



Secretariat-General
Directorate General for Informatics

D02.04 Final Report

Specific Contract n° 063 under Framework Contract DIGIT/2020/OP/0005 – BEACON – Lot 2:

Study on Technical Solutions for Organisers of European Citizens' Initiatives

Date : 30/06/2023

Doc. Version : [3.00]

Template Version : 2.5

Disclaimer

This deliverable was prepared for DG-DIGIT by PwC & Sopra Steria consortium under SC063 and is the European Commission's property. The views expressed in this document are purely those of the authors and may not, in any circumstances, be interpreted as stating an official position of the European Commission. The European Commission does not guarantee the accuracy of the information included in this document, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the authors to ensure that they have obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

© European Union, 2023

Table of Contents

List of Tables	5
List of Figures	5
List of Abbreviations	6
Executive Summary	7
1. Introduction	17
1.1. The European Citizens' Initiative and the collection of statements of support	17
1.2. Problem Definition	17
1.3. ECI Legal framework and key assumption	18
1.4. Structure of This Report	19
1.5. Limitations of the study	19
2. Objective and Scope of the Study	21
3. Methodology: A Three-Phase Approach	22
4. Phase I: Fact-Findings	23
4.1. Step I - Identify and Define the Technical Solutions Proposed for the ECI's Organisers	23
4.2. Step II - SWOT Analysis of the Technical Solutions	25
4.3. Step III - Stakeholders' Consultations: Questionnaire and Interviews	27
5. Phase II: Analysis of Results	31
5.1. Presentation and Analysis of the Data Collected in Phase I	31
5.1.1. Results' Summary: Organisers " <i>Fur Free Europe</i> " - " <i>Stop Finning</i> ", and the ECI Campaign	32
5.1.2. Results' Summary: Auditor of the CTIE of the Luxembourg Government	33
5.2. Solutions Functional and Technical Requirements	34
5.2.1. Definitions of the Technologies for the Implementation of the Embeddable Solutions	34
5.2.2. Technical Solutions: Functional and Technical requirements	35
5.2.3. Operational Management, Auditing, Implementation and Maintenance Costs of the Technical Solutions	38
5.2.4. Data Protection and the Current ECI's Regulation	44
5.2.5. Risk and Security Assessment	46
6. Phase III: Recommendations	65
6.1. Key Takeaways on the Technical Solutions' Main Elements and Benefits	65
6.2. Key Takeaways on Technical Implementation, Operational Management and Costs	65
6.3. Key Takeaways on the Technical Solutions: Security, Data Protection Risks and Mitigation Strategies	66
6.4. Key Takeaways on the Impact of the Embeddable Technical Solutions on UX	67
6.5. Recommendations on the UX Approach to Succeed in the Implementation	68
6.6. Recommendations on the Embeddable Solutions' Auditing Mechanism and Estimated Costs	69
6.7. General Recommendations and Scenarios to Consider for the European Commission	70
6.8. Recommendations for a Future Viewpoint	71
Bibliography	73

Research Team - Biography	75
List of Annexes	77
Annex I - Work Plan and Project's Objectives	77
Annex II - Risks Matrix	79
Annex III - ECI's Stakeholders' Questionnaire	80
Annex IV - ECI's Stakeholders' Answers	81
Answers: Centre des Technologies de l'information de l'État Luxembourg	81
Answers: Fur Free Europe	86
Answers: the ECI Campaign	89
Answers: Stop Finning – Stop the Trade	94
Annex V - Email sent from the German Federal Office for Information Security to the Secretariat General on 31 January 2023	97

List of Tables

Table 1: Implementation, Maintenance, Operational Management, Regulatory, Risks	13
Table 2: Risks for each Embeddable Solution	14
Table 3: List of technical solutions.....	23
Table 4: SWOT analysis of iframe solution - TS01	25
Table 5: SWOT analysis of Iframe in Microfrontend solution - TS02.....	26
Table 6: SWOT analysis of API gateway solution - TS03.....	26
Table 7: Stakeholders' Matrix and Preliminary Impact of an embeddable solution.....	28
Table 8: Stakeholders' Summary of Interviews Dates and Approvals.....	31
Table 9: Inductive Coding of organisers interviews	32
Table 10: Inductive Coding of auditor's interview.....	32
Table 11: Operational Management.....	39
Table 12: Costs for the Auditing and the Certification of embeddable solution.....	41
Table 13: Costs (effort) of Implementation and Maintenance.....	42
Table 14: Costs (in €) of Implementation and Maintenance	43
Table 15: Impact on Performance	43
Table 16: Impact on the ECI Regulation	45
Table 17: General assessment of security and data protection risks.....	47
Table 18: Risks for each Embeddable Solution	48
Table 19: Risk Likelihood/Impact matrix.....	79

List of Figures

Figure 1: Study's Methodology	22
Figure 2: ECI's Stakeholders	28
Figure 3: iframe solution (TS01)	35
Figure 4: iframe solution in Micro Frontend (TS02)	38
Figure 5: API Gateway solution (TS03).....	38
Figure 6: Number of Risks	48
Figure 7: Securing the 3-Step Pathway of the Personal Data Collection Process.....	64
Figure 8: Project Tasks	77
Figure 9: Project's Objectives	77
Figure 10: Project Schedule	78

List of Abbreviations

Abbreviation	Full Title
CDN	Content Distribution Networks
CSP	Content Security Policy
CSS	Cascading Style Sheets
CTIE	Centre des Technologies de l'information de l'État – Luxembourg
COCS	Central Online Collection System
CORS	Cross-Origin Resource Sharing
CSRF	Cross-Site Request Forgery
DoS	Denial of Service
DDoS	Distributed Denial of Service
ECI	European Citizens' Initiative
EFF	The Electronic Frontier Foundation
GUID	Globally Unique Identifier
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IOCS	Individual Online Collection System
NPM	Node Package Manager
PPID	Pairwise pseudonymous identifiers
REDOS	Regular Expression Denial of Service Attackers
SSL	Secure Sockets Layer
SRA	Security Risk Assessment
SSRF	Server-Side Request Forgery
SWOT	Strengths, Weaknesses, Opportunities, and Threats
OWASP®	The Open Worldwide Application Security Project®
TLS	Transport Layer Security
XFS	Cross-Frame Scripting
XSS	Cross-site Scripting

Executive Summary

Since 1 January 2023, the online collection of statements of support for European citizens' initiatives, must be done through the European Commission's Central Online Collection System (COCS).

The COCS does not offer the possibility to decentralise an embeddable solution on an external website, while it does provide for the possibility to implement a link on campaigning websites to redirect citizens to the COCS, who then support an ECI and provide their personal data on the European Commission's secure system. In this context, this study evaluates the technical solutions for decentralising the support collection form (the frontend part) of the COCS on external websites under certain conditions (so-called embeddable solutions). This follows a request by ECI organisers to the European Commission to have such an embeddable solution that allows citizens to provide their support directly on the organisers' campaigning websites.

The study has identified three embeddable solutions, which have been evaluated having regard to the European Commission's concerns about the security and data protection risks of such embeddable solutions, the potential need to adapt Regulation (EU) 2019/788 (ECI Regulation¹), the costs associated with their implementation and long-term maintenance (for organisers, the European Commission and Member States), and how these solutions can interact with the COCS backend² part on the European Commission secure servers.

A three-phase methodology was designed, with two major investigative phases and one conclusive phase³ to address the key research questions:

Are there one or more embeddable solutions that the Commission can offer to ECI organisers that ensure security and personal data protection, which are compliant with the ECI Regulation? What are the estimated impacts from an operational management and budgetary perspective?

Stakeholder Consultations: Business View versus Risk View

We collected the views of two organisers and one civil society organisation. Their general business view is that an embeddable solution should be offered by the European Commission. The two organisers interviewed considered that an embeddable solution would better engage and maintain the supporters on the organisers' campaigning website and improve the chances to collect more financial donations. Supporters are seen as potential financial donors, and they provide a return on the initial investment. An embeddable solution would also provide the possibility to customise the collection form, and to collect analytics and extract information on the statements of support to target the supporters. Moreover, it allows decentralisation to third parties' websites, offering a wider impact. They also considered that an embeddable solution would facilitate the harvesting of supporters' emails for signing up for their newsletter and for future activities.

The national certifying authority interviewed articulated serious concerns as regards to the possible security and data protection risks for the safety of EU citizens' personal data, and expressed opposition to the implementation of an embeddable solution by the European Commission for the frontend² part of the COCS. In his opinion, security and data protection risks outweigh the potential benefits of an embeddable solution offered to organisers. He considers that with an embeddable solution, and especially with the API Gateway solution, the European Commission risks to lose control (in the sense of not being able to enforce the security standards, risk mitigation measures and rules related to the process of collection of statements of support). He also underlined that an embeddable solution has not been identified as a general need by organisers nor as being critical to the proper general functioning of the ECI instrument.

¹ Regulation (EU) 2019/788 of the European Parliament and of the Council of 17 April 2019 on the European citizens' initiative.

² Websites consist of two parts: the frontend which end-users see, and the backend, which provides the services to the frontend part.

³ Further information on the methodology is provided in Chapter 3, and on the limitations of the study in section 1.5.

Technical Solutions: Main Elements and Benefits

In the SWOT⁴ analysis this study identified three possible technical solutions that could provide an answer to the research questions. The first technical solution identified is named *'iframe'*. An iframe is an in-line frame and it is commonly used to embed specific content like external ads, videos, tags, or other interactive elements into a page. The main advantage of iframe is that it can be easily placed almost anywhere within a website. This first Iframe solution provides organisers with a 'view' within their campaigning website on the whole COCS frontend part located on the European Commission servers. The second technical solution identified is *'iframe + Micro Frontend Application'*. Micro Frontend permits to decompose the COCS of the European Commission website into independent 'microapps' working loosely together. This second solution would provide organisers with a 'view', within their campaigning website, on the support collection form of the COCS frontend part located on the European Commission servers. This is different from the first iframe solution, where the whole COCS frontend website of the European Commission would be loaded within the campaigning website. The third technical solution identified is *'API Gateway solution'*. The European Commission will have to set up an API Gateway for the ECI, which can be used together with a support collection form developed by the European Commission, a third party, or the ECI organisers themselves. If the API Gateway will not be available for the ECI, as an alternative, the support collection form could be decentralised via web services, which also offer customisable opportunities.

All three solutions would only partially meet the organisers' needs, because these solutions will not easily allow the customisation of the collection form, or the collection of analytics, or the decentralisation on third parties' websites.

