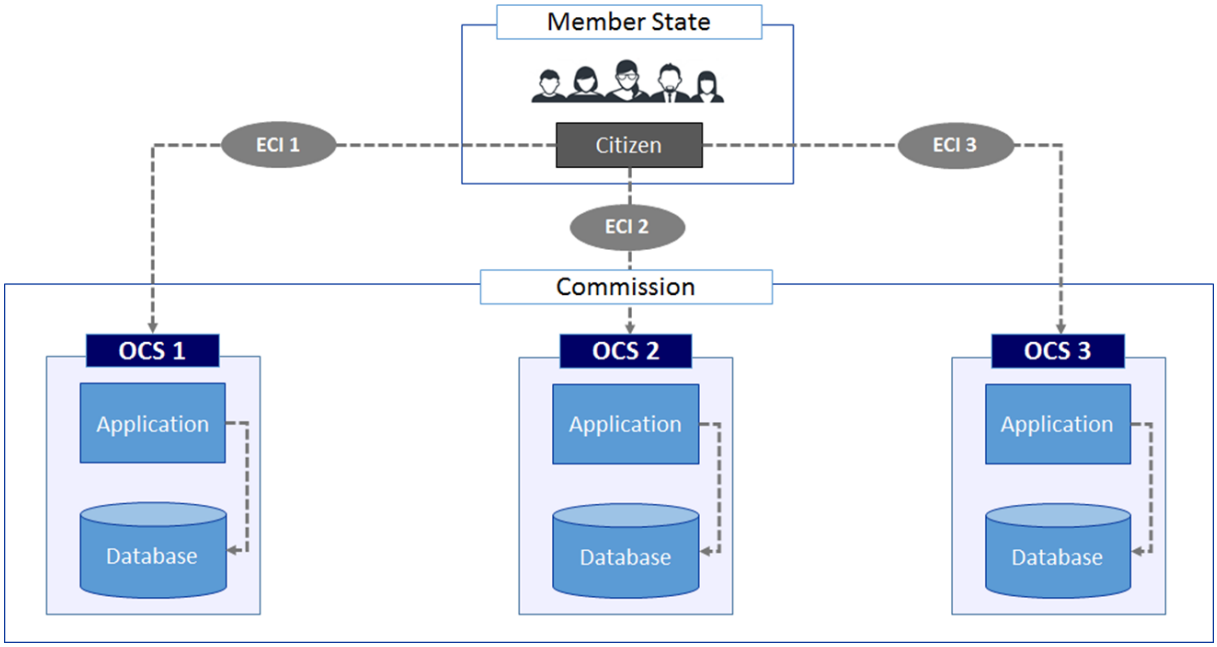


Figure 9: Architecture of scenario 2

Figure 9 represents the architecture of scenario 2. In this case, the various standalone online collection systems are hosted only by the European Commission.

5.2 LEGAL ANALYSIS

Please refer to section 4.2 Legal analysis for a description of the key novelties, introduced by the GDPR, and also reflected in the Regulation 45/2001 currently under revision that are relevant for the ECI Regulations. The sections below analyse the specific impact of these changes in the light of the proposed architecture for scenario 2.

5.2.1 Specific implications for scenario 2

Impact on data protection roles

In scenario 2, the following ECI stakeholders maintain the same role in terms of data protection obligations as in scenario 1:

- The citizen who supports an ECI (*data subject*)
- The national data protection authorities (as *supervisory authorities*[47])

[47] Refer to section 4.2.1 for the new figure of the 'lead supervisory authority' established by the GDPR in case of cross-border processing of personal data.

- The competent authorities in the Member States, who act as verifiers of the statements of support received (acting as *data controllers* when validating the statements of support received).

As in scenario 1, there is a new stakeholder that joins the data protection chain in certain circumstances: the Data Protection Officer (see section 4.2.1).

The main difference between scenario 1 and 2 relates to the roles performed by the organiser and the European Commission, which vary depending on the format in which statements of support are collected (i.e. online and/or in paper). The analysis that follows also takes into account the paper format, even if the focus of this study are the changes implied by the online collection system.

For paper statements of support

In scenario 2, when statements of support are collected *in paper*, the organiser is responsible for collecting and storing the statements of support, as it is already the case in the current situation, and therefore remains the *data controller*. In addition to collecting them in a secure manner, the organiser is responsible for making them available to the competent authorities in the Member States for their verification, and for doing so in compliance with the appropriate technical and security standards.

There is however the possibility within scenario 2 that organisers are required to scan the statements of support in paper, which they have collected themselves, and to upload them to the online collection system hosted by the European Commission. In this case, the Commission would be responsible for sending these statements of support together with the other statements of support directly collected online through its online collection system to the national competent authorities, without any further involvement of the organisers.

In terms of responsibilities, this would mean that the organiser would still remain *data controller* with regard to the personal data collected in the statements of support received in paper format. However, the Commission would become the *data processor* for these paper statements of support, as soon as they are uploaded to its online collection system, and would also be responsible for transmitting them to the competent authorities in the Member States, thereby reducing responsibility of the organiser at this processing phase. This is so in accordance with Regulation 45/2001 on the processing of personal data by EU institutions and bodies, currently under review to comply with the GDPR principles.

Summary: When statements of support are collected in paper, the organiser remains data controller (together with the national competent authorities verifying the statements of support). The European Commission may acquire the role of data processor if a requirement is introduced for these statements of support to be scanned and uploaded by organisers to its online collection system. In such case the Commission is also responsible for transmitting them to the competent authorities in the Member States together with the online statements of support, thereby reducing the responsibility of the organiser at this processing phase.

For online statements of support

The situation changes when statements of support are collected online. Compared to scenario 1, scenario 2 does not foresee any third party organisation acting as a hosting provider of the online collection software: The Commission alone provides both the online collection software and hosts the statements of support in its data centre by default. The third party disappears thus from the data protection chain (see Figure 10).

Another key feature of this scenario, compared to scenario 1, is the fact the Commission becomes 'data controller' when processing online statements of support, whilst in scenario 1 it was acting only as 'data processor', under the instructions of the organiser.[48] This is explained at least based on the following grounds:

- First, the organiser no longer has as in scenario 1 a possibility to either choose the software or the hosting provider of the online collection system: these services are provided by default by the European Commission. Therefore, the organiser no longer has the possibility to *determine the means* of the processing of personal data;
- Second, in scenario 1 the organiser had the ultimate responsibility for ensuring the security and compliance of the online collection system, while here the Commission is fully in charge of the compliance with the security requirements;
- Finally, the organiser no longer has the right to access and consult the processed personal data, as it is the Commission that stores the data and sends the online statements of support received directly to the competent authorities in the Member States for their verification, with no involvement of the organiser. The organiser still has a possibility to monitor the progress of the number of statements of support received through a dedicated dashboard, but he/she no longer has access to the personal data collected – a key difference compared to scenario 1.

Summary: When statements of support are collected online, the Commission is responsible alone as data controller, with no involvement of the organiser. The competent authorities in the Member States also remain data controllers for the purposes of the verification of the collected statements of support. The absence of a meaningful role of the organiser in this case is shown in Figure 10 by means of a diagonal shading.

[48] In scenario 1, the organiser is considered as data controller for both paper and online statements of support, while the European Commission or the third party providing the hosting of the online collection software act as data processors for the online statements of support (see section 4.2.3).

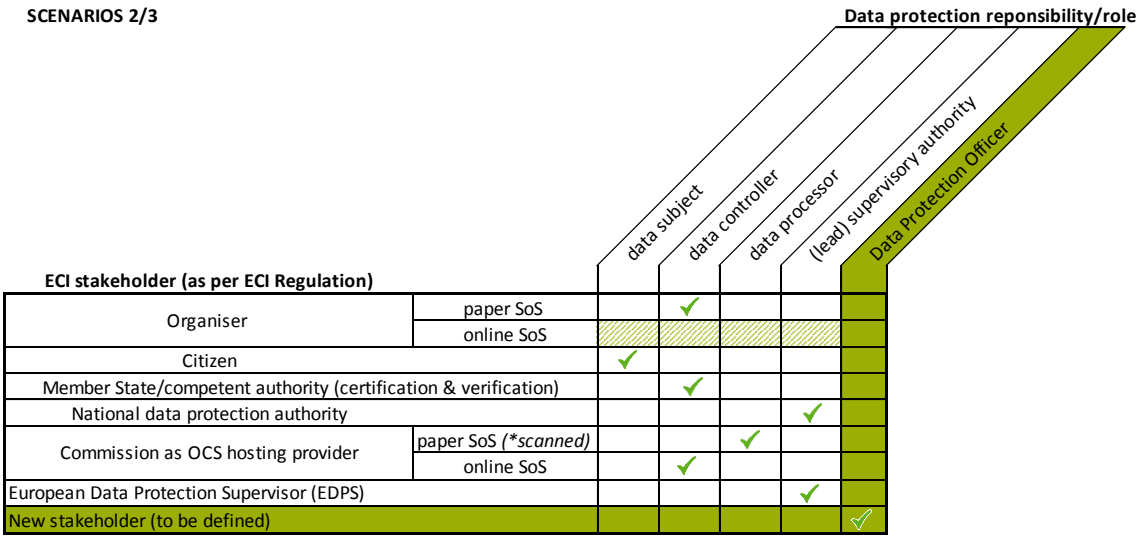


Figure 10: ECI stakeholders and responsibilities based on GDPR - Scenarios 2 and 3[49]

Impact on liabilities

- In scenario 2, **when collecting statements of support in paper**, **the organisers are liable** for any damage caused to the data subjects who gave them their statements of support, **together with the national competent authorities**, if the latter create any damage to the data subject when verifying and certifying the statements of support transferred to them by the organisers. If the statements of support collected in paper are scanned and uploaded by the organisers to the online collection system managed by the European Commission, the latter becomes data processor for these statements of support and may be held responsible for any damage caused when processing them and later transmitting them to the competent authorities at national level;

- **When collecting statements of support online**, **only the Commission and the national competent authorities** for verifying and certifying the statements of support **can be held liable** as data controllers for any damage caused as a result of an infringement of their data protection obligations.[50] **Organisers are exempt from any liability** in this case, given their no-role in terms of data protection obligations arising from the GDPR.

[49] In the figure displayed, the green diagonal shading indicates no particular role in the data protection chain.
[50] As laid down in Articles 65 and 69 of the proposed revised Regulation 45/2001 (applicable to the European Commission) and Articles 82 GDPR (applicable to the national competent authorities).

Evaluation Criteria	Stakeholder	Score	Description
Impact of GDPR/Regulation (EC) No 45/2001 under revision on ECI stakeholders	European Commission	●●●●○	• The online collection software hosting is always provided by the European Commission. • The European Commission is considered as data controller for the statements of support collected online. • The European Commission can be considered as data processor for statements of support collected in paper once they have been scanned and uploaded to its online collection system by organisers.
	Competent Authorities (and data protection authorities in Member States)	●●●●○	• The competent authorities are considered as data controllers when verifying and certifying both the statements of support collected in paper and online. • The data protection authorities in the Member States are considered as supervisory authorities and a lead supervisory authority is established by GDPR as a one-stop-shop for the cross-border processing of personal data.
	Organisers	●●●●○	• Organisers are considered as data controllers only for the statements of support collected in paper. • Organisers do not have any (meaningful) data processing role when statements of support are collected online.
Impact on liabilities	European Commission	●●●●○	• Under the previous data protection rules, only data controllers were liable in case of damages caused to the data subject when processing their data. • According with the new GDPR and Regulation 45/2001 under revision, both data controllers and data processors may face liabilities in proportion to their role. • The possibility to impose administrative fines by the supervisory authorities/EDPS to the data controller and the data processor is now foreseen in case of non-respect of their data protection obligations. • The European Commission may now face liabilities as data processor (for scanned paper SoS), and also as data controller (for online SoS)
	Competent Authorities		
	Organisers		

Table 13: overview of the legal analysis - scenario 2

5.3 ORGANISATION ANALYSIS

5.3.1 Convenience

Scenario 2 does not involve third party organisations. Hence, the convenience of the scenario is higher as the European Commission, in this case, is the only entity in charge of the Online Collection System.

According to this scenario:

- The online collection system is considered as de facto certified. Consequently, compared to the current situation, the ECI process is shortened and there is no need to prepare the documentation for the certification anymore;
- Ensuring that the personal data collected are not used for any other purpose than the indicated support for an initiative, as well as ensuring the implementation of the appropriate technical and organisation measures to protect personal data is the responsibility of the data controllers.
- The statements of support are collected both online and in paper. In order to ease the process, the ones collected in paper could be scanned by the organisers, outside of the system, and then uploaded to the online collection system. Online forms are then sent to the competent authorities by the Commission while the process to send the paper forms stays similar to the current situation.

However, in case paper statements of support are scanned, the responsibility to send them to the respective Member States could be switched to the Commission. There would be therefore a shared responsibility between the organisers and the European Commission. In this case, an online dashboard should be developed, allowing the organisers to have a view on the amount of statements of support collected.

5.3.2 Certification

In this scenario, the online collection system of the European Commission is considered as de facto compliant with the ECI Regulation and the Implementing Regulation (EU) 1179/2011 as well as with the Commission Decision (EU, Euratom) 2017/46. It is however questionable whether an Implementing Regulation is necessary under this scenario, given that no third party systems are possible and no certification is needed.