Technical Solutions: Security, Data Protection Risks and Mitigation Strategies

All solutions identified present high security and data protection risks, which should be carefully considered by the European Commission before deciding on their potential implementation. **These risks are associated with the decentralisation of the embeddable solution on any other external website.** For all three solutions, supporters will physically insert their personal data on the organisers' campaigning websites. A malicious actor could threaten the confidentiality, integrity and availability of the personal data when EU citizens fill in the support form via the organisers' campaigning websites if these are insecure websites.⁵ By decentralising the collection of personal data, there is an increased risk of data breach in comparison to the, currently offered, redirection option to the COCS on the European Commission secure servers. However, there is a substantial technical difference with the three solutions identified (which affects and increases risk) and it relates to location of the source code of the support collection form. The source code of the API Gateway collection form would be located on the campaigning websites; this will further increase the risk that the European Commission will lose control of the process of collection of statements of support. Furthermore, the decentralised source code is vulnerable to manipulation as the frontend part of this solution will be independent from the COCS backend, and it will only transmit the supporters' personal data to the European Commission storage, or potentially to another data storage set up by the organisers or other malicious actors. The iframe, instead, provides organisers with a 'view' on the COCS frontend part located on the European Commission servers. In this latter case, the source code of the collection form will still be located only on the European Commission servers, and as such there is no transmission of data involved. For all three solutions, personal data collected will still be stored within the COCS backend on the European Commission servers.

The iframe solutions pose a medium-high security risk, while the API Gateway solution poses a high security risk to the personal data of the EU citizens. This study has identified seven major risks for the iframe solutions, while the API Gateway solution presents fifteen major risks. Main security and data protection breaches could be caused by phishing, cross-site scripting, code injection, security misconfiguration, excessive data exposure, mass assignment, etc. These types of risks are explained and detailed in [section 5.2.5](#) below. For all these risks, the study suggests specific mitigation

⁴ SWOT stands for Strengths, Weaknesses, Opportunities, and Threats. A SWOT analysis is a technique for assessing these four aspects of a project. The analysis can help to understand different scenarios and options, and in particular what is the best option for a successful strategy for the future.

⁵ Art. 33 of the Regulation (EU) 2018/1725, on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

strategies (see [section 5.2.5](#)). Nevertheless, it is important to highlight that **there are no mitigation strategies that can offer the same level of security as the current redirection option of the centralised COCS**, which provides citizens with the possibility of filling in the form with their personal data on the highly secure server of the European Commission. Mitigation strategies, if properly applied, only reduce the risks identified, however, the overall conclusion is that in any of the solutions **the residual risk after mitigation remains high**, because most **organisers have limited technical and security expertise on the risks associated with an embeddable solution**. In addition, most organisers will not be experts, and as seen in interviews, they have limited understanding of the risks associated with the collection of personal data via an embeddable solution. Therefore, the European Commission cannot base its risk mitigation strategies on trust of the organisers' compliance with the rules.

In addition to the above risks, interviews revealed that some organisers have also decentralised the IOCS support collection form in the websites of partners organisations which were not covered by the certification. Our study has found that risks of data breach increase when the support collection form is decentralised in many other websites that are not audited; these risks also apply to the embeddable solutions identified in this study. Organisers that were interviewed do not seem to be aware of these risks, as they indicated that they trusted the private collection software provided to them, and the fact that the same software has been initially certified by the German certifying authority (BSI), and that their main campaigning website was also certified. However, that certification was issued by the national authority based on the submitted information that the IOCS support collection form would only be hosted on one campaigning website. The national authority was not informed that organisers decentralised the support collection form on other websites.⁶ Further security risks derive from potential misuse and mishandling of the support collection form by organisers, other malicious actors, and the possibility of data being collected in private data storages, a risk that can only to a limited extent be mitigated through an auditing or a certification process. There is also a risk that the other websites, where the support collection form was embedded, were not located within the European Union territory (as mandated by the ECI Regulation⁷) but outside.

One of the organisers has also indicated that the embeddable solution could provide them with the possibility of obtaining, harvesting, and saving supporters' emails, not only to be used in the context of their ECI but also for future and/or other long-term activities. Given the scope limitation in the ECI Regulation, the collection of email addresses for such broader purpose is not allowed as part of the collection of statements of support within the ECI context. It would also require a separate additional consent under the GDPR.

Considering that any of the embeddable solutions will imply a technical change to the current COCS, and personal data/statements of support will be collected via the campaigning websites, if the European Commission would consider implementing one of the embeddable solutions, it will have to produce a yearly security plan (which includes a risk assessment) specific for the embeddable solution to cover the identified risks and mitigation measures needed to address those risks. It will also need to ensure auditing of the embeddable solution decentralised on any campaigning website. Furthermore, for the embeddable solution using the API Gateway, the organisers will need to produce their own security plan, which will need to be regularly updated as well as every time a new risk arises.

Operational Management and Implementation's Costs

Operational management impacts the European Commission and the organisers in terms of the team required for the implementation and maintenance of the embeddable solution.

In terms of technical implementation, all solutions identified are viable and can be implemented for the frontend part of the COCS. As regards to the complexity of implementation and estimated costs, all solutions require substantial effort and costs for their implementation and yearly costs for maintenance. For implementation, the estimated costs are one-off costs for the development of the solution by the European Commission and the organisers' integration of the embeddable solution on maximum three campaign websites. The first iframe solution is easy to implement for the EC and the

⁶ Email sent from the BSI, German Federal Office for Information Security (ECI websites' certification authority) to the Secretariat General on 31 January 2023. (Annex V)

⁷ Art.11 of the Regulation (EU) 2019/788.

organisers. In terms of costs, it is medium-costly for the European Commission (€39,000 to €58,500 one-off) and low for organisers (€9,750). The second iframe solution has a medium-high difficulty of implementation for the European Commission, while it will be relatively easy for the organisers to integrate in their campaigning websites. In terms of costs, the second iframe solution, is high-costly for the European Commission (€117,000 to €156,000), and relatively low for organisers (€9,750). The API Gateway solution, instead, is hard to implement and high-costly for both the European Commission (€156,000 to €195,000) and the organisers (€19,500 to €58,500).

Long term maintenance for the embeddable solutions also requires efforts on both the EC and the organisers. Maintenance costs are estimated on a yearly basis, for each initiative and for a maximum of three campaign websites where the embeddable solution is decentralised. The first iframe solution is easy to maintain and requires low costs for both the EC (€9,750 to €13,000 per year) and the organisers (€6,500 per year). The second iframe solution has medium difficulty and requires medium maintenance costs for the European Commission (€39,000 to €58,500 per year), while it is easy to maintain for the organisers and has relatively low costs (€6,500 per year) on them. The API Gateway solution, instead, is hard to maintain and requires very high maintenance costs for both the European Commission (€58,500 to €78,000 per year) and the organisers (€39,000 per year). Detailed estimate of costs for the implementation and maintenance are provided in [section 5.2.3.2](#) below.

Recommendation on the Embeddable Solutions' Auditing Mechanism and Estimated Costs

For all three solutions, in terms of security risk management, the most effective way of controlling security and data protection risks would be to set up a new certification/auditing mechanism conducted by the Member States authorities or by the European Commission, and with a set of technical requirements comparable (but stricter) to the ones previously provided for the IOCS under Implementing Regulation (EU) 2019/1799. As mentioned above, it is important to stress that most organisers have limited technical and security expertise on the risks associated with an embeddable solution. In addition, the European Commission cannot base its security risk management on trust of the organisers' compliance with the rules, therefore, on these premises, we strongly recommend setting up an audit mechanism if an embeddable solution is implemented. The auditing of the organisers' websites and the embeddable solution should be performed every 4 months, during the 12-month collection process (including the initial auditing/certification of the system). However, as indicated by the national certifying authority during the interview, Member States may not have the necessary resources/budget to perform regular audits and/or the certification process if this involves several websites, because the process is very time consuming and costly. These costs, if outsourced to a private company, would require a security expert to work an average of 5 working days per single audit and per each campaign website (this work is estimated at €3,250 every 4 months). In addition, there are the initial costs of the auditing (or the certification) for the embeddable solution before starting the collection of statements of support, which are estimated at €10,000 (one-off costs). The complexity of the auditing and its costs could put an excessive burden on national authorities.⁸ As to contain those costs, it is recommended to allow the embeddable solution only for a limited number of campaigning websites (1 to 3). This limit may however only partially meet the business needs of the organisers. Given that the ECI Regulation currently does not contain such audit and certification mechanism, an amendment of the regulation through the ordinary legislative procedure would be necessary. As a temporary solution, and only for the Iframes' technology, the organisers could sign a personal data joint controllership agreement with the European Commission that specifies the technical, security and organisational measures, as pre-conditions for obtaining the solution. The joint controllership agreement would also contain provisions regarding the regular auditing by the Commission of the organisers' websites. Further, the joint agreement should also tackle the organisers' compliance with the principles laid down in the Decision (EU, Euratom) 2017/46⁹. For the API Gateway solution an amendment of the ECI Regulation would be compulsory before considering any possible implementation. This is a high-risk solution which impacts and drastically change the

⁸ Interview with the Luxembourg Government authority, held on 10 February 2023. Evidence attached to Annex IV.

⁹ Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission.

current COCS, as the source code of the support collection form will be located on the organisers' websites, and not anymore on the European Commission secure servers.

General Recommendations and Scenarios to Consider for the European Commission

From the above discussion and analysis of the operational management, implementation, costs, security and data protection risks, we have come to the following recommendations in relation to the embeddable solutions identified, in order of preference:

- a) First-best option: Do Nothing;
- b) Second-best option: Consider Implementing the iframe + MicroFrontend;
- c) Third-best option: Do not implement the API Gateway.

Our first recommendation is that "Do Nothing" (hence not offering any embeddable solution), is the best defensible option under this assessment. Maintaining the current system as-is has important benefits, notably that the critical risks associated with the embeddable options are avoided. The European Commission can continue to offer and improve the user-friendliness of the current COCS in its centralised and secure form on its servers. No certification and auditing by a dedicated authority is required. There are no additional associated costs for the European Commission or organisers as the COCS will continue to be offered as a free-of-charge turnkey solution to organisers. The COCS has proven already in its three years of operation to be effective, as two initiatives collected over 1 million statements of support with the current redirection option. Supporters have expressed a high satisfaction rate for the current COCS. Emails and personal data of EU citizens are well protected on the European Commission servers. Following this recommendation would mean that the European Commission would not need to spend substantial costs for implementing and maintaining a very costly solution. "Do nothing" however presents the weakness that no alternative is offered to those organisers that would like to have an embeddable solution on their website to address their needs. This study has not considered alternative options to address those needs, as the research questions strictly focussed on the embeddable solutions as advocated by the stakeholders concerned.

As a second-best option, we recommend the European Commission to consider implementing the iframe with the Microfrontend application solution. It would help to maintain the supporters on the campaigning websites; they can provide their support without being redirected to the European Commission website. Organisers can collect emails at the end of the collection process in compliance with the ECI Regulation. This solution will provide an alternative to the existing redirection option of the COCS. It is a less risky solution than the API Gateway solution. As a matter of fact, given that, as of January 2023, almost 50% of website navigations in Europe are done on a mobile device (and that increases every year), if the European Commission will implement the iframe, we recommend that this solution is designed in first instance for smartphones, and later then for the other devices (mobile first design). Iframes are responsive for mobile, and the iframe first configuration would be organised by the European Commission on the COCS, but these settings could be edited and adjusted by the organisers according to their campaigning websites.

We have excluded from our recommendations the first iframe solution as it would not bring any benefit in framing the whole COCS within the organisers' campaigning websites, while the iframe solution with the Microfrontend allows only the support collection form to be iframed in the organisers' websites, however, with this solution the organisers cannot gather data analytics, as they could have done with the IOCS or with an API Gateway solution. This iframe solution is costly for the European Commission, which should cover the implementation, maintenance, and auditing on top of the management costs of the COCS. Auditing would also introduce a new role and activity for the European Commission and/or national authorities, and possibly costs for the organisers. However, this solution is less costly than the API Gateway solution, because with this Microfrontend, the European Commission would maintain one application, instead of maintaining several applications like for the API (the API gateway solution requires very technical components like libraries, middlewares, transmission between frontend and backend).

As a third-best option we do not recommend the European Commission to implement the API Gateway solution, because the drawbacks outweigh the benefits of its implementation. First, it will be difficult and very costly for both the European Commission and the organisers to implement and

maintain. It is a high-risk technical solution prone to the risk of security and data protection breaches. It presents relevant challenges for the dedicated authorities (Commission or potentially the Member States' authorities) as the solution's source code must be regularly audited to mitigate the most important risks.

This solution also does not meet the expressed needs of organisers that stated that an embeddable solution should be kept as easy as possible to accommodate those organisers with limited knowledge of IT. Of all embeddable solutions, the transmission of personal data via an API Gateway allows the least control by the European Commission before the data reach the European Commission's data storage, thus presenting substantial risks. The purpose of a "transmission" API is to transfer personal data collected by the campaigning sites to the central storage. This solution would pose risks comparable to the ones of an IOCS. A malicious actor could target not only the embeddable solution, the campaigning website of the organisation, but also take control of the personal data of the EU citizens before they are sent to the European Commission servers. In addition, there is a risk that organisers would be able to re-build a new individual collection system just by using the API endpoint as a transmission interface to send the data to the central system; nothing would prevent the organisers to store the data locally before transmitting the information to the central system.

Recommendations for a Future Viewpoint

In conclusion, while from a technical perspective all solutions are feasible, from a security and data protection risks perspective, **a direct answer to the research questions is that there is not an embeddable solution that can be offered to ECI's organisers that ensures the current level of security and data protection currently offered by the COCS solution with the redirection option.** The COCS ensures that the personal data of EU citizens are collected, transferred and stored directly on the secure servers of the European Commission without any third-party interference.

Further, some of the organisers' business needs, like the need to harvest supporters' emails for other purposes than defined under the ECI Regulation, raise concern about the possible misuse of data, and the embeddable solution itself increases the risks of data mishandling and data breach. If the embeddable solution would lead to a data breach, it could also lead to reputational damage for the European Commission and the ECI instrument. Although there are mitigation strategies for the risks reported, it is very unlikely that organisers will have the necessary skills and the capacity to set up and implement proper mitigation strategies, and acquiring them through external providers will involve substantial costs. Therefore, we estimate that the residual risks, even with the mitigation strategies in place, will be still high. Consequently, an embeddable solution is unlikely to be as secure as the current COCS fully hosted in the European Commission premises.

If an embeddable solution is offered to organisers, the European Commission will need to bear (most of) the high costs associated with the development, the maintenance, the operation, and the auditing of the embeddable solution.

On a cost-benefit analysis, major red flags not to implement an embeddable solution would be the risks of data breach, the high costs to mitigate these risks, the reputational damage resulting from a data breach, the significant cost for the European Commission in financial terms and in terms of operational resources necessary to implement and maintain the embeddable solution. Furthermore, the embeddable solution may also have a limited impact and benefit on the supporters' journey to provide their support.

Given the above considerations, if the European Commission would decide to bear the risks and the costs associated with the offering of an embeddable solution, our recommendation would be to consider implementing the "iframe" solution in the format of the Micro Frontend, because it will be a compromise option between the organisers business needs, and the European Commission's concern for security and personal data protection risks. **This solution, however, poses a medium-high security risk of a data breach, and only offers limited security** under the pre-condition that proper security risk management is in place for both parties, the European Commission and the organisers. Therefore, **this solution should be implemented only after a careful consideration and a full cost-benefit analysis.**

Final Report

Table 1¹⁰: Implementation, Maintenance, Operational Management, Regulatory, Risks

	Technical Solutions	iframe + better UX (TS01)	iframe + Micro frontend (TS02)	API Gateway + form (TS03)
Organiser's Needs	Organisers Business Needs	partially meets needs	partially meets needs	partially meets needs
Costs: Implementation and Maintenance	Implementation difficulty for EC	low	medium-high	high
	Implementation effort for EC	medium	high	high
	Implementation difficulty for organisers	low	low	high
	Implementation effort for organisers	low	low	high
	Long term maintenance difficulty EC	low	medium	high
	Long term maintenance effort EC	low	medium	high
	Long term maintenance difficulty organisers	low	low	high
	Long term maintenance effort organisers	low	low	high
Impact	Mobile solution (customisation with related costs for the EC)	Responsive for mobile (iframe first configuration, but can be editable by organisers)	Responsive for mobile (iframe first configuration, but can be editable by organisers)	Responsive for mobile (relies on organisers to set proper styles)
	Impact on the redesign of the COCS	minimum	medium	high
	Campaign Site Performance Impact	high	high	high
Impact: Regulatory	Regulatory impact	Medium (joint controllership agreement - temporary and/or amendment)	Medium (joint controllership agreement - temporary and/or amendment)	High (amendment required)
Operational Management	Operations (internal team involved and profiles)	medium	medium-high	high
	Security Plan (for the embeddable solution)	Set up by the EC on a yearly basis and for their own system	Set up by the EC on a yearly basis and for their own system	2 security plans: 1 set up by the EC, and 1 set up by the organisers for the frontend part.
	Compliance review of audit requirements (Risks, Security, Regulatory per each campaign website)	Yes; audit twice during the collection period. (Once at the beginning and once after 6 months).	Yes; regularly required during the collection process (beginning, then every 4 months until conclusion of collection)	Yes; regularly required during the collection process (beginning, then every 4 months until conclusion of collection)
	Complexity of auditing the code (IT solution embedded in campaign site)	low	medium	High
Security and Data Protection	Security risks	medium-high	medium-high	high
	Data protection risks	medium-high	medium-high	high
	Phishing	high	high	high
	Cross-site scripting	high	high	high
	Code Injection	high	high	high
	Security misconfiguration	medium-high	medium-high	high
	Excessive data exposure	medium-high	medium-high	high
	Mass assignment	medium-high	medium-high	high

¹⁰ In the table the different categories are evaluated according to a 4 points scale with different colours: Low, Medium, Medium-High, High.

Table 2: Risks¹¹ for each Embeddable Solution

	Risk	Likelihood	Impact	Risk Level	Risk Response Strategy reduced with Technical Mitigation	Residual Risk
Iframe (TS01 and TS02)	Phishing	4	4	16	Content Security Policy	medium-high
	Clickjacking	3	5	15	Client-side methods Server-side methods	medium-high
	Cross Site Scripting - Cross Frame Scripting	4	5	20	Secure frameworks Applying context sensitive coding Content Security Policy Sandbox attribute	high
	Security Misconfiguration	4	5	20	Specified HTTP verbs Cross-Origin Resource Sharing Policy	high
	Excessive Data Exposure	3	5	15	Filter Sensitive Data Classify sensitive and personally identifiable information Implement a schema-based response validation mechanism	medium-high
	Mass Assignment	4	4	16	Whitelist Built-in features to blacklist Enforce schemas for the input data payloads	medium-high
	Code Injection	4	5	20	Whitelist Encode HTML outputs Use a static type of system Use the HttpOnly flag for cookies Avoid JavaScript code serialization	high
API gateway (TS03)	Security Misconfiguration	4	5	20	API life cycle API response payload schemas Specified HTTP verbs Cross-Origin Resource Sharing Policy	high

¹¹ Risk Matrix is based on the PM² Methodology and it is attached to Chapter 8 of this report.

Final Report

	Broken Object Level Authorization	4	5	20	<p>Authorization Mechanism</p> <p>Random and unpredictable values as GUIDs</p> <p>Tests to evaluate the authorization mechanism</p>	high
	Broken User Authentication	3	5	15	<p>Authentication Mechanisms</p> <p>Multi-factor authentication.</p> <p>Anti brute force mechanisms</p> <p><u>Account Lockout / Captcha Mechanism</u></p>	medium-high
	Excessive Data Exposure	3	5	15	<p>Filter Sensitive Data</p> <p>Classify sensitive and personally identifiable information</p> <p>Implement a schema-based response validation mechanism</p>	medium-high
	Lack of Resources & Rate Limiting	3	5	15	<p>Use Docker</p> <p>Limit calls to API</p> <p>Server-side validation</p> <p>Maximum size of data</p>	medium-high
	Broken Function Level Authorization	4	5	20	<p>Deny all access by default</p> <p>Review your API endpoints</p> <p>Check user's group/role</p>	high
	Mass Assignment	4	4	16	<p>Whitelist</p> <p>Built-in features to blacklist</p> <p>Enforce schemas for the input data payloads</p>	medium-high
	Injection	5	5	25	<p>Validate incoming data</p> <p>Specific syntax</p> <p>Limit the number of returned records</p> <p>Data types and strict patterns</p>	very high
	Improper Assets Management	4	5	20	<p>Inventory all API</p> <p>Document all aspects of your API</p> <p>API documentation available</p>	high
	Insufficient Logging & Monitoring	4	4	16	<p>Log all failed authentication attempts</p>	medium-high

Final Report

					<p>Logs should be handled as sensitive data</p> <p>Security Information and Event Management (SIEM)</p> <p>Configure custom dashboards</p>	
Node Package Library (TS03)	Cross Site Scripting	4	5	20	<p>Keep Software Up to Date</p> <p>Scan For Vulnerabilities</p> <p>Encode And Sanitize User Input</p> <p>Web Application Firewall</p>	high
	Cross Site Request Forgery	4	5	20	<p>Synchronizer Token Pattern</p> <p>Double submit cookie technique</p> <p>Verifying Origin With Standard Headers</p> <p>Same-Site Cookies</p> <p>Enabling User Interaction</p>	high
	Code Injection	4	5	20	<p>Whitelist</p> <p>Encode HTML outputs</p> <p>Use a static type of system</p> <p>Use the HttpOnly flag for cookies</p> <p>Avoid JavaScript code serialization</p>	high
	Distributed Denial Of Service	5	5	25	<p>Design a Robust Architecture</p> <p>Use Cloud-Based Hosting from Major Providers</p> <p>Have a DDoS Response Plan</p> <p>Have a Static Version of Your Website</p> <p>Incorporate AI into your security stack</p>	very-high
	Regular Expression Denial Of Service Attacks	5	5	25	<p>Implement a strict time cut-off on search</p> <p>Preformat/validate your regular expressions</p> <p>Have the regex operation does not happen on the user thread</p>	very-high

1. Introduction

1.1. The European Citizens' Initiative and the collection of statements of support

The European Citizens' Initiative (ECI) is one of the major innovations introduced in the EU Treaties by the Treaty of Lisbon. It aims at involving citizens more closely in the agenda setting at EU level. A group of citizens that would like to launch a successful initiative has to collect statements of support from at least 1 million EU citizens from no less than seven Member States to call on the European Commission (EC) to propose legislation on matters where the EU has competence to legislate. The rules and procedures governing the ECI are set out in Regulation (EU) 2019/788 on the citizens' initiative (ECI Regulation) and were complemented by the Implementing Regulation (EU) 2019/1799,¹² laying down technical specifications for individual online collection systems. A group of citizens (the ECI's organisers) can only start gathering support for their initiative after their initiative has been registered by the European Commission. Statements for support can be signed online or in paper format. Depending on the Member State, the citizens have to fulfil certain data requirements when filling out the statement of support form.