5.3.3 Verification

The respective Member States are responsible for the verification of the personal data for the purpose of certifying the number of valid statements of support (ECI Regulation, Articles 5.3 and 8.2). Compared to scenario 1, the responsibility to send the statements of support to the competent authorities is switched from the organisers to the European Commission.

The verification process could benefit from the EU File Sharing Service (see section 3.4), to securely exchange digital documents from one system to another. This platform allows to replace paper documents or files stored on DVDs and CDs by a secure and digitised system-to-system exchange of information. It could be used to implement a secure transmission of the statements of support from the organisers to the competent authorities. In addition to providing a secure transmission, the EU File Sharing Service could also offer the possibility to automate the sending of those support and therefore simplify and accelerate the process.

Evaluation Criteria	Stakeholder	Score	Description
Convenience	European Commission	●●●●○	• No third party is involved, the Commission always provides the online collection system. • A dashboard could be developed by the Commission for the organisers to have a view on the amount of statements of support collected.
	Competent Authorities		• n/a
	Organisers	●●●○○	• The statements of support collected in paper could be scanned by the organisers and uploaded on the online collection system. • When statements of support are collected online, the organisers do not have any responsibility.
Certification	European Commission	●●●●●	• The online collection system of the European Commission is considered as de facto compliant with the ECI Regulation and the Regulation ((EU) 1179/2011).
	Competent Authorities	●●●●●	
	Organisers	●●●●●	
Verification	European Commission	●●●●●	• The European Commission sends the online statements of support to the Member States competent authorities. • This process could benefit both from the scan functionality and EU file transfer service to increase the security and efficiency of the transmission of statements of support.
	Competent Authorities	●●●●○	• The national competent authorities verify the statements of support.
	Organisers	●●●○○	• The organisers are responsible for scanning the statements of support collected in paper and upload them to the online collection system.

Table 14: overview of the organisation analysis - scenario 2

5.4 TECHNICAL ANALYSIS

5.4.1 Implementation

Considering the Commission's online collection software, scenario 2 is identical to scenario 1. The considerations made in the assessment of scenario 1 are therefore also applicable to scenario 2. The scoring of the evaluation criteria improves slightly as the absence of third party online collection software provider facilitates all aspects of the implementation. In addition, the certification process is not applicable anymore (see section 5.3.2). Nonetheless, regular audits are recommended to ensure that security requirements are enforced.

5.4.2 Operations

The operational aspects of scenario 2 are similar to scenario 1. A positive impact on the system administration is reported as only the Commission's online collection system must be monitored.

The results of the assessment are summarised in the Table 15 hereunder.

Evaluation Criteria	Category	Score	Description
Implementation	Installation	●●●◐○	• The source code is in a pom.xml file, easing the installation. It is prepared to be used by the most widely used Java compilation environment: maven.
	Scalability	●●●●○	• The online collection software, in a physical or virtual server, fully achieve its objective. • Each ECI requires an individual server.
	Maintenance	●●●◐○	• In the short term, changes are foreseen to integrate and deploy the new front-end. • On the long term, other modifications can be anticipated, such as the integration of eID.
Operations	System administration	●●●◐○	The following activities are covered: • Installation of the system; • Update of the software based on discovered flaws and security breaches, revision of log files during the life-cycle of the system; • Disposal/migration.
	Verification process	●●●○○	• This scenario offers no improvement of the verification process.

Table 15: overview of the technical analysis - scenario 2

5.5 SECURITY ANALYSIS

5.5.1 Security architecture

In this scenario, the Commission is responsible for the compliance of its online collection system with the ECI Regulation. The system will be centralised up to a certain extent for a better management of possible security breaches (physical or logical). However, if a vulnerability affecting the hosting service and data centre is exploited, it may impact every online collection system deployed on it.

In case of unauthorized access with system administrator permissions to the Commission's hosting service, all the online collection systems would be exposed. For political reasons, the online collection systems may be the target of sophisticated cyber-attacks. As it is part of European Commission infrastructure, this aspect should always be kept in mind when analysing a threat or attack.

Potential improvements of the security architecture include:

- Logically isolating (separate private networks) the online collection system within the data centre of the Commission from other applications outside the ECI;
- Performing audits and/or penetration tests in the systems;
- The hosting service should be maintained and monitored. If a failure or an attack is detected, it is must be managed for all online collection systems contained therein.

The aspects for improvement, developed in scenario 1 (see section 4.5.1) are also applicable to this scenario.

5.5.2 Software development security

It is recommended to implement an incremental approach towards security in order to increase the security level over time as the online collection system is getting more mature.

The aspects for improving the Regulation, developed in scenario 1 (see section 4.5.2), also apply to this scenario.

5.5.3 Data security & integrity

The aspects for improving the Regulation, developed in scenario 1 (see section 4.5.3), also apply to this scenario.

5.5.4 Identity and access management

For centralised applications, the provisioning of accounts presents an opportunity for an attacker to create a valid account without proper identification and authorisation processes. OWASP provides recommendations to address this risk in the following guidelines:

- https://www.owasp.org/index.php/Test_Account_Provisioning_Process_(OTG-IDENT-003)
- https://www.owasp.org/index.php/Test_User_Registration_Process_(OTG-IDENT-002)

Those guidelines aim at:

- Verifying that the identity requirements for user registration are aligned with business and security requirements;
- Validating the registration process.

Evaluation Criteria	Stakeholder	Score	Description
Security architecture	European Commission	●●●●○	• The Commission's hosting service and data centre are compliant with the ECI Regulation, and centralised for a better management of possible security breaches.
	Competent Authorities	●●●●○	• Communications with the Commission's servers and data centre is less changeable in security configurations (both perimetral systems and the online collection system itself).
	Organisers	n/a	• n/a
Software development security	European Commission	●●●●○	• The European Commission develops, maintains and improves an online collection system that is considered as de facto compliant with the ECI Regulation and the Regulation ((EU) 1179/2011).
	Competent Authorities	●●●●○	• The integration with the EU File Sharing Service is the only piece of software that needs to be developed by the Member States.
	Organisers	n/a	• n/a
Data security & integrity	European Commission	●●●●○	• The storage and sending of the data collected in the Commission's online collection system, for the verification by the Member States, is done under the sole responsibility of the Commission and complies with Commission Decision (EU, Euratom) 2017/46.
	Competent Authorities	●●●●○	• The reception and storage of the data collected from the Commission's online collection system of each initiative (exported data), for the verification, is done in accordance with national regulations for IT security.
	Organisers	●●●●○	• A malicious organiser (insider) could try to hack the Commission's online collection system exploiting a possible vulnerability to manipulate the data.
	External user	●●●●○	• A malicious client user (outsider) could try to hack the Commission's online collection system exploiting a possible vulnerability to manipulate the data.
Identity and access management	European Commission	●●●●○	• The access of the Commission, as an admin role, has several security requirements in the Annex of the Implementing Regulation – section 2.7.3 h.
	Organisers	●●●●○	• The organisers have a limited access to the online collection system , with no direct access to the personal data collected online.

Table 16: overview of the security analysis - scenario 2

5.6 COSTS ANALYSIS

5.6.1 European Commission

Common assumptions for the estimates are detailed in scenario 1 (see section 4.6.1)

The following assumptions apply only to scenario 2:

- It is assumed that all 20 ECIs are implemented with the Commission's online collection software and hosted by the Commission;
- The average yearly hosting cost is 15,000 euros per ECI;
- Licensing fees are considered for EU File Sharing Service, eIDAS, and the OCR software for a total of 300,000 euros;
- The configuration of a new ECI requires on average 8 days of a system administrator and 3 days of a developer;
- Integration with an OCR reader tool is foreseen and costs will be similar to the EU File Sharing integration;

- Register integration: full integration is considered, giving the opportunity to merge the online collection software and the Register into a single software, allowing automation of the deployment of the ECI website from the Register. After the automated deployment, customisation of the stylesheets and other graphical elements are the only things to do in order to have an online collection software instance up and running. This also allows to reduce drastically the costs of helpdesk. The additional benefit of not having to maintain the Register is not taken into account for this assessment;
- Maintenance costs of the online collection software is expected to be reduced by 25% compared to the AS IS, but additional costs are considered for the maintenance of the Register (180 days per year);
- Support and helpdesk costs are expected to be tripled compared the AS IS situation because of the support for the Register and increase of ECI.

As a result, the costs for the Commission of the scenario 2 are estimated as follows:

			Scenario 2				
			Year 1 (2019)	Year 2	Year 3	Year 4	Year 5
European Commission	**Infrastructure**		**€ 500,000**	**€ 630,000**	**€ 630,000**	**€ 630,000**	**€ 630,000**
		Hosting	€ 330,000	€ 330,000	€ 330,000	€ 330,000	€ 330,000
		Fees/Licenses	€ 170,000	€ 300,000	€ 300,000	€ 300,000	€ 300,000
	Development		***€ 356,845***	***€ 110,745***	***€ -***	***€ -***	***€ -***
		OCS Back-end					
		OCS Front-end					
		EU File Sharing Service interface	€ 73,830				
		OCR Reader integration	€ 73,830				
		eIDAS integration	€ 98,440				
		Register integration	€ 110,745	€ 110,745			
	Maintenance		***€ 224,000***	***€ 273,500***	***€ 273,500***	***€ 273,500***	***€ 273,500***
		OCS	€ 198,000	€ 148,500	€ 148,500	€ 148,500	€ 148,500
		Register		€ 99,000	€ 99,000	€ 99,000	€ 99,000
		Tools & frameworks	€ 26,000	€ 26,000	€ 26,000	€ 26,000	€ 26,000
	Support & Operations		***€ 84,500***	***€ 214,240***	***€ 214,240***	***€ 214,240***	***€ 214,240***
		ECI Instance Configuration	€ 56,000	€ 153,440	€ 153,440	€ 153,440	€ 153,440
		Helpdesk	€ 28,500	€ 60,800	€ 60,800	€ 60,800	€ 60,800
	Certification		***€ -***	***€ -***	***€ -***	***€ -***	***€ -***
	TOTAL		**€ 1,165,345**	**€1,228,485**	**€1,117,740**	**€1,117,740**	**€1,117,740**
	TOTAL ACCRUED		**€ 1,165,345**	**€2,393,830**	**€3,511,570**	**€4,629,310**	**€5,747,050**

Table 17: Costs estimates for the Commission - scenario 2

The total cost of scenario 2 for the European Commission over a period of 5 years is 5,747,050 euros.

5.6.2 Organisers

For scenario 2, since the assumption is that all ECIs will be running on the online collection system of the Commission, organisers no longer incur any costs.

Table 18 summarises the scores of the costs analysis.

Evaluation Criteria	Category	Score	Description
Costs Commission	Infrastructure	●●●○○	• Similar to the AS IS situation. Lower ECI unit hosting cost but some additional costs, such as the EU File Sharing Service fees
	Development	●●●○○	• Half a million euros investment should be made to configure the online collection software for a permanent hosting in DIGIT data centre and to add new functionalities
	Maintenance	●●●●○	• Similar to AS IS situation
	Support	●●○○○	• Costs tripled due to support for all ECI and a wider set of features
Costs Organisers	Infrastructure	●●●●●	• Organisers no longer incur any costs
	Development	●●●●●	• Organisers no longer incur any costs
	Maintenance	●●●●●	• Organisers no longer incur any costs
	Support	●●●●●	• Organisers no longer incur any costs

Table 18: Overview of the costs analysis - scenario 2

5.7 SUMMARY OF ADAPTATIONS REQUIRED IN THE IMPLEMENTING REGULATION 1179/2011

As explained above, whether there is a need for an Implementing Regulation under this scenario is questionable. In any case, some adaptations in the technical specifications compared to the current ones would be needed for the implementation of this scenario.

The following sections need to be modified in Regulation (EU) 1179/2011 to implement scenario 2. As most of the modifications proposed for the Annex are similar to scenario 1, the reader should refer to section 4.7, except for the following paragraphs:

- Recital 5 should be rewritten to remove the reference to organisers and refer to Regulation (EC) 45/2001, or its revised version if applicable, as well as to Commission Decision (EU, Euratom) 2017/46.
- It is advised to supress recital 6 since the online collection system provided by the Commission is the only possibility for collecting statements of support online. The hosting of the online collection system is also provided by the Commission, with no involvement of organisers.
- In Annex – section 2.8, it is advised to mention that each online collection system instance shall be managed independently and logically separated.
- In section 2.12, it is advised to specify the signatories' right to access their information, in accordance with Regulation (EC) 45/2001, or its revised version if applicable . Signatories can, after submitting their personal data during the session in which they complete the statement of support form, request the organisers, as data controllers, to rectify any inaccurate information or to erase it.
- In sections 2.18.2 and 2.19.4, it is advised to mention that updates and patches should be installed, tested and validated on the testing environment before being applied in production.

6 SCENARIO 3

6.1 DESCRIPTION

Scenario 3 considers the online collection system as a single online platform. It evaluates the feasibility and impact of providing the online collection system as a single online platform managed by the Commission in a cloud-based centralised environment, from a legal, organisation, technical, and security point of view.