Until 31 December 2022, the ECI Regulation provided the ECI's organisers with two online options (in addition to the paper format) to collect statements of support for their initiatives: a central online collection system (COCS) and an individual online collection system (IOCS). Therefore, ECI's organisers could have used the European Commission's COCS, which is in place since 1 January 2020, and it is provided cost-free. The COCS is a turnkey solution that does not require any further Member State certification. It is easy to set up and is multilingual, customisable and accessible for people with disabilities. It can be implemented with a redirection button to be placed on the ECI's organisers websites. In alternative to the COCS, ECI's organisers could have also set up their own IOCS or relied on a software¹³ developed by a third party.

However, Art. 11 of the ECI Regulation states that the option of using the IOCS was only valid for initiatives registered by 31 December 2022. From 1 January 2023, the ECI Regulation made mandatory for ECI's organisers to use the COCS provided by the European Commission system for their online collection of statements of support.

The COCS was developed by DIGIT according to the ECI Regulation to provide a secure environment for the online collection of personal data. The ECI Regulation made the European Commission the data controller of the personal data hosted on the European Commission servers, providing the highest level of data protection. The COCS offers End 2 End encryption of personal data, it is compliant with EUGDPR and all EC decisions and regulations on matters of security and data protection. Further, the COCS uses the European Commission secured infrastructure, and offers the automatic export and fast submission to Member States of the statements of support for successful initiatives that collected at least 1 million statements of support.

ECI's organisers, who wished to use their own IOCS, had to ensure that the system had adequate security features in place as required under the ECI Regulation and its Implementing Regulation. Furthermore, before starting the online collection, organisers had to secure the certification of their individual system by the national authorities of the Member State in which the data collected were stored.

1.2. Problem Definition

Given that the COCS is from 1 January 2023 the only online collection system allowed by the current ECI Regulation and available to ECI's organisers to collect statements of support, the European Commission has been approached by some stakeholders to allow for technical solutions that smoothen the online support process for EU citizens that visit their campaigning websites. The request

¹² Non-legislative act.

¹³ The ECI Campaign developed the Open ECI software, which was the only third-party software available for organisers and alternative to the official EC's online collection system. The ECI Campaign. "*OpenECI software*". <https://citizens-initiative.eu/openeci/>. Accessed on 8 February 2022.

was to have a technical option to allow citizens to support the initiative on the campaigning websites. This option could be particularly attractive for sponsors who campaign for the initiative, as it generates additional traffic to their own website. One of the options considered is to allow for the possibility to 'embed' in the organisers' campaigning website (or their campaigners' websites) the frontend application of the COCS. This option would go further than the currently available redirection option, in which the campaigning website contains a link to the COCS, where citizens can directly submit their statements of support (and thus their personal data) in a secure environment managed by the European Commission. With a decentralised embeddable solution, citizens will physically insert their personal data on the campaigning websites. The claimed benefits of this technical option would be that the citizens do not have to leave the campaigning websites, shortening the customer journey and leading to lower abortion rates, as well as the greater likelihood that the citizens will stay on the organisers' (or sponsors') websites. An additional benefit would be that the organisers can customise the support form in a way that matches with the look-and-feel of their own campaigning site. Nevertheless, an embeddable technical solution for the frontend part of the COCS carries certain security concerns and associated risks, and they can also present challenges from an operational, data protection and budgetary perspective.

It is also valuable to state at this stage that an embeddable solution will not be something similar to the now phased out IOCS. In fact, the IOCS was an independent alternative system, able to collect and store data independently from the COCS. This study strictly focuses on evaluating all possible embeddable technical options for the frontend part of the COCS, in other words the personal data collected will still be stored within the COCS backend. Therefore, the embeddable solutions identified will not represent an alternative system to the COCS, but if they will be eventually implemented, they will be complementary to the COCS, as they will work together with the COCS backend.

1.3. ECI Legal framework and key assumption

The collection of statements of support, both online and on paper, requires the collection of personal data on a large scale under the ECI Regulation. The data processed during the life cycle of an ECI's initiative is governed by the below regulations and decisions, from the most to the less specific to the matter:

1. Regulation (EU) 2019/788¹⁴ on the European Citizens' initiative;
2. Regulation (EU) 2018/1725¹⁵ on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data;
3. Regulation (EU) 2016/679¹⁶ (General Data Protection Regulation)
4. Decision (EU, Euratom) 2017/46¹⁷ on the security of communication and information systems in the European Commission.

The Implementing Regulation (EU) 2019/1799¹⁸, which laid down the technical specifications for the individual online collection systems (IOCS) pursuant to Regulation (EU) 2019/788, is not in the scope of this study, as the IOCS was phased out by the end of 2022. Initiatives registered as of 1 January

¹⁴ Regulation (EU) 2019/788 of the European Parliament and of the Council of 17 April 2019 on the European citizens' initiative.

¹⁵ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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.

¹⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

¹⁷ Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

¹⁸ Implementing Regulation (EU) 2019/1799 of 22 October 2019 laying down technical specifications for individual online collection systems pursuant to Regulation (EU) 2019/788 of the European Parliament and of the Council on the European citizens' initiative.

2023 can only use the COCS for the online collection of statements of support. However, the experiences acquired with the IOCS could be indirectly relevant for this study.

In consideration of the above regulations and the fact that the collection of statements of support implies the processing of personal data at a large scale, this study assumes that the support collection process of an ECI should offer, in first instance, the highest level of security for the collection of the personal data of EU citizens. In no way the support collection process should undermine the security of the personal data. Therefore, in the assessment of the embeddable solutions, the contractor is mindful that such solutions would need to be secured to the highest level possible.

1.4. Structure of This Report

This report is organised into the following chapters:

- Chapter 1, the current chapter, introduces the reader to the background information on the European Citizens' Initiative, the ECI legal framework, and the structure of this report. It also defines the problem based on the ECI's stakeholders' request to allow for technical solutions that smoothen the online process of signing for EU citizens that visit their campaigning websites.
- Chapter 2, focuses on the objective and scope of this study. It describes the challenges to overcome and sets the key research questions that this study attempts to answer.
- Chapter 3, introduces the three-phase methodology structured to gather the necessary information to answer the research questions.
- Chapter 4, elaborates on Phase I of the methodology: *fact-findings*. It provides the relevant information for this study: definition and SWOT analysis of the technical solutions proposed, the structure of the ECI's stakeholders questionnaire and the interviews. This chapter also provides some preliminary assessment based on the preliminary SWOT analysis.
- Chapter 5 elaborates on Phase II of the methodology: *analysis of results*. It provides an evaluation of the data collected in Phase I, including an analysis of the technical solutions functional and technical requirements. This chapter also presents results on the impact of the solutions on costs, operations, and management for the ECI's stakeholders, as well as on the risk and security aspects.
- Chapter 6 elaborates on Phase III of the methodology: *recommendations*. It depicts the actions and measures to be taken in different areas in order to make the change. The chapter provides analytical key takeaways and recommendations for a future viewpoint on the implementation of a technical solution for the frontend part of the COCS.

1.5. Limitations of the study

The study only had regard to the ECI Regulation. The Implementing Regulation (EU) 2019/1799 is not in the scope of the study. This latter regulation lays down the technical specifications for the individual online collection systems (IOCS) but does not contain technical specifications for alternative frontend embeddable solutions. Moreover, since 2023, organisers can no longer use any IOCS for the online collection of statements of support. However, the experiences acquired with the IOCS are indirectly relevant for this study because several of the risks and threats associated with the IOCS and reported in the implementing regulation are also related - the study identified - to the implementation of the embeddable solutions.

One of the organisers' claimed benefits of using the embeddable solution is that it would improve the users' journey in the online support of a citizens' initiative, because the citizen could stay within the same environment of the organisers' website. This study, however, has not collected primary data from EU citizens/ECI supporters that have previously used the IOCS and/or the COCS to corroborate these claims. Nonetheless, supporters are the ones who can really assess the user journey in the process of collection of statements of support. Citizens/Supporters provide a user journey assessment, which would help to verify some of the claims made by organisers during the interviews (e.g., that by using an embeddable solution the supporters would be more engaged and emotionally attracted by the campaigning website, that supporters are irritated to be redirected). DIGIT, however,

has provided the contractor with raw data from surveys compiled by ECI supporters in previous years. These surveys were launched contemporaneously to the collection of statements of support, which showed that supporters reported a high satisfaction rate with the use of the COCS that is based on a re-direct solution, referring citizens to the EC secure website where citizens can directly sign. Supporters' satisfaction indicates that the current COCS provides all the necessary means to EU citizens that decide to support an ECI. Furthermore, the respondent for *Stop Finning* stated that supporters' complaints in relation to the redirection option were very limited out of the total statements of support collected of about 1.1 million (*"We got this feedback, not hundreds of complaints, but we got them."*). The respondent for *Fur Free Europe* also confirmed that an initiative success is not related to the tool used for the support collection, but it relies on the quality of the campaign. These data, analysed together, indicate that an embeddable solution from a supporter perspective would not provide major benefits of what is offered with the current COCS solution. Furthermore, the auditor of the Luxembourg government, who from 2012 certified 42 online collection systems hosted by the European Commission, noticed that during the certification process, he did not receive complaints from organisers on this point. Yet, the above analysis is not based on a proper comparative assessment of what the supporters' journey and experience would be in using the COCS with the current redirection option versus an embeddable solution. In fact, while organisers have expressed their needs for an embeddable solution, it does not automatically follow that organisers' needs will be the same of supporters' needs. It may be that an embeddable solution, while meeting organisers' needs, will not have a meaningful impact on the supporters' journey in supporting an ECI. This analysis, however, will need to be addressed in a specific study.

2. Objective and Scope of the Study

Based on the necessity to address the problem defined above, the European Commission has mandated the PwC-Sopra Steria consortium to deliver a specific project with the objective to produce an independent study on technical solutions for organisers of European Citizens' Initiatives to smoothen the signing process of their initiative via their campaigning website, which are compliant with Regulation (EU) 2019/788 and the EU legal framework on Security and Data Protection, with estimated impacts from a security, operational management, budgetary and data protection perspective.