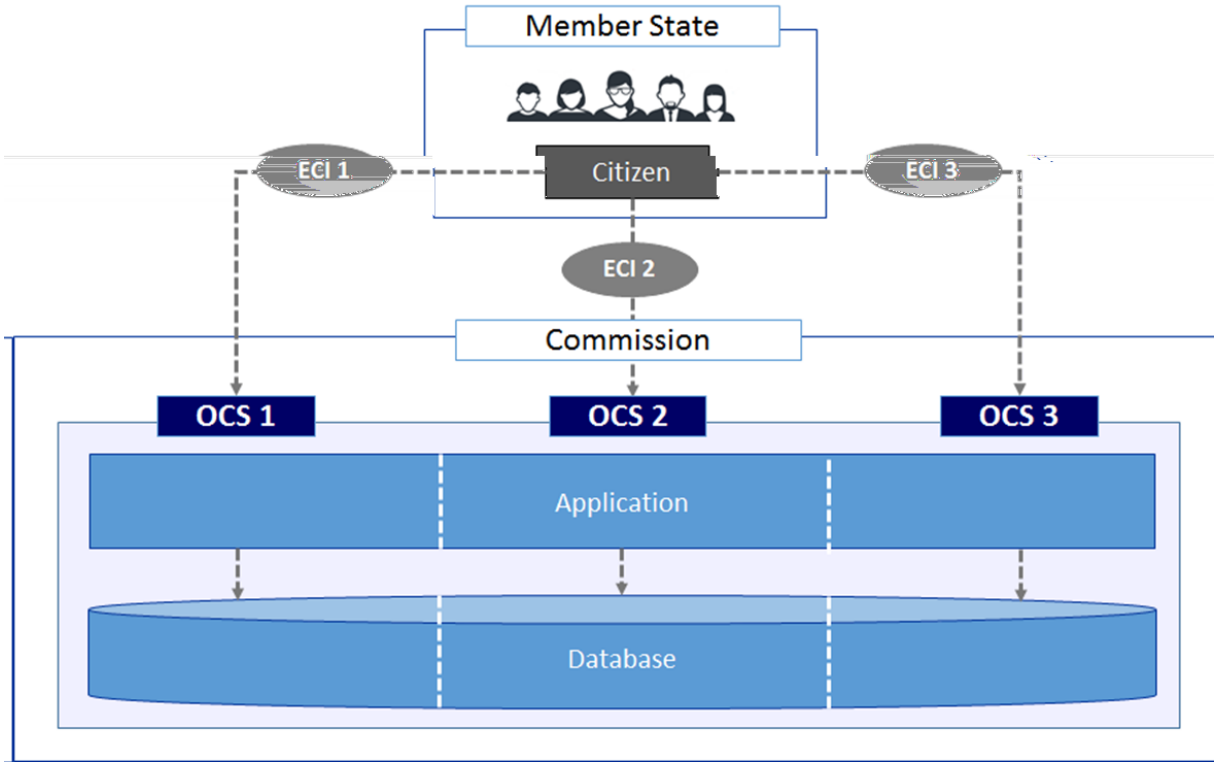
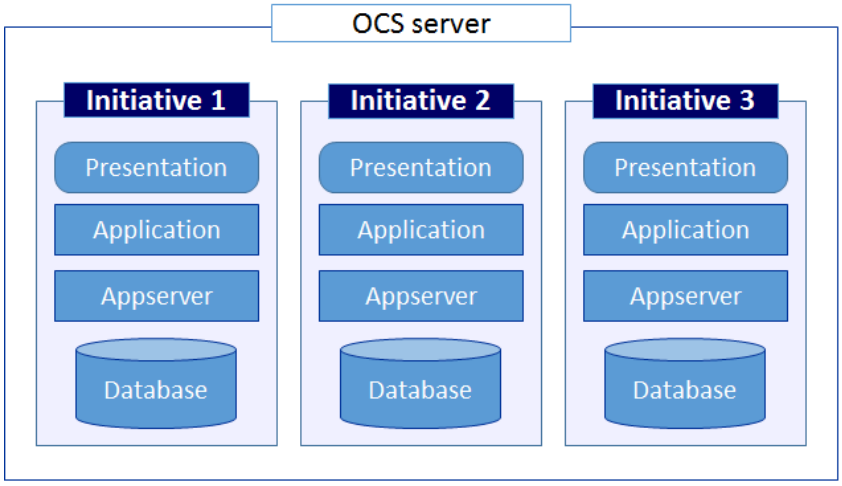


Figure 11: Architecture of scenario 3

Figure 11 shows the architecture of scenario 3, as a possible alternative to scenario 2, consisting in a centralised online platform, managed by the European Commission and logically divided into different online collection system.

Regarding the different Online Collection Systems, a number of variations of their implementation are possible. The most relevant ones are described in the sections below, namely, central server (option 1), central server and database (option 2), central server, database and business logic (option 3), and central software with partially specific presentation (option 4).

6.1.1 Central server



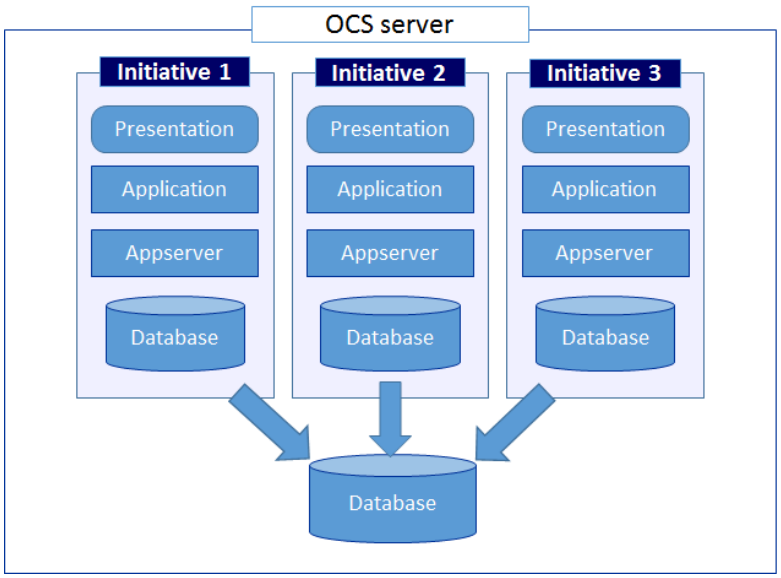
The common hardware and system software is used by separate instances of the appserver, one for each initiative, each with a different presentation layer, application software and database.

Figure 12: construction of the central server

In this construction (see Figure 12), the central server of the online collection system hosts all the instances of the initiatives in a separated way. In each instance, three layers are distinguished: the front-end or presentation layer, the business logic layer and the data layer.

Compared to scenario 2, this construction maintains the full flexibility of each initiative, while optimising some of the administrative tasks such as the login and the systems administration. However, the benefits of the centralisation remain minor as it still requires time, for example, to establish the online collection system for a new initiative.

6.1.2 Central server and database



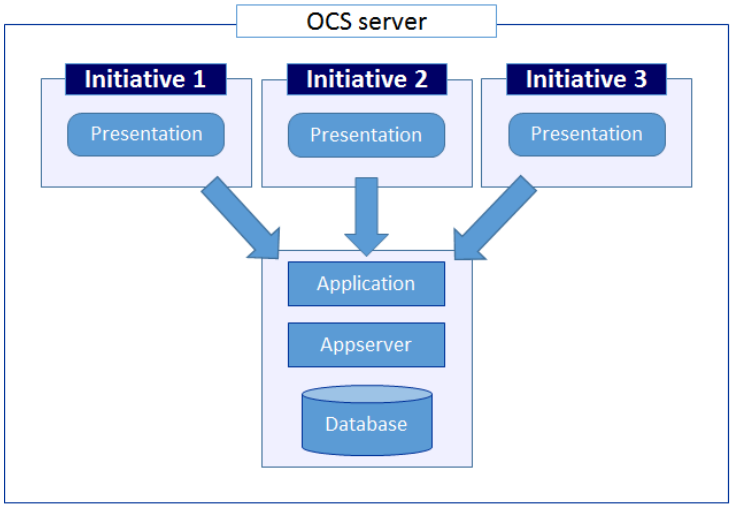
The common hardware and system software is used by separate instances of the appserver, one for each initiative, each with a different presentation layer and application software.

All initiatives use the same database for storing the statements of support. Statements of support of one initiative are separated from the statements of other initiatives by including the ID of the initiative in each row.

Figure 13: construction of the central server and database

In this construction (see Figure 13), the different initiatives share the same hardware, system software and database. Compared to the previous option (see 6.1.1), the database management tasks are highly reduced. However, the management of the application and its application server (appserver) are still not centralised, the effort required to establish a new ECI is therefore still significant.

6.1.3 Central server, database and business logic



All hardware and software in the OCS server is shared between the initiatives. The ID of the initiative allows to isolate the different initiatives in the online collection software, as well as in the database.

Each initiative may have its own presentation layer. Depending on the policy, this may be completely different (JSP, html, gif, jpg and CSS files), medium different (html, gif, jpeg and CSS files) or with limited differences (only gif, jpeg and CSS files).

Presentations of different initiatives are located in different directories in the server.

Figure 14: construction of the central server, database and business logic

This variation (see Figure 14) uses only one application server and one application and each initiative may have its own interface. Part of this interface layer could be implemented in the MVC platform embedded in the application server.

The interface could also vary depending on the level of constraint of the guidelines and policy defining the level of personalisation organisers can bring to personalise the files (JSP, html, jpg, gif, CSS).

This approach, more centralised than the others, reduces the burden of administrative tasks. However, it has the disadvantage of limiting the choice of user interface between the different initiatives.

The presentation could also vary depending on the policy:

- With a relaxed policy, the initiatives may have completely different aspects, allowing the organisers to personalise the JSP, html, jpg, gif, CSS files;
- With a moderately restrictive policy, only html, jpg, gif and CSS files can be changed;
- With a more restrictive policy, only jpg, gif and CSS files can be changed, limiting the differences in the presentation of the various initiatives.

Thanks to the main benefit of this implementation, the establishment of an instance of the online collection system for a new initiative can be a matter of minutes instead of days. Likewise, all other administrative tasks during the life-cycle of an initiative will also benefit from an enormous reduction of workload and an increase of the speed of service.

6.1.4 Central system with customisation of the presentation layer

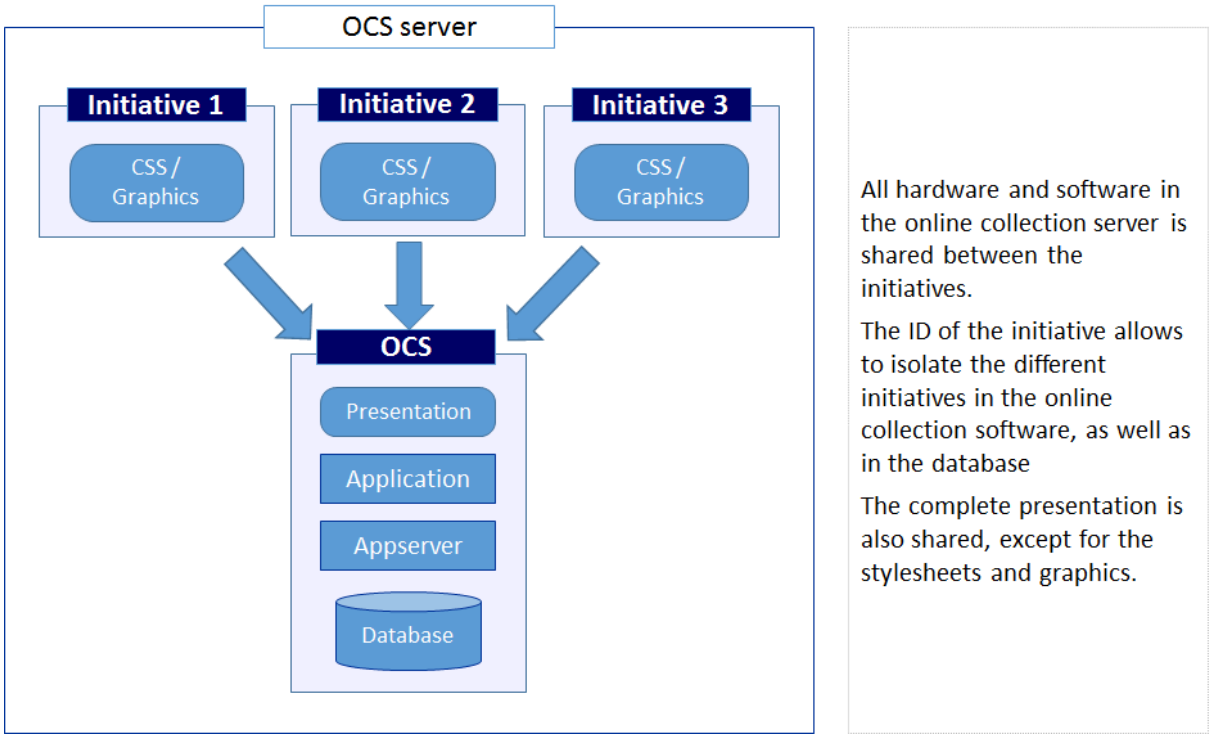


Figure 15: Central system with customisation of the presentation layer

This variation (see Figure 15) involves the unification of the complete online collection system, except for the contents of the graphics, e.g. the file logo.gif may contain a different graphic for one initiative than for others, but in all cases it would have the same filename.

6.1.5 Recommended implementation

The implementation described in 6.1.3 offers the best increase in terms of the speed of service and decrease in workload, while allowing enough freedom for the organisers to establish an attractive user interface for their initiative.

Although each implementation could allow for enhanced features, this option and the one described in 6.1.4 make the implementation of such features easier thanks to their centralisation. As a result, in the following sections, evaluation is done for the option 6.1.3, though in majority of the cases, the results do not differ much between options 6.1.3 and 6.1.4.

The enhanced features, which option 6.1.3 provides, include:

- Web tool for the administrators, integrating the most common administrative tasks in the online collection system, such as creating a new initiative, user/role administration, log revision, etc.;
- Auto-administration, allowing the organisers to personalise the user interface of their initiative by means of uploading / downloading files, retrieving statistics, closing initiatives, user administration, etc.;
- Periodic server signature on the database to guarantee its integrity;
- Facilities for remote invocation, for example embedding the support form in pages on other servers, using frames or iframes. The consequences of this feature on the security aspects, especially on Cross-Site scripting, should be analysed. As the embedded page should be able

to interact with the user, Web Services cannot be used in this case. However, embedding the page into other pages would result in the same or even better ease of use for the organisers, and a very similar experience for the user.

6.2 LEGAL ANALYSIS

Refer to section 5.2 for the legal analysis of scenario 3 as the legal analysis made for scenario 2 also applies to scenario 3. The proposed technical architecture for scenario 3 does not entail any new implications in terms of data protection roles and liabilities compared to scenario 2.

Evaluation Criteria	Stakeholder	Score	Description
Impact of GDPR/Regulation (EC) No 45/2001 under revision on ECI stakeholders	European Commission	●●●●○	• The online collection software hosting is always provided by the European Commission. • The European Commission is considered as data controller for the statements of support collected online. • The European Commission can be considered as data processor for statements of support collected in paper once they have been scanned and uploaded to its online collection system by organisers.
	Competent Authorities (and data protection authorities in Member States)	●●●●○	• The competent authorities are considered as data controllers when verifying and certifying both the statements of support collected in paper and online. • The data protection authorities in the Member States are considered as supervisory authorities and a lead supervisory authority is established by GDPR as a one-stop-shop for the cross-border processing of personal data.
	Organisers	●●●●○	• Organisers are considered as data controllers only for the statements of support collected in paper. • Organisers do not have any (meaningful) data processing role when statements of support are collected online.
Impact on liabilities	European Commission	●●●●○	• Under the previous data protection rules, only data controllers were liable in case of damages caused to the data subject when processing their data. • According with the new GDPR and Regulation 45/2001 under revision, both data controllers and data processors may face liabilities in proportion to their role. • The possibility to impose administrative fines by the supervisory authorities/EDPS to the data controller and the data processor is now foreseen in case of non-respect of their data protection obligations. • The European Commission may now face liabilities as data processor (for scanned paper SoS), and also as data controller (for online SoS)
	Competent Authorities		
	Organisers		

Table 19: overview of the legal analysis - scenario 3

6.3 ORGANISATION ANALYSIS

6.3.1 Convenience

In scenario 3, similarly to scenario 2, the European Commission is the only entity hosting the online collection software. The different aspects of this scenario are thus similar to scenario 2 (see 5.3.1). The same applies to the dashboard and scan functionalities.

In addition, this scenario offers the possibility to implement a Central Authentication Service, such as a Single Sign-On protocol. In this case, the citizen is only required to fill all his/her personal data the first time he/she authenticates him/herself to support an initiative. His/her personal data are then saved and re-used the next time he/she is authenticating his/herself to support an ECI.

6.3.2 Certification

The analysis of the evolution of the certification process of the online collection system in scenario 3 is similar to scenario 2 (see 5.3.2.).

6.3.3 Verification

Similarly to scenario 2 (see 5.3.3), scenario 3 could also benefit from the EU File Sharing Service to increase the security and efficiency of the transmission of statements of support.

Evaluation Criteria	Stakeholder	Score	Description
Convenience	European Commission	●●●●○	• No third party is involved, the EC provides the OCS as a single online platform. • A dashboard could be developed by the Commission for the organisers to have a view on the amount of statements of support collected.
	Competent Authorities		• n/a
	Organisers	●●●●○	• The statements of support collected in paper could be scanned by the organisers and uploaded on the online collection system. When they are collected online, the organisers do not have any responsibility. • A Central Authentication Service, a single sign-on protocol might be implemented.
Certification	European Commission	●●●●●	• The online collection system of the European Commission is considered as de facto compliant with the ECI Regulation and the Regulation ((EU) 1179/2011).
	Competent Authorities	●●●●●	
	Organisers	●●●●●	
Verification	European Commission	●●●●●	• The European Commission sends the online statements of support to the Member States competent authorities. • This process could benefit both from the scan functionality and EU file transfer service to increase the security and efficiency of the transmission of statements of support.
	Competent Authorities	●●●●○	• The national competent authorities verify the statements of support.
	Organisers	●●●○○	• The organisers are responsible for scanning the statements of support collected in paper and upload them to the online collection system.

Table 20: overview of the organisation analysis - scenario 3

6.4 TECHNICAL ANALYSIS

6.4.1 Implementation

Scenario 3 shares a number of similarities with scenario 2; the installation presents the same degree of complexity. However, this installation only needs to be performed once. Any new initiative will only require to be added in the database and file-system, which could be done in a matter of minutes. Depending on the option chosen, the configuration and/or implementation of the front-end might take a bit longer, but everything could be achieved in a few days.

The certification is no longer required as the Commission's online collection system is considered as de facto be compliant with the security requirements (see section 6.3.2). Nonetheless, regular audits are recommended to ensure that security requirements are enforced.

Scalability and maintenance are also facilitated, as a common platform allows to share both IT and human resources.

6.4.2 Operations

The considerations highlighted in the previous section regarding the implementation of scenario 3 are also applicable to the operational phase. The main added value of this scenario is the ability to deploy the resources required by a new ECI in a few minutes. In addition, any security issues and bug in the online collection system can be fixed for all initiatives at once.

The other key added value of a central platform is that it allows to implement more controls to support the verification process.

The scoring of the evaluation criteria therefore improves on almost all aspects compared to scenarios 1 and 2.

Evaluation Criteria	Category	Score	Description
Implementation	Installation	●●●●◐	• New initiatives are included in the pre-existing database and file-system. • The source code is in a pom.xml file to ease the installation. It is prepared to be used by the most widely used Java compilation environment: maven.
	Scalability	●●●●●	• The online collection software, in a physical or virtual server, fully achieves its objective. • The initiatives are stored in the same OCS, such a server could host over 50 initiatives.
	Maintenance	●●●●◐	• In the short term, changes are foreseen to integrate and deploy the new front-end. • On the long term, other modifications can be anticipated, such as the integration of eID. • The maintenance efforts are less demanding as it needs to be done only once for all initiatives.
Operations	System administration	●●●●◐	• The following activities are covered: ○ Installation of the system ○ Update of the software based on discovered flaws and security breaches, revision of log files during the life-cycle of the system ○ Disposal/migration • The task are more efficient since they apply to all the initiatives at the same time.
	Verification process	●●●●○	• This scenario allows to implement more controls to support the verification process

Table 21: overview of the technical analysis - scenario 3

6.5 SECURITY ANALYSIS

6.5.1 Security architecture

In this scenario, the Commission is responsible for the compliance of its online collection system with the ECI Regulation. The considerations made in scenario 2 (see section 5.5.1) are also applicable although the scoring for the European Commission will be higher as the efforts for enforcing security architecture will decrease.

Some additional specific considerations are worth mentioning: since the system is centralised, it is more vulnerable to some specific types of security issues, such as denial of service attacks.

Section 2.8 of the Annex of Implementing Regulation (EU) 1179/2011, on database security and data integrity, may need to be revised to reflect the specific case of scenario 3.

6.5.2 Software development security

In this scenario the European Commission develops, maintains and improves a central online collection platform compliant with the ECI legislation.

It is recommended to implement an incremental approach towards security in order to increase the security level over time as the online collection system is getting more mature.

The aspects for improving the Regulation, developed in scenario 2 (see section 5.5.2), also apply to this scenario although the scoring for the European Commission will be higher as the efforts for enforcing software development security will decrease.

6.5.3 Data security & integrity

The aspects for improving the Regulation, developed in scenario 2 (see section 5.5.3), also apply to this scenario.

6.5.4 Identity and access management

The aspects for improving the Regulation, developed in scenario 2 (see section 5.5.4), also apply to this scenario.

Evaluation Criteria	Stakeholder	Score	Description
Security architecture	European Commission	●●●●●	• The central Commission online collection platform is compliant with the ECI Regulation, and centralised for a better management of possible security breaches (physical or logical).
	Competent Authorities	●●●●○	• Communications with the central Commission online collection platform is less changeable in security configurations (both perimetral systems and the online collection system itself).
	Organisers	n/a	• n/a
Software development security	European Commission	●●●●●	• The Commission develops, maintains and improves a central online collection platform that is considered as de facto compliant with the ECI Regulation and the Regulation ((EU) 1179/2011).
	Competent Authorities	●●●●●	• The integration with the EU File Sharing Service is the only piece of software that needs to be developed by the Member States.
	Organisers	n/a	• n/a
Data security & integrity	European Commission	●●●●○	• The storage and sending of the data collected in the Commission's online collection system, for the verification by the Member States, is done under the sole responsibility of the Commission and complies with Commission Decision (EU, Euratom) 2017/46.
	Competent Authorities	●●●●○	• The reception and storage of the data collected from the Commission's online collection system of each initiative (exported data) for the verification, is done in accordance with national regulations for IT security.
	Organisers	●●●●○	• A malicious organiser (insider) could try to hack the central Commission online collection platform, exploiting a possible vulnerability to manipulate the data.
	External user	●●●●○	• A malicious client user (outsider) could try to hack the central Commission online collection platform, exploiting a possible vulnerability to manipulate the data.
Identity and access management	European Commission	●●●●○	• The access of the Commission, as an admin role, has several security requirements in the Annex of the Implementing Regulation – section 2.7.3 h.
	Organisers	●●●●○	• The organisers have a limited access to the online collection platform, with no direct access to the personal data collected online.

Table 22: overview of the security analysis - scenario 3

6.6 COSTS ANALYSIS

6.6.1 European Commission

It should be noted that the development is spread over two years given the complexity and dependencies in the architecture of this solution. Common assumptions for the estimates are detailed in scenario 2 (see section 5.6)

The following assumptions apply only to scenario 3:

- It is assumed that all 20 ECIs are implemented with the Commission's online collection software and hosted by the Commission;
- The yearly hosting cost is estimated to 300,000 euros for the whole platform;
- Licensing fees are considered for EU File Sharing Service, eIDAS, and the OCR software for a total of 300,000 euros[51];
- The configuration of a new ECI requires on average 2 days of a system administrator and 5 days of a developer;
- Integration with an OCR reader tool is foreseen and costs will be similar to the EU File Sharing integration;
- Register integration: full integration is considered, giving the opportunity to merge the online collection software and the Register into a single software, allowing automation of the deployment of the ECI website from the Register. After the automated deployment, customisation of the stylesheets and other graphical elements are the only things to do in order to have an online collection software instance up and running. This also allows to reduce drastically the costs of helpdesk. The additional benefit of not having to maintain the Register is not taken into account for this assessment;
- Maintenance costs of the online collection software is expected to be reduced by 25% compared to the AS IS, but additional costs are considered for the maintenance of the Register (180 days per year);
- Although still higher than the AS IS situation, the support and helpdesk costs are expected to be lower than Scenario 2 because of better automation of the deployment process of a new ECI.

As a result, the costs for the Commission of the scenario 3 are estimated as follows:

[51] EU File Sharing Service and eIDAS costs are only applicable from the deployment in production in Year 3.

			Scenario 3				
			Year 1 (2018)	Year 2 (2019)	Year 3	Year 4	Year 5
European Commission	**Infrastructure**		**€ 60,000**	**€ 350,000**	**€ 630,000**	**€ 630,000**	**€ 630,000**
		Hosting	€ 30,000	€ 330,000	€ 330,000	€ 330,000	€ 330,000
		Fees/Licenses	€ 30,000	€ 20,000	€ 300,000	€ 300,000	€ 300,000
	Development		***€ 514,349***	***€ 506,966***	***€ 110,745***	***€ -***	***€ -***
		OCS Back-end	€ 246,100	€ 123,050			
		OCS Front-end	€ 169,809	€ 125,511			
		EU File Sharing Service interface	€ 24,610	€ 49,220			
		OCR Reader integration	€ 24,610	€ 49,220			
		eIDAS integration	€ 49,220	€ 49,220			
		Register integration		€ 110,745	€ 110,745		
	Maintenance		***€ 59,000***	***€ 59,000***	***€ 273,500***	***€ 372,500***	***€ 372,500***
		OCS	€ 33,000	€ 33,000	€ 247,500	€ 247,500	€ 247,500
		Register				€ 99,000	€ 99,000
		Tools & frameworks	€ 26,000	€ 26,000	€ 26,000	€ 26,000	€ 26,000
	Support & Operations		***€ 70,500***	***€ 70,500***	***€ 146,840***	***€ 146,840***	***€ 146,840***
		ECI Instance Configuration	€ 42,000	€ 42,000	€ 97,440	€ 97,440	€ 97,440
		Helpdesk	€ 28,500	€ 28,500	€ 49,400	€ 49,400	€ 49,400
	Certification		***€ -***	***€ -***	***€ -***	***€ -***	***€ -***
	TOTAL		**€ 703,849**	**€ 986,466**	**€1,161,085**	**€1,149,340**	**€1,149,340**
	TOTAL ACCRUED		**€ 703,849**	**€ 1,690,315**	**€2,851,400**	**€4,000,740**	**€5,150,080**

Table 23: Costs estimates for the Commission - scenario 3

The total cost of scenario 3 for the European Commission over a period of 5 years is 5,150,080 euros.