This study implies the evaluation of the possibility and feasibility of decentralising the frontend part of the COCS, which could be embedded in an external site under certain conditions. But also, to evaluate the impact/cost to have such an embeddable solution on an external site and make it interact with the COCS backend. Security, personal data and budget conditions shall be considered.

In order to achieve the above-mentioned objective, the scope of the study is to identify a technical solution that responds to the identified business needs of the organisers, while addressing the security, data protection and operational risks as well as management and budgetary impacts identified both on the side of the Commission and the organisers of the initiatives concerned.

The scope is reached by answering the key research questions, that will be addressed in this study:

Are there one or more embeddable solutions that the Commission can offer to ECI organisers that ensure security and personal data protection, which are compliant with the ECI Regulation? What are the estimated impacts from an operational management and budgetary perspective?

The study highlighted three embeddable technical solutions that can partially meet the needs of the ECI's organisers. In order to assess the technical options and provide recommendations to the European Commission, several steps (below) were followed:

1. List the embeddable technical solutions that can potentially meet the ECI stakeholders' business needs;
2. Provide a SWOT analysis of the technical solutions identified;
3. Contrast the outcomes of the SWOT with the ECI stakeholders' business needs;
4. Analyse the challenges of embeddable solutions;
5. Consider the impact of the solutions on the European Commission, the organisers and the Member States authorities involved;
6. Define other possible technical options (if any);
7. Produce the study with our recommendations.

3. Methodology: A Three-Phase Approach

The proposed methodology for this study comprises two major investigative phases, and one conclusive phase. These three phases are: I) Fact-Findings; II) Analysis of Results; III) Recommendations.

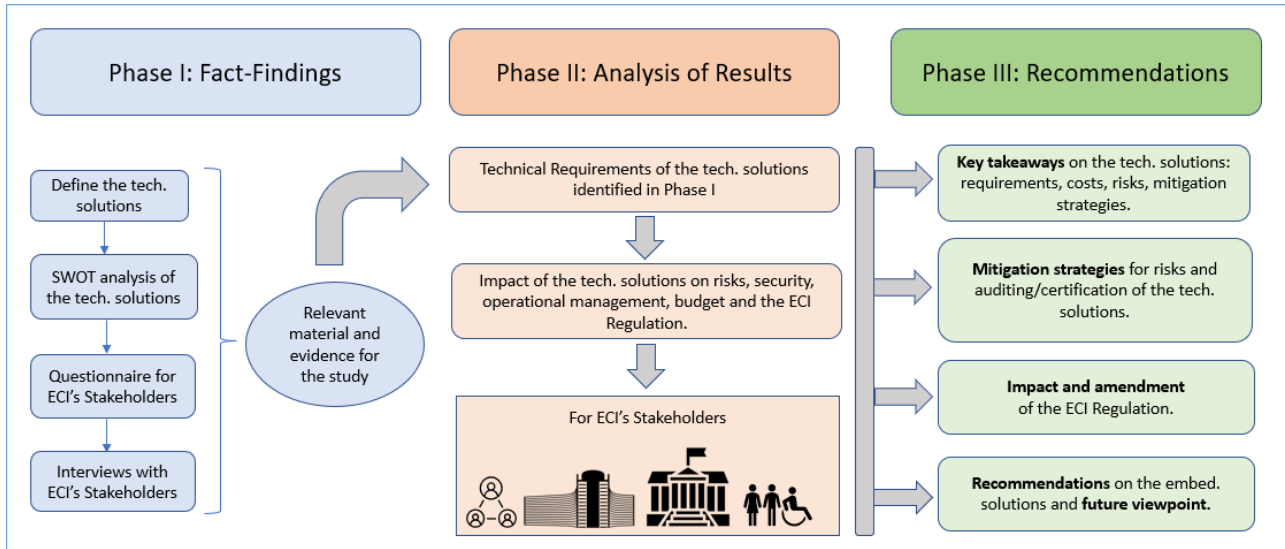


Figure 1: Study's Methodology

In Phase I, *fact-findings*, the contractor executed the data collection in three steps: 1) identify and define the technical solutions; 2) SWOT analysis of the technical solutions; 3) stakeholders' consultations with structured questionnaire and interviews. These consultations, aimed at gathering the ECI's organisers business needs, further complement the data presented in the SWOT analysis. After completion of Phase I, the contractor compared the list of the technical solutions proposed with the findings of the ECI's stakeholders' consultations.

In Phase II, *analysis of results*, the contractor presented and evaluated the data collected in Phase I. In this Phase, evaluation criteria were applied to all technical solutions proposed. In particular, the solutions are evaluated in detail for their functional and technical requirements, the opportunities, and risks that they present, as well as for their impact on costs, and operational management for ECI's stakeholders if they are eventually implemented. Further evaluation criteria are about evaluating the impact of the technical solutions on the current ECI Regulation. Finally, the contractor provides some ideas, guidelines and/or examples on how to improve the user experience of EU citizens, if the embeddable solutions are implemented.

In Phase III, *recommendations*, the contractor provided a full understanding of the key takeaways on the evaluation criteria established in Phase II. A future viewpoint on the scenarios for recommendation is fully developed to provide the European Commission with a clear answer to the key research questions.

Both Phase II and Phase III were developed after the conclusion of the stakeholders' consultations.

4. Phase I: Fact-Findings

The first phase of the study consists of three steps aimed at identifying the key fact-findings that provide for the final report. These steps are:

- Step I - Identify and define the technical solutions that could be embedded in the websites of the ECI's organisers. (Section 4.1)
- Step II - SWOT Analysis of the technical solutions. (Section 4.2)
- Step III - Stakeholders' consultations: Questionnaire and Interviews. (Section 4.3)

4.1. Step I - Identify and Define the Technical Solutions Proposed for the ECI's Organisers

This section focuses on the definition of the technical solutions identified.

The contractor, in a preliminary assessment, identified three possible technical solutions that can provide an answer to the research questions:

- 1)iframe + better UX of the COCS;
- 2)iframe + Micro Frontend Application (impact on COCS structure);
- 3)API Gateway + collection form (provided by the European Commission, ECI's organisers, or third parties).

Table 3 below lists and codifies the identified technical solutions and frame them within the study's objective and scope at chapter 2 above.

Table 3: List of technical solutions

Technical Solution code (TS)	Technical Solution Short Title	Description	Frame the Solution within the Study's Objective
TS01	iframe + better UX of the COCS	An in-line frame used to embed specific content from one page to another page.	Provide the possibility to visualize the whole EC COCS website of the initiative within the ECI's organisers' website.
TS02	iframe + Micro Frontend Application	Decomposing the European Commission COCS website into independent "microapps" working loosely together. This allows to load only the support forms within the ECI's organisers website via an iframe and not the whole EC COCS website.	Provide the possibility to visualise only the COCS support form within the ECI's organisers' website.
TS03	API Gateway + collection form (provided by the European Commission, ECI's organisers, or third parties).	Use of the existing EC's API Gateway together with a collection form implemented by the European Commission, a third party, or the ECI's organisers. This solution requires the creation of a Rest API with the necessary operations to be able to send the request to the server.	Provide the ECI's organisers with: <ol style="list-style-type: none"> 1. The possibility to set up their own collection forms and link them to the European Commission API Gateway or 2. Rely on a collection form created by the European Commission or a third party.

The first technical solution (**TS01**) identified is named "iframe" which should be accompanied by an improved user experience of the COCS.

An iframe is an in-line frame with an HTML structure that lets someone insert an HTML document into another HTML document and display it as a webpage. It is represented as an <iframe> tag. Iframes are commonly used to embed specific content like external ads, videos, tags, or other interactive elements into a page. It is supported by all major web browsers and is included in the

latest HTML5 specifications. Iframe has one major advantage that can be easily placed almost everywhere within a website.¹⁹

When the web browser encounters an iframe element, it creates a new HTML document environment to load the content within. It takes the code and renders it as its own website that is then put entirely within the parent browsing page. It is called an inline frame because to the user it is all one web page. It provides the ECI's organisers with an embeddable solution for their initiatives' websites to load the COCS within their own website. The solution prescribes the insertion of a button within the European Commission ECI's initiative website, where then the ECI's organisers can copy the iframe code and add it to their own website. This is a simple process.

The second technical solution (**TS02**) identified is named "iframe + Micro Frontend Application" which can also be accompanied by an improved user experience in the COCS.

The term Micro Frontends extends the concepts of micro services to the frontend world. The idea behind Micro Frontends is to think about a website or web app as a composition of features which are owned by independent teams. Each team has a distinct area of business or mission it cares about and specialises in. A team is cross functional and develops its features end-to-end, from database to user interface. However, this idea is not new. It has a lot in common with the Self-contained Systems concept.

Micro Frontend permits to decompose the COCS of the European Commission website into independent "microapps" working loosely together. This allows the sharing of the COCS support collection form through an iframe within the ECI's organisers websites. This is different from the solution TS01, where the whole EC COCS website is loaded within the iframe.

The third technical solution (**TS03**) identified is named "API Gateway + collection form (widget provided by the European Commission and/or external stakeholders (ECI's organisers, third parties)". An API gateway is an API management tool that sits between a client and a collection of backend services. An API gateway acts as a reverse proxy to accept all Application Programming Interface (API) calls, aggregate the various services required to fulfil them, and return the appropriate result. It is common for API gateways to handle common tasks that are used across a system of API services, such as user authentication, rate limiting, and statistics. It provides a single entry point for clients to access multiple backend services, and can perform a variety of functions such as routing requests, load balancing, authentication and authorization, request/response transformation, and caching.

API gateways are commonly used in microservices architecture where there are many small, independent services that need to be accessed by different clients. By using an API gateway, clients can access these services through a single endpoint, simplifying the client-side code and reducing the number of network connections required. Overall, an API gateway is a powerful tool that can help simplify the complexity of microservices architecture and improve the scalability, reliability, and security of distributed systems.

For this third technical solution, one of the options considered is that the European Commission sets up an API Gateway for the European Citizens' Initiative, which can be used together with a support collection widget/form developed by the European Commission, a third party, or the ECI's organisers themselves. If the API Gateway will not be available for the ECI, as an alternative the widget could be decentralised via web services, which also offer customisable opportunities. This solution requires the creation of a Rest API with the necessary operations to be able to send the request to the server.

This solution would provide the European Commission or the ECI's organisers with the possibility to create their own support collection form on their chosen website and then link it to the COCS backend where data would be transmitted. This latter point, however, raises concerns because organisers would be able to transfer data to another storage before the data reach the COCS backend on the European Commission servers.

¹⁹ Yuen, P.K. and Vincent Lau. (2003). *Practical Web Technologies*. Addison Wesley, p. 34.