6.6.2 Organisers

For scenario 3, since the assumption is that all ECIs will be running on the online collection system of the Commission, organisers no longer incur any costs.

Table 24 summarises the scores of the costs analysis.

Evaluation Criteria	Category	Score	Description
Costs Commission	Infrastructure	●●●●○	• Large decrease of the infrastructure costs expected as the whole system can be sized according to the workload.
	Development	●●●○○	• An investment of 1,130,000 € should be made to configure the online collection software for a permanent hosting in DIGIT data centre and to add the full set of new functionalities
	Maintenance	●●●●○	• Lower than AS IS situation
	Support	●●●○○	• Costs doubled compared to the AS IS but it covers a wider set of features, including integration of the Register and automation of the deployment
Costs Organisers	Infrastructure	●●●●●	• Organisers no longer incur any costs
	Development	●●●●●	• Organisers no longer incur any costs
	Maintenance	●●●●●	• Organisers no longer incur any costs
	Support	●●●●●	• Organisers no longer incur any costs

Table 24: Overview of the costs analysis - scenario 3

6.7 SUMMARY OF ADAPTATIONS REQUIRED IN THE IMPLEMENTING REGULATION 1179/2011

The following are the sections that need to be modified in the Annex of Implementing Regulation (EU) 1179/2011 to implement scenario 3. Since most of the modification proposed for the Annex are the same as in scenario 2, the reader should refer to section 5.7, with the exception of the following paragraphs:

- In Annex – section 2.3, it is advised to specify that the online collection system consist on web-based application set up for the purpose of collecting statements of support for citizen's initiatives. Also it is recommended to mention if there is one server used for more than one initiative, all initiatives using the same server are adequately separated, guaranteeing that statements of support are registered only in the initiative for which the citizen has expressed his support.
- In section 2.4, it is advised to include that in case of different initiatives using the same system, the organisers of each initiative shall only have access to their own initiative (but not to the data collected).

7 EVALUATION AND COMPARISON

This chapter summarises the assessment of the three scenarios as well as their pros and cons in a SWOT analysis. Table 25 presents the results of the assessment for the three scenarios.

Dimension	Evaluation criteria	Scenario 1	Scenario 2	Scenario 3
Legal	Impact of GDPR	●●●○○	●●●●○	●●●●○
	Impact on liabilities	●●●○○	●●●●○	●●●●○
Organisational	Convenience	●●●○○	●●●◐○	●●●●○
	Certification	●●●◐○	●●●●●	●●●●●
	Verification	●●◐○○	●●●●○	●●●●○
Technical	Implementation	●●◐○○	●●●◐○	●●●●◐
	Operations	●●●○○	●●●◔○	●●●●◔
Security	Security architecture	●●●○○	●●●●○	●●●●◐
	Software development security	●●◔○○	●●●●◐	●●●●●
	Data security & integrity	●●◐○○	●●●●○	●●●●○
	Identity and access management	●●●○○	●●●●○	●●●●○
Costs	European Commission	●●●◐○	●●●○○	●●●◐○
	Organisers	●●●○○	●●●●●	●●●●●

Table 25: Summary of the scenarios assessment

On all criteria, scenario 3 scores better, or is at least equivalent to the other scenarios, as shown in Figure 16.

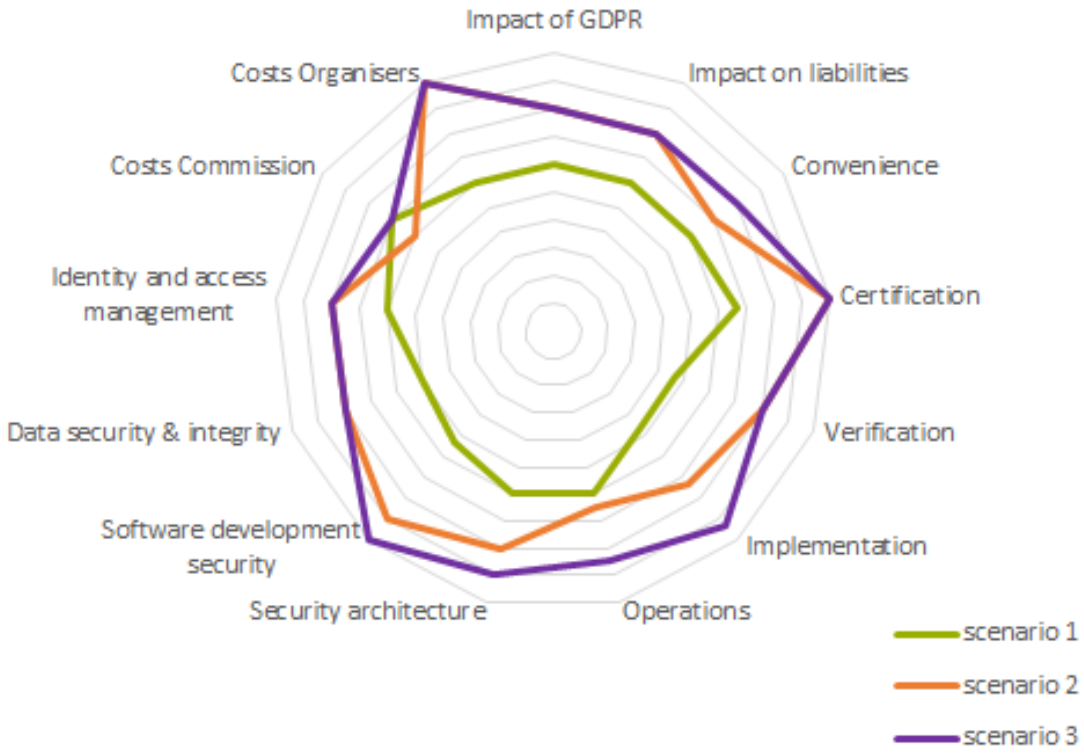


Figure 16: Evaluation and comparison of the three scenarios

AS IS - TOTAL	€ 774,500	€ 774,500	€ 972,500	€ 972,500	€ 972,500
AS IS - TOTAL ACCRUED	€ 774,500	€1,549,000	€2,521,500	€3,494,000	€4,466,500
Scenario 1 - TOTAL	€ 1,010,600	€ 781,380	€ 781,380	€ 781,380	€ 781,380
Scenario 1 - TOTAL ACCRUED	€ 1,010,600	€1,791,980	€2,573,360	€3,354,740	€4,136,120
Scenario 2 - TOTAL	€ 1,165,345	€1,228,485	€1,117,740	€1,117,740	€1,117,740
Scenario 2 - TOTAL ACCRUED	€ 1,165,345	€2,393,830	€3,511,570	€4,629,310	€5,747,050
Scenario 3 - TOTAL	€ 703,849	€ 986,466	€1,161,085	€1,149,340	€1,149,340
Scenario 3 - TOTAL ACCRUED	€ 703,849	€1,690,315	€2,851,400	€4,000,740	€5,150,080

Table 26: Summary of the total costs for the AS IS and the 3 scenarios

The costs of scenario 1 should be contrasted with the costs of maintaining the AS IS situation. According to the data collected by Kurt Salmon, yearly hosting, maintenance and operational costs reach 775,000 euros in the AS IS situation and will increase to 970,000 euros once the Register comes into the perimeter. Scenario 1 will limit the yearly costs down to 780,000 euros after the minimal integration of the Register.

Scenario 2 is more expensive than the other two scenarios as all the ECIs would be running on the Commission's online collection software and hosted by the Commission. Operational costs remain high and proportional to the number of ECIs with little gain achieved by the consolidation of all ECIs in DIGIT data centre. Scenario 2 will lead to an important increase of the yearly costs to 1,120,000 euros and gives little hope to recover the investments made despite the additional functionalities.

Although the total costs of scenario 3 are higher than scenario 1, it presents several benefits such as the adjustment of the infrastructure to the real workload of the system. This solution is also the one that results in the deepest integration (or consolidation) with the Register and with other elements provided by DIGIT such eIDAS and the EU File Sharing Services. Given the initial investment required, the break-even point will not be reached within the five year period that has been considered for this assessment. However, this solution offers several additional features such as the OCR reader, Register and eIDAS integration, which are expected to contribute positively to the success of the new version of the online collection system.

Finally, the break-even point could be reached in case of increase in the number of initiatives which use the online collection system per year (estimation is based on the total number of 20 initiatives per year).

In addition to those conclusions, the Table 27 summarises the results of the SWOT analysis of the three scenarios.

	SCENARIO 1	SCENARIO 2	SCENARIO 3
Strengths	• Organisers are free to choose between the online collection software provided by the European Commission or by third party organisations. • The Commission guarantees that its online collection system follows the technical specifications and publishes the OCS as open source code for external verification. • The Commission and the competent authorities do not have direct access to the online collection system data. • The national competent authorities are considered as data controllers for all statements of support (paper and online). • Data protection authorities in the Member States are considered as supervisory authorities that monitor compliance with EU data protection rules.	• The European Commission develops, maintains and improves an online collection system, free of charge and compliant with the ECI Regulation. • This scenario does not involve third party organisations: the European Commission always provides the online collection system. • The European Commission is considered as data controller for the statements of support collected online and may become data processor for the paper SoS that are scanned and uploaded to its online collection system. • The competent authorities are considered as data controllers for all statements of support (paper and online). • Data protection authorities in the Member States are considered as supervisory authorities that monitor compliance with EU data protection rules • When statements of support are collected online, the organisers do not have any responsibility regarding the processed personal data. • The certification of the online collection system is no longer required. • The European Commission sends all statements of support to the Member States' competent authorities. • The Commission's hosting service and data centre are compliant with the ECI Regulation, and centralised for a better management of possible security breaches. • The competent authorities do not have direct access to the online collection system. • Organisers have a limited access to the online collection system, with no direct access to the personal data collected via the online statements of support.	• The European Commission develops, maintains and improves an online collection system, free of charge and compliant with the ECI Regulation. • This scenario does not involve third party organisations: the European Commission always provides the online collection system. • The European Commission is considered as data controller for the statements of support collected online and may become data processor for the paper SoS that are scanned and uploaded to its online collection system • The competent authorities are considered as data controllers for all statements of support (paper and online). • Data protection authorities in the Member States are considered as supervisory authorities that monitor compliance with EU data protection rules. • When statements of support are collected online, organisers do not have any responsibility regarding the processed personal data. • The certification of the online collection system is no longer required. • The European Commission sends all statements of support to the Member States' competent authorities • The maintenance efforts are less demanding as it needs to be done only once for all the initiatives. • This scenario allows to implement more controls to support the verification process. • The Commission's hosting service and data centre are compliant with the ECI Regulation, and centralised for a better management of possible security breaches. • The competent authorities do not have direct access to the online collection system. • The organisers have a limited access to the online collection system, with no direct access to the personal collected via the online statements of support. • This scenario offers the best cost-benefit results at mid-term, both for the infrastructure and the human costs.

	SCENARIO 1	SCENARIO 2	SCENARIO 3
Weaknesses	• The online collection software hosting provider is only considered as data processor for the online statements of support. • Organisers are responsible as data controllers for both paper and online SoS. • Organisers are in charge of requesting the certification of the online collection system when they don't use the Commission provided system • If organisers opt for an online collection system implemented by a third party, the installation is likely to be more cumbersome. • Organisers need to ensure that the online collection system complies with the requirements. • This scenario offers no improvement of the verification process.	• Organisers could be made responsible for scanning the statements of support collected in paper and uploading them to the online collection system. • This scenario offers no improvement of the verification process. • The implementation and operational costs are higher since all ECIs are supported by the online collection system provided by the European Commission.	• The organisers could be responsible for scanning the statements of support collected in paper and uploading them to the online collection system.
Opportunities	• The European Commission and the third party, acting as providers of the online collection software hosting, may incur liabilities as data processors for the statements of support collected online. • Two new roles are established under certain circumstances to enhance compliance with the EU data protection rules: the Data Protection Officer (DPO) and the lead supervisory authority.	• Two new roles are established under certain circumstances to enhance compliance with EU data protection rules: the DPO and the lead supervisory authority. A dashboard could be developed by the Commission for the organisers to have a view on the amount of statements of support collected. • The sending of statements of support for verification could benefit from the EU file transfer service to implement a more secure transmission of the statements of support.	• Two new roles are established under certain circumstances to enhance compliance with EU data protection rules: the DPO and the lead supervisory authority. • A dashboard could be developed by the Commission for the organisers to have a view on the amount of statements of support collected. • A Central Authentication Service, a single sign-on protocol might be implemented. • The sending of statements of support for verification could benefit from the EU File Sharing Service to implement a more secure transmission of the statements of support.

	SCENARIO 1	SCENARIO 2	SCENARIO 3
Threats	• Organisers are considered as data controllers concerning the processing of both paper and online SoS • Organisers submit the statements of support to the relevant competent authorities. • Even if the hosting service is compliant with the Regulation, it may have some security breaches (physical or logical) not covered. • A malicious user (outsider) could try to hack the online collection system exploiting a possible vulnerability.	• In the short term, changes are foreseen to integrate and deploy the new front-end. On the long term, modifications can be foreseen to integrate eID. • A malicious organiser (insider) or client user (outsider) could try to hack the Commission's online collection system exploiting a possible vulnerability to manipulate the data.	• In the short term, changes are foreseen to integrate and deploy the new front-end. On the long term, modifications can be foreseen to integrate eID. • A malicious organiser (insider) or client user (outsider) could try to hack the Commission's online collection system exploiting a possible vulnerability to manipulate the data.