4.2. Step II - SWOT Analysis of the Technical Solutions

A SWOT analysis is an analytical method which is used to identify and categorise significant positive factors (Strengths and Opportunities) and negative factors (Weaknesses and Threats) faced either in a particular arena, such as an organisation, or a territory, a region, a nation, or a city. In this specific study, a SWOT analysis provides an outlook into the positive and negative factors of the technical solutions identified. Further, a SWOT analysis provides preliminary material that is helpful for a subsequent and more in-depth analysis about whether a technical solution can solve or attempt to solve the stated problem. In other words, a SWOT analysis indicates at a preliminary stage which technical solution (one or more) responds to the identified business needs of the ECI's organisers, while addressing the security, data protection and operational risks as well as management and budgetary impacts identified for all stakeholders involved, including the European Commission, the ECI's organisers of the initiatives, and the Member States authorities concerned. By contrasting the technical solutions' positive and negative factors, and how they operate, the study can provide an eminent position and a contribution to the strategic planning process for future decisions in relation to the stated problem in Chapter 1 above. Strategic planning requires that the future pattern of actions to be taken by the European Commission should match strengths with opportunities, block and/or control threats and seek or at least attempt to overcome weaknesses.

In relation to the technical solution 1 (TS01), the below SWOT analysis was conducted:

Table 4: SWOT analysis of iframe solution - TS01

SWOT Analysis – Solution TS01: iframe + better UX of the COCS	
Positive	Negative
Strength	Weaknesses
<ul style="list-style-type: none"> • Easy to implement for the European Commission and the ECI's organisers. • Easy to maintain in the long term. • Minimum changes to COCS. 	<ul style="list-style-type: none"> • Solution presents security and data protection risks in the ECI's organisers' websites: • The ECI regulation today does not foresee an audit of the frontend part. • The boundaries of the collection system are not defined in the ECI regulation (the frontend part is not included). • Embedded iframe will require a better UX design of the original COCS to properly show the support form in the ECI's organisers' website (as the whole COCS page will be visible within the iframe). • Iframes may impact the performance.
Opportunities	Threats
<ul style="list-style-type: none"> • Provide an embedded solution to ECI's organisers for their websites with an improved UX for the support process. • It is recommended that the website is audited or certified. • Auditing of the website will require an amendment of the ECI's regulation. • Recommend updating to better define the boundaries of a collection system (including the frontend part) 	<ul style="list-style-type: none"> • Embeddable iframe on ECI's websites can be hacked (possible to implement malicious code to steal users' inputs/personal data). • iframe code can be replicated in any websites even outside the European Union. • With iframe injection is possible to have cross-site scripting attack. • Cross-Frame Scripting (XFS) combines Iframes with malicious JavaScript to steal data from users. • Clickjacking. • iframe Phishing. • Full list of risks is in Table 18 under section 5.2.5. below. • The EC will partially lose control on the Frontend part of the collection system.

In relation to the technical solution 2 (TS02), the below SWOT analysis was conducted:

Table 5: SWOT analysis of Iframe in Microfrontend solution - TS02

SWOT Analysis – Solution TS02: iframe + Micro Frontend Application (impact on COCS structure)	
Positive	Negative
Strength	Weaknesses
<ul style="list-style-type: none"> Decomposing the COCS of the European Commission website into independent “microapps” working loosely together. This allows to load only the support forms within the ECI’s organisers website via an iframe and not the whole EC COCS website. Micro Frontend application could implement ethical hacking, which is a process of detecting vulnerabilities in an application, system, or organization’s infrastructure that a hacker can use to exploit an individual or organization. 	<ul style="list-style-type: none"> Same weaknesses as solution TS01. Costly to implement for the European Commission. Maintaining the Micro Frontend application is demanding for the European Commission, if and when the system needs to be up to date with the latest technologies.
Opportunities	Threats
<ul style="list-style-type: none"> Same opportunities as solution TS01. Isolate application from EC servers (specifically the COCS support form) and provide an embeddable solution for ECI’s organisers’ websites. 	<ul style="list-style-type: none"> Same threats as solution TS01. Full list of risks is in Table 18 under section 5.2.5. below.

In relation to the technical solution 3 (TS03), the below SWOT analysis was conducted:

Table 6: SWOT analysis of API gateway solution - TS03

SWOT Analysis – Solution TS03: API Gateway + collection form (widget provided by the EC, the ECI’s organisers, or third parties).	
Positive	Negative
Strengths	Weaknesses
<ul style="list-style-type: none"> Centralize endpoint collection data. Data are standardised. EC can identify the requesting caller and restrict the use of its services only to the websites using the API gateway in association with IP filtering. 	<ul style="list-style-type: none"> Same weaknesses as solution TS01. Costly for ECI’s organisers if they want to implement the form/widget by themselves. It requires IT development expertise. (e.g. complexity to include the EU Captcha of the European Commission.) If the collection form is provided by the European Commission, may not work with all websites, and may not satisfy all the demand from the ECI’s campaigning websites. Additional operational costs for the European Commission to offer and operate such a solution (interaction with ECI’s organisers that runs those services, technical risks, reputational risk). The EC will have to implement an API Gateway (although the EC already has an API Gateway solution in place, this solution is currently not available in the Sensitive Non Classified environment where the ECI is located).

Opportunities	Threats
<ul style="list-style-type: none"> • Same opportunities as solution TS01. • Provide ECI’s organisers with the opportunity to have their own collection form and design. • ECI regulation should ask to explicitly audit the code to make sure that ECI's organisers do not store any personal data or ask for any additional personal data (ex. email, gender, religion, etc.) • Give the possibility to an external company to develop and propose an alternative to the COCS by proposing a collection form that will look different and may respond to the needs of the ECI's organisers. • For the EC to develop their own support collection form connected to the API gateway: <ul style="list-style-type: none"> a) the EC will bear the costs of developing the support collection form with less costs for ECI's organisers; b) This will limit risks. • Using API gateway + IP filtering will prevent that the support collection form is copied in other websites not audited/certified. 	<ul style="list-style-type: none"> • Embeddable iframe on ECI’s websites can be hacked (possible to implement malicious code to steal users inputs/personal data). • After certification/audit of the websites, ECI's organisers or hackers could modify the code of the support collection form by • For custom-made support collection form by ECI's organisers it is difficult to audit the code (ex. check if they store locally personal data, or if they collect more data than what is required by the collection process.) • inserting malicious code, without informing the EC and/or Member States authorities. • If the support collection form is developed by the ECI's organisers or a third party, when there is a problem with the support form, there could be a dispute of responsibility between the support collection form provider and the EC's backend services about who is responsible and for what (ex. unavailability, issues, etc.). This could affect the reputation of the EC and the whole ECI initiative and its process. • The EC will lose all control on the Frontend part of the collection system. • A solution equivalent to an IOCS could be developed by organisers outside the EC control and this solution could store personal data locally before transmitting them to the COCS. • Full list of risks is in Table 18 under section 5.2.5. below.

4.3. Step III - Stakeholders’ Consultations: Questionnaire and Interviews

This section presents an overview of the stakeholders involved in the European Citizens’ Initiative with description of their roles and a preliminary explanation of how an embeddable solution might impact them.

Figure 2 below graphically depicts the key stakeholders that rotate around the ECI’s ecosystem. These six main stakeholders are: the Secretariat General (European Commission), DG DIGIT (European Commission), the initiatives’ organisers, the Member States’ authorities, the ECI Campaign, and the EU citizens.



Figure 2: ECI's Stakeholders

An outline of the ECI stakeholders' role is provided in Table 7 below, together with a preliminary impact assessment of how an embeddable solution might affect each stakeholder.

Table 7: Stakeholders' Matrix and Preliminary Impact of an embeddable solution

Stakeholders	Role	Preliminary Impacts if an embeddable solution is implemented
Secretariat General	Business and Project Owner.	SG, in its role of project and business owner, can be impacted financially in first instance. But the impact would spread to the management of such new reality, the risks associated with the embeddable solutions, and for the amendment of the ECI Regulation. SG will need to align with DIGIT in relation to the new auditing scheme.
DIGIT	System Supplier including the Central Online Collection System.	DIGIT in its quality of system supplier will be on the frontline for the development of the embeddable solution. In addition, DIGIT would be impacted financially, including the associated costs for operation and management of the embeddable solution. DIGIT would also need to provide its technical inputs on the risks assessment of the embeddable solution and on the amendment of the ECI Regulation. DIGIT will face the consequences if a dispute arises in relation to any technical problems related to the deployment and functioning of the embeddable solution. DIGIT will need to set up the new auditing scheme together with SG.
Initiative Organisers	Set up the Initiative – They currently use the COCS with the redirection option to collect statement of support.	Organisers would have the opportunity to use the embeddable solutions on their campaigning websites. This will allow them to maintain the supporters' attention on their own website. Further, the UX of the signing process through their websites could be improved. They would also be impacted financially if they need to have someone with IT expertise to set up the embeddable solution.
Member State Authorities	They oversee certifying the initiatives' websites. This was a compulsory step under the IOCS system. They also verify the statements of support collected at national level.	Member States authorities are mostly concerned with risks linked to security and data protection. If an embeddable solution is implemented, they would most likely need to provide a certification to the initiative websites that will use such a solution.

Final Report

The ECI Campaign	Developed the OpenECI, a campaign-friendly independent software that before 31 December 2022 could be used to collect support under the Individual Online Collection System. From 1 January 2023, the OpenECI is not allowed by the ECI Regulation and cannot be used by organisers.	The ECI Campaign could benefit from the opportunity to use their previous experience. They will not be impacted financially, instead they could find a further opportunity if they are allowed to develop the embeddable solutions. The amended ECI Regulation would need to contemplate (or not) the possibility of a third-party development of an embeddable solution.
EU Citizens	EU citizens represent the potential pool of supporters for the initiative.	EU citizens represent the pool of supporters for the initiative. They are the final users of the COCS, and those who eventually sign via the embeddable solution if it will be implemented.

The contractor prepared a structured questionnaire for the collection of primary data from the ECI stakeholders. This questionnaire has been prepared with the aim to identify the opportunity to offer an embeddable solution considering the ECI's organisers business needs, and the EC' concerns for the security of the embeddable solution and the data protection risks, including operational management and costs associated with implementation. The questionnaire was submitted to four stakeholders that have provided specific inputs on the business and technical needs for a decentralised embeddable solution on campaigning websites. These stakeholders fall into the below categories:

- Organisers of citizens' initiatives (Fur Free Europe and Stop Finning);
- National administrations entrusted with the certification authority (CTIE Luxembourg Government);
- Providers of Open ECI software for the Individual Online Collection Systems (The ECI Campaign).

The structured questionnaire was not submitted to the Secretariat General and DIGIT, because this is an independent report by a contractor engaged by these two stakeholders.

For the EU citizens, instead, it was not in the scope of the project to include them within the qualitative research process. Many of them would not have the required technical skills to discuss about an embeddable solution. Their concerns would mostly be based on the user experience part, but UX has only a limited scope in this study.

The contractor ensured the comprehensiveness of the questionnaire and the coverage of all topics relevant to understand the organisers business needs. In preparing the questionnaire the contractor has taken into consideration the limited technical knowledge that some of the ECI's organisers may have. Therefore, at a first glance, the questionnaire has the scope to collect information from a business perspective and to understand the organisers' needs to have an embeddable solution on their website for the collection of statements of support.

The questionnaire is mostly based on open-ended questions, which give the organisers the complete freedom to provide the answers they want in the manner they want.

The questionnaire (Annex III) consists of six main questions, four of which are open-ended questions and two are closed questions with the possibility to provide further contribution upon choosing the option listed.

The questionnaire begins with a general question about why it is important for organisers to have an embeddable solution on their initiative websites. It continues asking the ECI's organisers if the European Commission should offer an embeddable solution for the frontend part of the support collection process. Further, the questionnaire asks the organisers to provide their feedback on the technical solutions identified by the contractor in the SWOT analysis, and to propose other technical solutions according to their knowledge and needs. The last part of the questionnaire asks the ECI's organisers to comment on the risks associated with an embeddable solution, and the impact that the solution could have on the initiative.

The respondents were contacted via email with the support of DIGIT and the Secretariat General of the EC. They have been asked to review the questionnaire and when possible, to provide an answer to the questions in writing. The questionnaire was also supplemented with interviews that were set up using an online platform. The interviews had the scope to discuss the questionnaire, explain it if

necessary, and to go more in detail of the answers provided. The interviews also provided an opportunity to discuss new topics raised with the questionnaire.

Four stakeholders were interviewed. Namely, one auditor of a Member State authority (Centre des technologies de l'information de l'État du Luxembourg), two ECI's organisers (Fur Free Europe, Stop Finning), and one civil society organisation (the ECI Campaign). Fur Free Europe utilised an individual online collection system (IOCS) provided by the ECI Campaign, while Stop Finning used the COCS. Both initiatives were successful in collecting over 1 million statements of support.

In relation to the ECI Campaign, we contacted them for a second interview, as we were interested in listening how they secured their support collection software (the Open ECI) and in particular the frontend part of their system. We were willing to hear about the OpenECI terms of services, and how they controlled the security of the support collection form which in the case of one initiative, we found out during the interview, was decentralised on many uncertified websites. However, the ECI Campaign representatives did not accept our invite for a second interview. We have also sent to them extra written questions, but we did not receive an answer.

In terms of sampling technique, the contractor relied on the *purposive sampling*. This is a *non-probability sampling*, which is usually considered biased since no randomisation is used in obtaining the sample of the stakeholders that will be interviewed or to whom the questionnaire will be submitted. However, in this project, the number of stakeholders that possess the trait of interest for the study, and that can provide the necessary inputs, is limited. Therefore, purposive sampling was deemed the only viable sampling technique in obtaining information from a very specific group of stakeholders.²⁰ All respondents for the questionnaire were chosen because they play a particular and important purpose in the ECI eco-system, and they have direct knowledge and experience with the online collection systems.

²⁰ Daniel, Johnnie. (2012). *Sampling Essentials: Practical Guidelines for Making Sampling Choices*. SAGE Publications, pp 87-92.

5. Phase II: Analysis of Results

The second phase of the methodology present the results of the interviews conducted with the ECI's stakeholders. In this Phase, evaluation criteria are applied to all technical solutions proposed. In particular, the solutions are evaluated in detail for their functional and technical requirements, the opportunities and risks that they present, as well as for their impact on costs, operational management for ECI's stakeholders if they are eventually implemented. Further evaluation criteria are about evaluating the impact of the technical solutions on the current ECI Regulation.

5.1. Presentation and Analysis of the Data Collected in Phase I

After the conclusion of the four interviews with the CTIE Luxembourg, two ECI's organisers (Fur Free Europe, Stop Finning), and the civil society organisation (the ECI Campaign), the contractor provided written transcripts²¹ of the interviews to each stakeholder. All stakeholders had the opportunity to review the content and approve it.

Table 8: Stakeholders' Summary of Interviews Dates and Approvals

Organisation / Entity	Key Person	Date of Consultation	Relevance	Approval of Answers' Minutes	Approval to have their names published in this report
CTIE Luxembourg	Mr Lionel Antunes	10/02/2023	National Authority entrusted with the authority to certify ECI's organisers collection system.	22/03/2023 (yes, via email)	22/03/2023 (yes, via email)
Fur Free Europe	Ms Elise Fleury	13/02/2023	Successful ECI's organisers using the Individual Online Collection System. These organisers also provided information on the COCS as they were co-organisers of the initiative <i>Save Cruelty Free Cosmetics</i> .	20/03/2023 (yes, via email)	20/03/2023 (yes, via email)
The ECI Campaign	Mr Carsten Berg (Director), Mr Daniel Pentzlin-Kordecki (Strategy Advisor), Mr Xavier Dutoit (IT Engineer)	14/02/2023	Since 2002, the ECI Campaign has been involved in the ECI. It is a grassroots coalition of democracy advocates that implemented the Open ECI software to support organisers to set up an Individual Online Collection Systems.	20/04/2023 (yes, via email)	20/04/2023 (yes, via email)
Stop Finning – Stop the Trade	Dr Nils Kluger	17/02/2023	Successful ECI's organisers using the Central Online Collection System.	28/03/2023 (yes, via email)	28/03/2023 (yes, via email)

The content of the interview was provided in an edited transcription. The edited transcript was chosen because the study may be publicly available and will target a wider audience. The edited transcript is cleaned up and edited to increase readability and clarity.

The results of the interviews were coded into qualitative coding. Qualitative coding is a process of systematically categorising extracts of transcripts from in-depth interviews in order to find themes and patterns. Coding the qualitative data makes the analysis more systematic and rigorous. It also provides transparency and reflexivity for the respondents, the authors and even the readers.

²¹ Full interviews' transcripts are attached to this report at Annex IV.

Qualitative coding enables to find insights that are truly representative of the business needs of the organisers to have an embeddable solution. The approach followed to qualitative coding is the inductive coding, which is a ground-up approach where the researcher derives the codes from the data. There are no preconceived notions of what the codes should be, but the researcher allows the narrative or theory to emerge from the raw data itself, find recurring patterns and themes.²² From the thematic analysis of the transcripts, certain excerpts point to the same underlying idea or meaning, these patterns and themes were identified and coded with a unifying code. The below tables report the coding identified in support of having the embeddable solution and in opposition to the embeddable solution.

Table 9: Inductive Coding of organisers interviews

Why organisers want an embeddable solution?		
Facilitate: the harvesting of supporters' emails; The signing up for their newsletter and for future activities	Better engage and maintain the supporters on the organisers' campaigning website	Improve the chances to collect more financial donations (Supporters are potential financial donors, and they provide a return on the initial investment.)
Would provide the possibility to customise the collection form.	To collect analytics and extract information on the support to target the supporters	Could be decentralised on third-parties' websites, offering a wider impact.

Table 10: Inductive Coding of auditor's interview

Why auditors are against an embeddable solution?		
Increases security concerns and risks of data breach.	Risks outweigh the potential benefits for organisers and supporters.	Reopens a debate closed with the phasing out of the IOCS.
Has high risks similar to the previous IOCS.	The EC would lose control of the collection process.	Concerned that organisers could misuse the solution to collect more personal data (e.g. emails, etc)
An embeddable solution is not a general need.	It is not critical to the EC's instrument.	The current COCS meets all needs, and it is secure, because it is bound by the IT security policies of the EC.

5.1.1. Results' Summary: Organisers "Fur Free Europe" - "Stop Finning", and the ECI Campaign

The answers provided by the two organisers and the civil society organisation can be summed up in a general business view that an embeddable solution should be offered by the European Commission. The two organisers interviewed also claimed that an embeddable solution would facilitate the harvesting of supporters' emails, also for signing up for their newsletter and for future activities. An embeddable solution would better engage and maintain the supporters on the organisers' campaigning website and improve the chances to collect more financial donations. Supporters are potential financial donors, and they provide a return on the initial investment. It was also claimed that an embeddable solution would provide the possibility to customise the collection form, and to collect analytics and extract information on the statements of support to target the supporters. An embeddable solution also would allow to be decentralised on third parties' websites, offering a wider impact.

Fur Free Europe organisers assert that their success was not determined by using an individual online collection system. They said that the support collection form probably did not make a difference in the number of support collected. Success depends more on having a strong campaign, than the tool.

²² Saldana, Johnny, (2015). *The Coding Manual for Qualitative Researchers*, 3rd ed. Arizona State University, USA: Sage Publications.

What however an embeddable solution would offer is to keep the attention of the supporters on the campaigning websites, would increase the ability of the organisers to grow their supporters' engagements, which in turn would promote a stronger focused campaign and a return on the initial investment.

In terms of risks associated with the use of an individual collection system, organisers for *Fur Free Europe* clarified that they were not worried about risks of data breach as they trusted the OpenECI software provided at a reasonable cost from the ECI Campaign. They trusted the tool and the fact that the OpenECI was certified by the German certifying Authority (BSI, certification body). Fur Free Europe's organisers embedded the OpenECI support collection form in 30 websites of partners organisations. This contributed to their success in collecting statements of support, however, apparently, they did not realise the risks associated in embedding the OpenECI support collection form in many uncertified websites. Fur Free Europe's organisers claimed that they knew the rules, which legally oblige them to follow a certain procedure. These organisers educated supporters on the data collection process, and they made official video of the ECI steps. They developed community management, and they said to the people that it was safe to provide their support via the OpenECI software.

The organisers of *Stop Finning* have sustained that organisers can handle risks, as many NGOs can handle personal data in huge numbers. Supporters want more information on the initiative, and they want to directly sign on the ECI campaign website, not on the EC external website. The organisers of *Stop Finning* stated that as organisers they have the problem of explaining and promoting the campaign (considering that only 2% of European citizens know the ECI), and in addition they have to explain that with the COCS the statements of support are stored in an external website run by the EC. They see this latter point as a drawback of installing an embeddable solution if the personal data are still stored by the EC. They suggested to keep the embeddable solutions as easy as possible for organisers and supporters.

In terms of risks, *Stop Finning* explained that their campaigning site crashed when they reached hundreds of thousands of visits in one day. With the implementation of an embeddable solution, the EC should provide feedback to organisers to have a scalable contract for their hosting services to sustain waves of statements of support. The scope of the ECI is to bring everybody to vote. With an embeddable solution all process for the supporters becomes streamlined, but with the COCS users have to do one more click to vote.

5.1.2. Results' Summary: Auditor of the CTIE of the Luxembourg Government

The auditor of the CTIE of the Luxembourg Government was interviewed on 10 February 2023 and provided answers to the questionnaire as an external stakeholder that has been supervising the certification of online collection systems and validation of statements of support since 2012, and who has therefore been in contact with organisers of European Citizens' Initiatives (ECI). During the whole duration of the first ECI Regulation, the CTIE has certified 42 online Collection Systems, reviewed the security plans and risk assessments submitted by 42 groups of ECI's organisers, and verified the statements of support for 14 ECIs. We have reasons to believe that the view expressed by the Luxembourg authority may be shared by the audit authorities of other Member States.

The CTIE auditor expressed his concerns about the implementation of an embeddable solution by the EC, because of the security risks associated with the embeddable solutions. These risks, in his opinion, outweigh the potential benefits for organisers and supporters. He drew some parallels with the IOCS, which at the time raised with him similar concerns about the handling of the personal data when organisers relied on such individual collection system. He was also concerned about the possibilities for organisers to collect and store personal data through this individual online collection system, (including extra data like email addresses), allowing them to constitute a repository of these data that could be reused at a later stage or even misused, which would be difficult to control.