Table 27: Summary of SWOT analysis

8 CONCLUSIONS

The objective of this study has been to assess the possible improvement of the process of online collection of the statements of support, considering three scenarios, a potential revision of the ECI legislative framework and the evolution of the situation in regards to technology and security threats.

The analysis covers the assessment of the three following scenarios:

- Scenario 1: update of the original scenario foreseen in the current ECI Regulation, where the online collection of statements of support is completed via individual online collection systems, under the responsibility of the organisers, based on the evolution of technology and security risks;
- Scenario 2: Specific case of the online collection systems, where only the online collection software and hosting service provided by the Commission are used;
- Scenario 3: Setting up a centralised online collection platform provided and operated by the European Commission.

This study focused on the potential benefits, weaknesses, opportunities and threats of the three scenarios for the online collection process.

As this study shows, there are a large number of complex issues to consider for the implementation of any of the analysed scenarios for the improvement of the process of online collection of the statements of support. Everis approach covered the analysis of all five - legal, business, technical, security and costs - requirements of each identified scenario. The scenarios were assessed based on the criteria identified in chapter 2: Approach and methodology.

During the process of the study, various criteria have been identified and analysed. The most important and relevant ones have been selected, and form the core of the evaluation matrix criteria, which has been applied to assess each scenario and to quantify the effects of each criterion on the scenario. The analysis of the strengths, weaknesses, opportunities and threats complemented each scenario's assessment. For the final evaluation and comparison between the solutions, the evaluation matrix has been applied (see Table 1 for the criteria).

From a legal point of view, various changes, both to the current ECI Regulation (EU) 211/2011 and Implementing Regulation (Regulation (EU) 1179/2011), are necessary for the implementation of the three scenarios. For scenarios 2 and 3, it is questionable whether an Implementing Regulation would still be needed to define the technical specifications given that the Commission will be the only one to provide the online collection system and that no certification will be needed. The analysis focused on the key implications in terms of data protection roles and liabilities that the new EU data protection rules are going to bring as from May next year in the context of the ECI. The key novelties, which the General Data Protection Regulation ((EU) 2016/679) and the revised Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies will introduce, are identified and summarised in section 4.1. The concrete implications of these novelties with regard to the revision of the ECI Regulation and its implementing Regulation are then separately analysed in each scenario. The most important impact of the new data protection rules is the extension of liabilities, according to which both data controllers and data processors will be subject to liabilities in proportion to their role, whereas under the previous data protection rules only data controllers could be held liable in case of damage caused

to data subjects as a result of their processing.. In addition, the GDPR created two new roles: the 'lead supervisory authority', which centralises the supervisory role of the national data protection authorities in one single body in case of cross-border processing of personal data, and the Data Protection Officer, in charge of monitoring compliance with the GDPR and providing advice to the data controller and to the data processor. Finally, another key difference between scenarios relates to the distribution of data protection responsibilities among the various ECI stakeholders, and in particular between the organisers and the European Commission.[52] In the first scenario the organiser is considered as data controller for the statements of support collected both online and on paper, while the European Commission or the third party as hosting providers of the online collection software are considered as data processors for the statements of support collected online only. Comparatively, in scenarios 2 and 3 the organisers are only considered as data controllers for the statements of support collected on paper. As the exclusive and default service provider of the online collection system, the European Commission takes over the responsibility as data controller for the online statements of support, freeing organisers of their data protection obligations. In this sense, the last two scenarios are the preferred options for reducing the burden of organisers in terms of liabilities in case of damage related to the data.

From the organisation perspective, scenario 3 scores the highest in terms of convenience, certification and verification. Both scenarios 2 and 3 allow the suppression of the certification and provide an improvement of the verification. In scenario 1, the suppression of the certification is also envisaged as regards the systems hosted by the Commission. In addition, scenario 3 could facilitate a Central Authentication Service, where citizen would be required to fill all his/her personal data only the first time and would authenticate himself/herself for supporting an initiative. Regarding the transfer of SoS to competent authorities at the start of the verification phase, all scenarios could benefit from the EU File Sharing Service to increase the security and efficiency of the transmission of statements of support, although the setup and operations would be easier in scenario 2 and 3.

The way to integrate the processing of statements of support collected on paper represents another challenge. Ideally, the online collection system should allow organisers to upload the scanned version of the paper statements of support, so that all statements of support could be submitted through the online collection system with a single timestamp. However, such an approach has a high impact of bandwidth and storage requirements even for a low percentage of paper statements of support, compared to the online ones. This approach has the advantage of allowing organisers to concentrate their initiatives' campaigns online, and probably in the future to push towards the collection of statements of support only online.

Scenario 3 provides the best technical performance and has various advantages over scenario 1 and 2. To begin with, the installation of the online collection system is performed only once, and any new initiative is just added to the database and file system, reducing the set-up time to a few minutes. In terms of scalability, this scenario is also the most attractive, as the resources could be continuously aligned on the actual workload without any significant effect to the performance of the system in terms of response time. Likewise, maintenance effort would be done once, and for all initiatives, in case of any changes to be applied to the system, which would allow to reduce the effort for maintenance as well. For operations' task too, scenario 3 would provide the most efficient solution

[52] The role of the national competent authorities as data controllers remains unchanged across the scenarios and it is therefore not highlighted in the conclusions.

for online collection system update, as the application of all the necessary actions to all initiatives is done at once.

From the security point of view, scenario 3 provides the best case in terms of security architecture, software development security, data security and integrity. In comparison with scenario 1, scenarios 2 and 3 shift the responsibilities from the organisers to the European Commission, making sure the online collection system is compliant with the Regulation, and the data collection and storage is done appropriately. The potential intentional and non-intentional manipulation of data is very unlikely (the probability of a possible malicious user hacking the online collection system is rather low); however, the possible damage in scenario 3 would be much higher than in scenarios 1 or 2. The main advantages of scenario 3 are stability, compliance and better management of possible security breaches (physical or logical).

Costs-wise, scenario 1 presents a better performance than the AS IS situation. On the other hand, although scenario 3 is more expensive, it offers several additional features such as the OCR reader, Register and eIDAS integration, which are expected to contribute positively to the success of the new version of the online collection system. Among the three scenarios, scenario 2 is the most expensive option, based on the fact that all the ECIs would be run on the Commission's online collection software and hosted by the Commission but with limited economies of scale. High yearly costs for maintenance and operations are not outweighed by the reduction of certification costs. Having in mind scenario 2 costs dependence on the number of ECIs, the costs could be even higher in the future, if opted for this scenario's implementation, as the number of ECIs could increase significantly.

From overall analysis, everis has concluded that scenario 3 would be the best option, in particular for organisers of initiatives and citizens' supporting ECIs. It would also contribute for the improvement and facilitation of the collection and verification of signatures for statements of support, while at the same time complying with identified legal, operation, technical, security and costs ideal description for identified criteria in this particular context. According to everis, scenario 3 is the most promising solution for the future, making an improvement of the online collection of the statements of support the most forward-looking and up-to-date to the highest standards.

Regarding the other scenarios, scenario 1 does not provide a significant change in comparison to the existing situation, and scenario 2 drawback would be relatively high costs in comparison to scenario 1 and 3, based on the estimation that the number of ECIs per year does not change significantly. Though similar to scenario 3, scenario 2 limited applicability and functionality, like missing Central Authentication Service puts it to unfavourable position. However, as it was indicated in the report, the complete move towards scenario 3 would significantly change the roles and responsibilities of organisers, competent authorities and European Commission, which might require time to be processed and agreed upon.

9 APPENDIX I – SCENARIO 1 DETAILED ASSESSMENT

Dimension	Evaluation criteria	Stakeholder	Ideal Example	Description/Justification	Score	Weight
Legal	Impact of GDPR	European Commission / Third party	As far as possible, the organisers are not in charge of processing personal data (The responsibility of the organisers as data controllers for the collection of statements of support is shifted to the European Commission)	The Online Collection System hosting provider is considered only as data processor for the online statements of support.	3.00	
		Competent Authorities	The competent authorities are considered as data controllers for the purposes of verifying and certifying the statements of support. Supervisory authorities are put in place to monitor data protection compliance at national level that are coordinated among themselves	- The competent authorities are considered as data controllers when verifying and certifying the statements of support collected both online and on paper. - The data protection authorities in the Member States are considered as supervisory authorities and a lead supervisory authority is established as a one-stop-shop in cases of cross-border processing of personal data	4.00	
		Organisers	As far as possible, the organisers are not in charge of processing personal data (The responsibility of the organisers as data controllers for the collection of statements of support is shifted to the European Commission)	The organisers are still considered as data controllers concerning the processing of both paper and online statements of support.	2.00	
				Criteria average Score		3.00
	Impact on liabilities	European Commission / Third party	The liability in case of damage caused to data subjects is shared among the different stakeholders, either as data controllers or processors, in proportion to their role and concrete responsibilities. The potential liability issues for the organisers are reduced.	- Under the previous data protection rules, only data controllers were liable in case of damages caused to the data subject when processing their data. - Under the new GDPR and Regulation 45/2001 under revision, both data controllers and data processors may face liabilities in proportion to their role and behaviour. - The possibility to impose administrative fines by the supervisory authorities/EDPS to the data controller and the data processor is now foreseen in case of non-respect of data protection obligations. - Consequently, the European Commission and the third party acting as Online Collection System hosting providers may now face liabilities as data processors for the online statements of support. The organisers and the competent authorities remain liable as data controllers for all statements of support collected in any format.	3.00	
		Competent Authorities				
		Organisers				
				Criteria average Score		3.00
Organisation	Convenience	European Commission / Third party	An Online Collection System is provided by the European Commission. As the responsibilities of organisers are lowered, an online dashboard is implemented to allow them to monitor the number of statements of support collected.	The European Commission or the third party provide a stand-alone Online Collection Software	3.00	
		Competent Authorities	n/a	n/a		
		Organisers	In case the system provided by the Commission is used by the organisers, their responsibilities and therefore their liability are low, making it easier and more attractive for them to launch and monitor an initiative.	The organisers are free to choose between the Online Collection System provided by the European Commission or by third party organisations.	3.00	
				Criteria average Score		3.00
	Certification	European Commission / Third party	The European Commission is responsible for making sure that the Online Collection System it provides complies with the appropriate security and technical requirements.	- The online collection system provided by the Commission is considered as de facto certified, which shorten the setup process of a new initiative. - In case a third party system is used, organisers are responsible to request certification and competent authorities to certify it.	4.00	
		Competent Authorities	The competent authorities only need to certify the Online Collection Systems of organisers (not the one provided by the European Commission).		3.00	
		Organisers	The organisers do not need to request the certification of the Online Collection System if they use the Commission provided system.		3.00	
				Criteria average Score		3.33
	Verification	European Commission	The statements of support are sent by the European Commission to the Member States competent authorities for verification. This transmission is done via a secure online file transfer.	The European Commission does not play any role in the verification of statements of support.	1.00	
		Competent Authorities	The national competent authorities are in charge of verifying the statements of support.	The national competent authorities verify the statements of support and deliver a certificate to the organisers.	4.00	
		Organisers	The responsibility of organisers is limited as far as possible. When they use the Commission provided system, they are not in charge of the transfer of the statements of support to national competent authorities. However, they remain in charge of transferring the statements of support collected in paper form to the European Commission.	The organisers submit the statements of support to the relevant competent authorities.	2.00	
				Criteria average Score		2.33

Technical	Implementation	Installation	The Online Collection System is implemented using well-known technologies and software stack, which are recognised as de facto standards.	The current EC Online Collection System is implemented in Java and available with Glassfish appserver. It should be slightly modified to use WebLogic as appserver, which is the standard in DIGIT data centre. It is also configured to be compiled with Maven, the most widely used Java compilation environment. Some efforts must be spent also on the packaging of the Online Collection System so that it can be easily installed in other environments. If organisers choose for an Online Collection System provided by a third party, the complexity of the configuration in order to meet all the ECI legistlative requirements should not underestimated.	2.00	
		Scalability	The Online Collection System architecture is designed in a way that allows scalability of resources without refactoring of the source code and with little or no development costs	In the eID for ECI study, it was shown that a standard Online Collection System server (similar to the ones available in DIGIT data centre) is able to process 4 million statements of support in one day. Given that each initiative must be installed on a dedicated server, this threshold is unlikely to be exceeded. Therefore scalability is not an issue. However, it is not the best used of resources as each server is not used to its full potential	2.00	
		Maintenance	The Online Collection System architecture makes it easy to maintain by isolating functionalities in layers and components.	In the short term, changes are foreseen to integrate and deploy the new front-end. On the long term, other modifications can be anticipated, such integration of eID and they won't require major refactoring of the code.	3.00	
				Criteria average Score		**2.33**
	Operations	System administration	The installation and monitoring of the Online Collection System doesn't create any burden for the system administrators in charge of the infrastructure on which it is running.	Under scenario 1, the situation remains unchanged compared to the AS IS situation with regards to system administration of the Online Collection System and its infrastructure	3.00	
		Communication	The Online Collection System supports the verification process by competent authorities and allows the most optimal use of the resources and infrastructure	This scenario offers no improvement of the verification process.	3.00	
				Criteria average Score		3.00
Security	**Security architecture**	Competent Authorities	Communications between the Competent authority and the Online Collection System are sufficiently secure (for example using https with TLS)	Communications with each organiser's platform may vary in the security configurations (both hosting perimetral systems and the Online Collection System) but it should meet the requirements laid down in the ECI Regulation.	3.00	
		Commission	The Commission's Hosting service and Data center are secure enough (with security certifications evidence), and compliant with the ECI regulation	Even if the hosting service is compliant with the Regulation, it may have some security breaches (physical or logical) not covered	3.00	
		Organiser	The organiser choose a hosting provider with adequate security level (including certifications evidence), and compliant with the ECI regulation.	Even if the hosting service is compliant with the Regulation, it may have some security breaches (physical or logical) not covered	3.00	
				Criteria average Score		**3.00**
	Software development security	Competent Authorities	Certification of the Online Collection System by the national competent authorities in Member States meets the security criteria (black/white box approach), in addition to the audit of the technical specifications.	The national authorities in Member States certify the organiser's Online Collection System is compliant with the Regulation	3.00	
		Commission	Development of the Commission's Online Collection System following technical specifications and taking into account Security in Development Lifecycle.	The Commission guarantees that the EC Online Collection System follows the technical specifications and it publishes the Online Collection System as open source code for external verification	3.00	
		Organiser	Development of the third party's Online Collection System following technical specifications and taking into account Security in Development Lifecycle.	Organisers need to ensure that the system used for their registered initiative complies with the relevant requirements under the Regulation Development of their own Online Collection System	2.00	
				Criteria average Score		**2.67**
	Data security & integrity	Competent Authorities	The process of reception and storage for verification is secure enough and compliant with regulation, guaranteeing integrity and confidentiality.	Reception and storage of the data collected from the Online Collection System of each initiative (exported data) for the verification, is done in accordance with Article 8(2).	3.00	
		Commission	The process of collecting, sending and storing of Statement of Support is secure enough and compliant with ECI regulation, guaranteeing integrity and confidentiality.	Sending and storage of the data collected in the Online Collection System, for the verification by the Member States, is done in accordance with Article 8(2).	3.00	
		Organiser	The process of collecting, sending and storing of Statement of Support is secure enough and compliant with regulation, guaranteeing integrity and confidentiality.	Sending and storage of the data collected in the Online Collection System, for the verification by the Member States, is made in accordance with Article 8(2).	2.00	
		External User	The Online Collection System is protected against intentional or unintentional manipulation from the client side.	A malicious user (outsider) could try to hack the Online Collection System exploiting a possible vulnerability	2.00	
				Criteria average Score		**2.50**

	Identify and access management	Commission	The Commission has only the necessary permissions to manage the information collected in the Online Collection System, and the process of identification and authentication is secure enough.	The Commission does not have direct access to the Online Collection System.		
		Organiser	The organiser has only the necessary permissions to manage the information collected in his/her Online Collection System, and the process of identification and authentication is secure enough.	The access of the organiser as an admin role, has several security requisites in the technical specifications 2.7.3 h	3.00	
	Criteria average Score					**3.00**
Cost	**Costs Commission**	Infrastructure	The infrastructure costs are optimised when compared to the AS IS situation by sharing common resources and sizing it according to workload, while meeting all ECI legislation requirements	An improvement of the ECI unit hosting cost is anticipated, but some additional costs, such the EU File Sharing Service fees, are taken into account.	3.00	
		Development	The development efforts are optimised when compared to the AS IS situation, taking into account the costs of adding the same functionalities in the current Online Collection System.	An investment of two hundred fifty thousand euros should be made to configure the Online Collection System for a permanent hosting in DIGIT data centre and to add new functionalities and the pay-off is achieved within five years.	3.00	
		Maintenance	The maintenance costs of the Online Collection System are optimised over a five-year period when compare to the AS IS situation.	Maintenance costs will be much lower than the AS IS situation due to savings on both the Online Collection System and the Register.	5.00	
		Support	The support and operational costs of the Online Collection System are optimised over a five-year period when compared to the AS IS situation	Support costs are slightly higher as some additional configuration should be done for each ECI due to the new functionalities but they remain limited.	3.00	
	Criteria average Score					**3.50**
	Costs Organisers	Infrastructure	The infrastructure costs are optimised when compared to the AS IS situation.	The infrastructure costs are similar to the AS IS situation	3.00	
		Development	The development efforts are optimised when compared to the AS IS situation.	No additional costs are incurred for scenario 1 compared to the AS IS situation	3.00	
		Maintenance	The maintenance costs of the Online Collection System are optimised over a five-year period when compare to the AS IS situation.	The maintenance costs are similar to the AS IS situation	3.00	
		Support	The support and operational costs of the Online Collection System are optimised over a five-year period when compared to the AS IS situation	The support and operational costs are similar to the AS IS situation	3.00	
	Criteria average Score					**3.00**

10 APPENDIX II – SCENARIO 2 DETAILED ASSESSMENT

Dimension	Evaluation criteria	Stakeholder	Ideal Example	Description/Justification	Score	Weight
Legal	Impact of GDPR	European Commission	As far as possible, the organisers are not in charge of processing personal data (The responsibility of the organisers as data controllers for the collection of statements of support is shifted to the European Commission)	- The online collection system hosting is always provided by the European Commission. - The European Commission is considered as data controller for the statements of support collected online. - The European Commission is considered as data processor for the statements of support collected on paper that have been scanned and uploaded to the online collection system by the organisers.	4.00	
		Competent Authorities (and data protection authorities in Member States)	The competent authorities are considered as data controllers for the purposes of verifying and certifying the statements of support. Supervisory authorities are put in place to monitor data protection compliance at national level that are coordinated among themselves	- The competent authorities are considered as data controllers when verifying and certifying the paper and the online statements of support. - The data protection authorities in the Member States are considered as supervisory authorities and a lead supervisory authority is established as a one-stop-shop in cases of cross-border processing of personal data.	4.00	
		Organisers	As far as possible, the organisers are not in charge of processing personal data (The responsibility of the organisers as data controllers for the collection of statements of support is shifted to the European Commission)	- The organisers are still considered as data controllers for the statements of support collected on paper. - The organisers do not have any (meaningful) data processing role when statements of support are collected online.	4.00	
				Criteria average Score		4.00
	Impact on liabilities	European Commission	The liability in case of damage caused to data subjects is shared among the different stakeholders, either as data controllers or processors, in proportion to their role and concrete responsibilities. The potential liability issues for the organisers are reduced.	- Under the previous data protection rules, only data controllers were liable in case of damage caused to data subjects when processing their data. - Under the new GDPR and Regulation 45/2001 under revision, both data controllers and data processors may face liabilities in proportion to their role and behaviour. - The possibility to impose administrative fines by the supervisory authorities/EDPS to the data controller and the data processor is now foreseen in case of non-respect of data protection obligations. - Consequently, the European Commission may now face liabilities as data processor for the statements of support collected on paper that are scanned and uploaded to the online collection system. Additionally, the European Commission may be held liable as data controller for the processing of the statements of support collected online. The competent authorities remain liable as data controllers for the statements of support collected in any format. Organisers are exempted from liabilities for online statements of support.	4.00	
		Competent authorities				
		Organisers				
				Criteria average Score		4.00
Organisation	Convenience	European Commission	An online collection system is provided by the European Commission. As the responsibilities of organisers are lowered, an online dashboard is implemented to allow them to monitor the number of statements of support collected.	- This scenario does not involve third party organisations, the European Commission always provides the online collection system. - A dashboard could be developed by the Commission for the organisers to have a view on the amount of statements of support collected.	4.00	
		Competent Authorities	n/a	n/a		
		Organisers	In case the system provided by the Commission is used by the organisers, their responsibilities and therefore their liability are low, making it easier and more attractive for them to launch and monitor an initiative.	- The statements of support collected in paper are scanned by the organisers and uploaded to the online collection system. When statements of support are collected online, the organisers do not have any responsibility.	3.00	
				Criteria average Score		3.50
	Certification	European Commission	The European Commission is responsible for making sure that the online collection system it provides complies with the appropriate security and technical requirements.	- The online collection system of the European Commission is considered as de facto compliant with the ECI Regulation and the Regulation ((EU) 1179/2011).	5.00	
		Competent Authorities	The competent authorities only need to certify the online collection systems of organisers (not the one provided by the European Commission).		5.00	
		Organisers	The organisers do not need to request the certification of the online collection system if they use the Commission provided system.		5.00	
				Criteria average Score		5.00
	Verification	European Commission	The statements of support are sent by the European Commission to the Member States competent authorities for verification. This transmission is done via a secure online file transfer.	- The European Commission sends all the statements of support to the Member States competent authorities. - This process could benefit from the EU file transfer service to implement a more secure transmission of the statements of support.	5.00	
		Competent Authorities	The national competent authorities are in charge of verifying the statements of support.	The national competent authorities verify the statements of support.	4.00	
		Organisers	The responsibility of organisers is limited as far as possible. When they use the Commission provided system, they are not in charge of the transfer of the statements of support to national competent authorities. However, they remain in charge of transferring the statements of support collected in paper form to the European Commission.	The organisers are responsible for scanning the statements of support collected in paper and upload them to the online collection system.	3.00	
				Criteria average Score		4.00

Technical	**Implementation**	Installation	The online collection system is implemented using well-known technologies and software stack, which are recognised as de facto standards.	In this scenario, to ease the installation the source code is in a pom.xml file. This is prepared to be used by the most widely used Java compilation environment: maven.	3.50	
		Scalability	The online collection system architecture is designed in a way that allows scalability of resources without refactoring of the source code and with little or no development costs	The online collection system in a physical or virtual server fully achieve its objective, the system allows to collect 4 million statements of support in one day. Under these circumstances each initiative requires an individual server.	4.00	
		Maintenance	The online collection system architecture makes it easy to maintain by isolating functionalities in layers and components.	In the short term changes are foreseen, due to the integration of eIDs, on a long term no other modifications can be anticipated.	3.50	
				Criteria average Score		3.67
	Operations	System administration	The installation and monitoring of the online collection system doesn't create any burden for the system administrators in charge of the infrastructure on which it is running.	This covers the following activities - Installation of the system - Update of the software based on discovered flaws and security breaches, and revision of log files during the life-cycle of the system, - Disposal/migration	3.50	
		Verification process	The online collection system supports the verification process by competent authorities and allows the most optimal use of the resources and infrastructure	This scenario offers no improvement of the verification process.	3.00	
				Criteria average Score		3.25
Security	**Security architecture**	Competent authority	Communications between the Competent authority and the online collection system are sufficiently secure (for example using https with TLS)	Communications with the Commission's servers and data centre is less changeable in security configurations (both perimetral systems and the online collection system)	4.00	
		Commission	The Commission's Hosting service and Data center are secure enough (with security certifications evidence), and compliant with the ECI regulation	The Commission's Hosting service and Data center are compliant with the ECI Regulation, and centralised for a better managing about possible security breaches (physical or logical)	4.00	
		Organiser	The organiser choose a hosting provider with adequate security level (including certifications evidence), and compliant with the ECI regulation.	n/a		
				Criteria average Score		4.00
	Software development security	Competent authority	Certification of the online collection system by the national competent authorities in Member States meets the security criteria (black/white box approach), in addition to the audit of the technical specifications.	No certification by competent authorities needed	5.00	
		Commission	Development of the Commission's online collection system following technical specifications and taking into account Security in Development Lifecycle.	The European Commission develops, maintains and improves an online collection system, free of charge and compliant with the ECI Regulation.	4.00	
		Organiser	Development of the third party's online collection system following technical specifications and taking into account Security in Development Lifecycle.	n/a		
				Criteria average Score		4.50
	Data security & integrity	Competent authority	The process of reception and storage for verification is secure enough and compliant with regulation, guaranteeing integrity and confidentiality.	The reception and storage of the data collected from the Commission's online collection system of each initiative (exported data), for the verification, is done in accordance with national regulations for IT security.	4.00	
		Commission	The process of collecting, sending and storing of Statement of Support is secure enough and compliant with ECI regulation, guaranteeing integrity and confidentiality.	The storage and sending of the data collected in the Commission's online collection system, for the verification by the Member States, is done under the sole responsibility of the Commission and complies with Commission Decision (EU, Euratom) 2017/46.	4.00	
		Organiser	The process of collecting, sending and storing of Statement of Support is secure enough and compliant with regulation, guaranteeing integrity and confidentiality.	A malicious organiser (insider) could try to hack the Commission's online collection system exploiting a possible vulnerability to manipulate the data	4.00	
		External User	The online collection system is protected against intentional or unintentional manipulation from the client side.	A malicious client user (outsider) could try to hack the Commission's online collection system exploiting a possible vulnerability to manipulate the data	4.00	
				Criteria average Score		4.00
	Identify and access management	Commission	The Commission has only the necessary permissions to manage the information collected in the online collection system, and the process of identification and authentication is secure enough.	The access of the Commission as an admin role has several security requirements in the technical specifications 2.7.3 h	4.00	
		Organiser	The organiser has only the necessary permissions to manage the information collected in his/her online collection system, and the process of identification and authentication is secure enough.	The organisers have a limited access to the online collection system with no direct access to the personal data for the data collected online.	4.00	
				Criteria average Score		4.00

Cost	**Costs Commission**	Infrastructure	The infrastructure costs are optimised when compared to the AS IS situation by sharing common resources and sizing it according to workload, while meeting all ECI legislation requirements	The infrastructure costs remains in the same price range compared to the AS IS situation. An improvement of the unit hosting cost is anticipated but the hosting of all ECIs and some additional costs, such the EU File Sharing Service fees, are taken into account.	3.00	
		Development	The development efforts are optimised when compared to the AS IS situation, taking into account the costs of adding the same functionalities in the current online collection system.	Half a million euros investment should be made over two years to configure the online collection system for a permanent hosting in DIGIT data centre and to add new functionalities.	3.00	
		Maintenance	The maintenance costs of the online collection system are optimised over a five-year period when compare to the AS IS situation.	Maintenance costs are expected to be lower than the AS IS situation, although the new functionalities imply extra maintenance costs compared to scenario 1.	4.00	
		Support	The support and operational costs of the online collection system are optimised over a five-year period when compared to the AS IS situation	Support costs are tripled compared to the AS IS due to support for all ECI instances and the need for configuration support for the Register. However, they cover a wider set of features, including full integration of the Register.	2.00	
	Criteria average Score					**3.00**
	Costs Organisers	Infrastructure	The infrastructure costs are optimised when compared to the AS IS situation.	Organisers no longer incur any costs	5.00	
		Development	The development efforts are optimised when compared to the AS IS situation.		5.00	
		Maintenance	The maintenance costs of the online collection system are optimised over a five-year period when compare to the AS IS situation.		5.00	
		Support	The support and operational costs of the online collection system are optimised over a five-year period when compared to the AS IS situation		5.00	
	Criteria average Score					**5.00**

11 APPENDIX III – SCENARIO 3 DETAILED ASSESSMENT

Dimension	Evaluation criteria	Stakeholder	Ideal Example	Description/Justification	Score	Weight
Legal	Impact of GDPR	European Commission	As far as possible, the organisers are not in charge of processing personal data (The responsibility of the organisers as data controllers for the collection of statements of support is shifted to the European Commission)	- The online collection system hosting is always provided by the European Commission. - The European Commission is considered as data controller for the statements of support collected online. - The European Commission is considered as data processor for the statements of support collected on paper that have been scanned and uploaded to the online collection system by the organisers.	4.00	
		Member States (competent authorities and data protection authorities)	The competent authorities are considered as data controllers for the purposes of verifying and certifying the statements of support. Supervisory authorities are put in place to monitor data protection compliance at national level that are coordinated among themselves	- The competent authorities are considered as data controllers when verifying and certifying the paper and the online statements of support. - The data protection authorities in the Member States are considered as supervisory authorities and a lead supervisory authority is established as a one-stop-shop in cases of cross-border processing of personal data.	4.00	
		Organisers	As far as possible, the organisers are not in charge of processing personal data (The responsibility of the organisers as data controllers for the collection of statements of support is shifted to the European Commission)	- The organisers are still considered as data controllers for the statements of support collected on paper. - The organisers do not have any (meaningful) data processing role when statements of support are collected online.	4.00	
				Criteria average Score		4.00
	Impact on liabilities	European Commission	The liability in case of damage caused to data subjects is shared among the different stakeholders, either as data controllers or processors, in proportion to their role and concrete responsibilities. The potential liability issues for the organisers are reduced.	- Under the previous data protection rules, only data controllers were liable in case of damage caused to data subjects when processing their data. - Under the new GDPR and Regulation 45/2001 under revision, both data controllers and data processors may face liabilities in proportion to their role and behaviour. - The possibility to impose administrative fines by the supervisory authorities/EDPS to the data controller and the data processor is now foreseen in case of non-respect of data protection obligations. - Consequently, the European Commission may now face liabilities as data processor for the statements of support collected on paper that are scanned and uploaded to the online collection system. Additionally, the European Commission may be held liable as data controller for the processing of the statements of support collected online. The competent authorities remain liable as data controllers for the statements of support collected in any format. Organisers are exempted from liabilities for online statements of support.	4.00	
		Competent authorities				
		Organisers				
				Criteria average Score		4.00
Organisation	Convenience	European Commission	An online collection system is provided by the European Commission. As the responsibilities of organisers are lowered, an online dashboard is implemented to allow them to monitor the number of statements of support collected.	- This scenario does not involve third party organisations, the European Commission provides the online collection system as a single online platform. - A dashboard could be developed by the Commission for the organisers to have a view on the amount of statements of support collected.	4.00	
		Competent Authorities	n/a	n/a		
		Organisers	In case the system provided by the Commission is used by the organisers, their responsibilities and therefore their liability are low, making it easier and more attractive for them to launch and monitor an initiative.	- The statements of support collected in paper are scanned by the organisers and uploaded on the online collection system. When they are collected online, the organisers do not have any responsibility. - A Central Authentication Service, a single sign-on protocol might be implemented.	4.00	
				Criteria average Score		4.00
	Certification	European Commission	The European Commission is responsible for making sure that the online collection system it provides complies with the appropriate security and technical requirements.	- The online collection system of the European Commission is considered as de facto compliant with the ECI Regulation and the Regulation ((EU) 1179/2011).	5.00	
		Competent Authorities	The competent authorities only need to certify the online collection systems of organisers (not the one provided by the European Commission).		5.00	
		Organisers	The organisers do not need to request the certification of the online collection system if they use the Commission provided system.		5.00	
				Criteria average Score		5.00
	Verification	European Commission	The statements of support are sent by the European Commission to the Member States competent authorities for verification. This transmission is done via a secure online file transfer.	- The European Commission sends all the statements of support to the Member States competent authorities. - This process could benefit from the EU file transfer service to implement a more secure transmission of the statements of support.	5.00	
		Competent Authorities	The national competent authorities are in charge of verifying the statements of support.	The national competent authorities verify the statements of support.	4.00	
		Organisers	The responsibility of organisers is limited as far as possible. When they use the Commission provided system, they are not in charge of the transfer of the statements of support to national competent authorities. However, they remain in charge of transferring the statements of support collected in paper form to the European Commission.	The organisers are responsible for scanning the statements of support collected in paper and upload them to the online collection system.	3.00	
				Criteria average Score		4.00

Technical	**Implementation**	Installation	The online collection system is implemented using well-known technologies and software stack, which are recognised as de facto standards.	In this scenario, to facilitate the process, new initiatives are included in the pre existed database and file-system. To ease the installation the source code is in a pom.xml file. This is prepared to be used by the most widely used Java compilation environment: maven.	4.50	
		Scalability	The online collection system architecture is designed in a way that allows scalability of resources without refactoring of the source code and with little or no development costs	The online collection system in a physical or virtual server fully achieve its objective, the system allows to collect 4 million statements of support in one day. Under these circumstances the initiatives are stored in the same online collection system, such a server could host over 50 initiatives.	5.00	
		Maintenance	The online collection system architecture makes it easy to maintain by isolating functionalities in layers and components.	In the short term changes are foreseen, due to the integration of eIDs, on a long term no other modifications can be anticipated. The maintenance effort for this scenario are less demanding since it is need to be done once for all initiatives.	4.50	
				Criteria average Score		**4.67**
	Operations	System administration	The installation and monitoring of the online collection system doesn't create any burden for the system administrators in charge of the infrastructure on which it is running.	This covers the following activities - Installation of the system - Update of the software based on discovered flaws and security breaches, and revision of log files during the life-cycle of the system, - Disposal/migration For this scenario, the task are more efficient since they apply to all initiatives at the same time.	4.50	
		Verification process	The online collection system supports the verification process by competent authorities and allows the most optimal use of the resources and infrastructure	This scenario allows to implement more controls to support the verification process.	4.00	
				Criteria average Score		**4.25**
Security	**Security architecture**	Competent authority	Communications between the Competent authority and the online collection system are sufficiently secure (for example using https with TLS)	Communications with the central Commission online collection system is less changeable in security configurations (both perimetral systems and the online collection system).	4.00	
		Commission	The Commission's Hosting service and Data center are secure enough (with security certifications evidence), and compliant with the ECI regulation	The central Commission online collection system is compliant with the ECI Regulation, and centralised for a better management of possible security breaches (physical or logical).	5.00	
		Organiser	The organiser choose a hosting provider with adequate security level (including certifications evidence), and compliant with the ECI regulation.	n/a	-	
				Criteria average Score		**4.50**
	Software development security	Competent authority	Certification of the online collection system by the national competent authorities in Member States meets the security criteria (black/white box approach), in addition to the audit of the technical specifications.	No certification by competent authorities needed	5.00	
		Commission	Development of the Commission's online collection system following technical specifications and taking into account Security in Development Lifecycle.	The Commission develops, maintains and improves a central Commission online collection system compliant with the ECI Regulation (and with extra technical specifications).	5.00	
		Organiser	Development of the third party's online collection system following technical specifications and taking into account Security in Development Lifecycle.	n/a	-	
				Criteria average Score		**5.00**
	Data security & integrity	Competent authority	The process of reception and storage for verification is secure enough and compliant with regulation, guaranteeing integrity and confidentiality.	The reception and storage of the data collected from the Commission's online collection system of each initiative (exported data), for the verification, is done in accordance with national regulations for IT security.	4.00	
		Commission	The process of collecting, sending and storing of Statement of Support is secure enough and compliant with ECI regulation, guaranteeing integrity and confidentiality.	The storage and sending of the data collected in the Commission's online collection system, for the verification by the Member States, is done under the sole responsibility of the Commission and complies with Commission Decision (EU, Euratom) 2017/46.	4.00	
		Organiser	The process of collecting, sending and storing of Statement of Support is secure enough and compliant with regulation, guaranteeing integrity and confidentiality.	A malicious organiser (insider) could try to hack the central Commission online collection system, exploiting a possible vulnerability to manipulate the data.	4.00	
		External User	The online collection system is protected against intentional or unintentional manipulation from the client side.	A malicious client user (outsider) could try to hack the central Commission online collection system, exploiting a possible vulnerability to manipulate the data.	4.00	
				Criteria average Score		**4.00**
	Identify and access management	Commission	The Commission has only the necessary permissions to manage the information collected in the online collection system, and the process of identification and authentication is secure enough.	The access of the Commission, as an admin role, has several security requirements in the technical specifications 2.7.3 h.	4.00	
		Organiser	The organiser has only the necessary permissions to manage the information collected in his/her online collection system, and the process of identification and authentication is secure enough.	The organisers have a limited access to the online collection system with no direct access to the personal data for the data collected online.	4.00	
				Criteria average Score		**4.00**

Cost	**Costs Commission**	Infrastructure	The infrastructure costs are optimised when compared to the AS IS situation by sharing common resources and sizing it according to workload, while meeting all ECI legislation requirements	The infrastructure costs remains in the same price range compared to the AS IS situation. An improvement of the unit hosting cost is anticipated but the hosting of all ECIs and some additional costs, such the EU File Sharing Service and eIDAS fees, are taken into account. In addition, the operations of the infrastructure will be greatly facilitated by this approach.	4.00	
		Development	The development efforts are optimised when compared to the AS IS situation, taking into account the costs of adding the same functionalities in the current online collection system.	An investment of one million one hundred thirty euros should be made to configure the online collection system for a permanent hosting in DIGIT data centre and to add the full range of new functionalities.	3.00	
		Maintenance	The maintenance costs of the online collection system are optimised over a five-year period when compare to the AS IS situation.	Maintenance costs are expected to be lower than the AS IS situation, although the new functionalities imply extra maintenance costs compared to scenarios 2.	4.00	
		Support	The support and operational costs of the online collection system are optimised over a five-year period when compared to the AS IS situation	Support costs are doubled compared to the AS IS situation. However, they cover a much wider set of features, including full integration of the Register and automation of the deployment.	3.00	
				Criteria average Score		**3.50**
	Costs Organisers	Infrastructure	The infrastructure costs are optimised when compared to the AS IS situation.	Organisers no longer incur any costs	5.00	
		Development	The development efforts are optimised when compared to the AS IS situation.		5.00	
		Maintenance	The maintenance costs of the online collection system are optimised over a five-year period when compare to the AS IS situation.		5.00	
		Support	The support and operational costs of the online collection system are optimised over a five-year period when compared to the AS IS situation		5.00	
				Criteria average Score		**5.00**

12 APPENDIX IV – TERMS AND ACRONYMS

12.1 ACRONYMS USED THROUGHOUT THE REPORT

Acronym	Institution
DMZ	Demilitarised Zone
DoS	Denial of Service
DPO	Data Protection Officer
EC	European Commission; the Commission
ECI	European Citizens' Initiative
EDPS	European Data Protection Supervisor
eID	Electronic Identification
eIDAS	Electronic Identification and Trust Services (EU Regulation 910/2014)
EU	European Union
HSM	Hardware Security Module
HW	Hardware
IDS/IPS	Intrusion Detector System / Intrusion Protection System
IP	Internet Protocol
ISO	International Standardisation Organisation
IT	Information Technology
MS	Member States
OCR	Optical Character Recognition
OWASP	Open Web Application Security Project
SAMM	Software Assurance Maturity Model
SDLC	Software Development Life Cycle
SoS	Statement of support
SW	Software
WAF	Web Application Firewall

Table 28: Acronyms

12.2 GLOSSARY

Term	Definition
Regulation (EU) 211/2011	Regulation on the citizens' initiative.
Regulation (EU) 2016/679	Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation).
Commission	Commission Implementing Regulation (EU) 1179/2011 of 17 November

Implementing Regulation (EU) 1179/2011	2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) 211/2011 of the European Parliament and of the Council on the citizens' initiative.
Regulation (EU) 910/2014	Regulation (EU) No 910/2014, of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
Directive 95/46/EC	Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Regulation (EC) 45/2001	Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.
Commission Decision (EU, Euratom) 2017/46	Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission

Table 29: Glossary