He also commented that in part, the current study reopens a debate closed when the ECI Regulation phased out the IOCS and centralised the collection of statements of support on the European Commission system. The auditor reported that the technical solutions presented by the contractor represent a modern approach, however, he again stressed his concerns for the risks associated with such solutions. In particular, he reported that the API Gateway solution offers the least control on the data collection before data reach the EC storage. The API Gateway solution, in his view, will transform the current Collection system in a simple transmission API losing all the benefits of the security checks performed by the COCS when collecting personal data. There are less technical constraints, if the EC provides an Iframe (TS01 and TS02), although also the iframe presents high risks of data breach. He asserted that an embeddable solution has never been identified as a general need for the organisers nor critical to the ECI's instrument. The current COCS, in his view, meets all needs, and it is secure; it is also bound by the IT security policies of the EC.

The auditor stressed that if an embeddable solution is implemented, it is necessary to establish a set of security requirements for the system used by the organisers. Auditing of this system would be needed, potentially done by national authorities; however, if the embeddable solution is embedded in many websites, the national authorities may not have the capability of auditing/certifying all these campaigning sites.

5.2. Solutions Functional and Technical Requirements

This section explains more in details the technical solutions functional²³ and technical²⁴ requirements. This section also introduces and review the technologies that will be used for the development of the frontend part of each of the three solutions. In terms of technical implementation, all solutions identified are viable, and they can be implemented for the frontend part of the COCS. All solutions identified would only meet partially the organisers needs.

5.2.1. Definitions of the Technologies for the Implementation of the Embeddable Solutions

The key technologies that are relevant to the development of the embeddable solutions identified are: the **Hypertext Markup Language (HTML)**, the **Cascading Style Sheets (CSS)**, the **iframe**, **Angular**, **Node js**, **Node Package Manager**.

The **HTML** and the **CSS** are two of the core technologies for building Web pages. HTML provides the structure of the page, CSS the (visual and aural) layout, for a variety of devices. Along with graphics and scripting, HTML and CSS are the basis of building Web pages and Web Applications.²⁵

An **iframe** is a HTML webpage that is embedded inside another webpage on a website, allowing for the inclusion of content from external sources, such as advertising, on webpages. On a general term, an iframe HTML element represents a nested browsing context, embedding another HTML page into the current one.²⁶

Angular²⁷ is a platform and framework for building single-page client applications using HTML and TypeScript. Angular is written in TypeScript. It implements core and optional functionality as a set of TypeScript libraries that have to be imported into the applications.

The architecture of an Angular application relies on certain fundamental concepts. The basic building blocks of the Angular framework are Angular components that are organized into NgModules.

²³ Functional requirements refer to what the embeddable solution is supposed to do (e.g. showcase the signature collection form within the campaign website, without the current redirection option.)

²⁴ Technical requirements refer to how the embeddable solution is built (which language, which standards, etc.)

²⁵ W3C. "HTML & CSS". Accessed on 22 February 2023. <https://www.w3.org/standards/webdesign/htmlcss>

²⁶ Mozilla. "<iframe>: the inline frame element". Accessed on 23 February 2023. <https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe>

²⁷ Angular. "Introduction to Angular concepts". Accessed on 14 March 2023. <https://angular.io/guide/architecture>

NgModules collect related code into functional sets; an Angular application is defined by a set of NgModules. An application always has at least a root module that enables bootstrapping, and typically has many more feature modules:

- Components define views, which are sets of screen elements that Angular can choose among and modify according to the program logic and data.
- Components use services, which provide specific functionality not directly related to views. Service providers can be injected into components as dependencies, making the code modular, reusable, and efficient.
- Modules, components and services are classes that use decorators. These decorators mark their type and provide metadata that tells Angular how to use them.
- The metadata for a component class associates it with a template that defines a view. A template combines ordinary HTML with Angular directives and binding markup that allow Angular to modify the HTML before rendering it for display.
- The metadata for a service class provides the information Angular needs to make it available to components through dependency injection (DI)

Node js²⁸ is an open source, cross-platform runtime environment for developing server-side and networking applications. Node js applications are written in JavaScript, and can be run within the Node.js runtime on several operating systems.

Node Package Manager²⁹ (**NPM**) is the world's largest software registry. Open-source developers from every continent use npm to share and borrow packages, and many organizations use npm to manage private development as well.

5.2.2. Technical Solutions: Functional and Technical requirements

5.2.2.1. TS01 (IFRAME) DESCRIPTION

The solution consists of implementing a component in Angular that is a button that shows the code of the iframe with which the organisers can have a simple way to add it to their web pages.

The solution can be divided into two parts. On the one hand, the commission must develop a component in Angular that would consist of a button that, when clicked by the organizer, would show the iframe code. This code is the one that the organizer must copy and add to the section of his web page where the initiative is located. In this way, the COCS would be embedded in the web page of the organisers.

The method described is easy to implement both for the European Commission and for the organisers, however, it is critical to always bear in mind the risks inherent in the development of the solution. The figure below shows how the iframe solution (TS01) will look like.

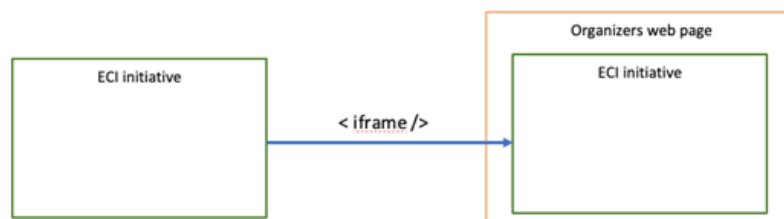


Figure 3: iframe solution (TS01)

²⁸ Tutorialspoint. "Node.js – Introduction". https://www.tutorialspoint.com/nodejs/nodejs_introduction.htm

²⁹ NpmDocs. "About npm". <https://docs.npmjs.com/about-npm>

How an iframe is implemented

	<p>As can be seen in the image, the development idea of the iframe is to add a "Share" button to the initiative created in the European Commission initiative website.</p>
	<p>The button will provide the user with the iframe code to embed in their web page. This piece of code will be configured with attributes to be set in organizer's web pages as simple as possible. When the user clicks on the button a modal window opens with the piece of code from the iframe</p>
	<p>The image shows how the embedded content would look like on the organiser's website.</p>

Iframe Whitelist

An iframe whitelist is a list of approved website domains that are allowed to display embedded content within an iframe on a particular website. An iframe is an HTML element that allows another webpage to be embedded within the current webpage.

To prevent security risks such as clickjacking attacks, website owners may choose to implement an iframe whitelist to limit the sources of content that can be displayed within an iframe on their website. By specifying a list of approved domains, the website owner can ensure that only trusted content is displayed within an iframe, and prevent malicious content from being displayed.

However, the remote deactivation of the iframe is not possible from a technical point of view, what is recommended in these cases is that from the server where the initiative is hosted, a whitelist is created which manages the web pages that can display the iframe. It is about configuring the server of the initiative on the EC servers. The EC servers must be configured to allow these external websites to iframe the EC initiative form, in order to do that, it can be used the whitelist. If in the whitelist there is no website indicated, this will prevent any external site to iframe the specific ECI page hosted on the EC servers.

The idea of making a whitelist with the authorized IP addresses is focused above all on the iframe solution in Micro Frontend, since in this way the form component is detached and added as an application on a server, in this way it can be selected through the whitelist which IP addresses can access the form, both the organisers and the public page of the initiative.

The form application can only be accessible from the servers that are added to the whitelist and thus prevent unknown pages from embedding the solution.

The initiative page to which users are redirected to sign cannot have the whitelist integrated as it is a public page.

The European Commission has to do a whitelist (set up a code and configure it) according to their infrastructure on the EC server.

5.2.2.2. TS02 (IFRAME + MICROFRONTEND) – DESCRIPTION

The solution consists of implementing a web application hosted on the servers of the European Commission based on the development of an angular form-type component. The data collected by this form will be sent to the COCS directly, thus preventing the collection of data individually.

Once this microfrontend is developed, it can be shared with the organisers through an iframe in the same way as in first iframe solution (**TS01**), with the difference that instead of embedding the entire web page in the organisers' page, the part of the form would simply be shared, minimizing thus the impact on the user experience (UX) of the organisers' page.

The described solution would imply a cost of development by the European Commission since the web application of the form (microfrontend) should be developed and, on the other hand, add as in the first iframe solution (TS01), a button in the initiative so that the organisers can add the form to the web pages. In this way it is possible to connect the statements of support collected on the organisers' website with the COCS. The figure below shows how the iframe solution with Micro Frontend (TS02) will look like.

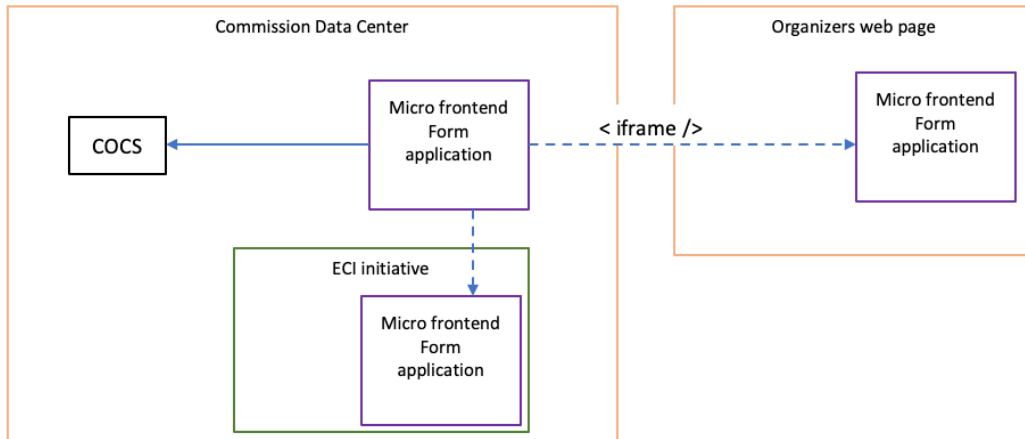


Figure 4: iframe solution in Micro Frontend (TS02)

5.2.2.3. TS03 (API GATEWAY) – DESCRIPTION

The solution is to create a Node js package that contains a library with the form component created in Angular. This package will be hosted on the European Commission's server and will be private, so it will be shared with the organisers individually. The form will be in charge of sending the data collected to the COCS through an API gateway that will serve as a communication tunnel between the form and the information collection system.

The solution described involves, on the part of the European Commission, implementing the Node js package with the library which contains the form that will be used to collect the information, and which will be implemented both on the Commission's own website initiatives and on the website of the organisers.

On the part of the organisers, the library created by the European Commission must be implemented on their website, for this they must have sufficient technical knowledge to add the form. The figure below shows how the API Gateway solution (TS03) will look like.

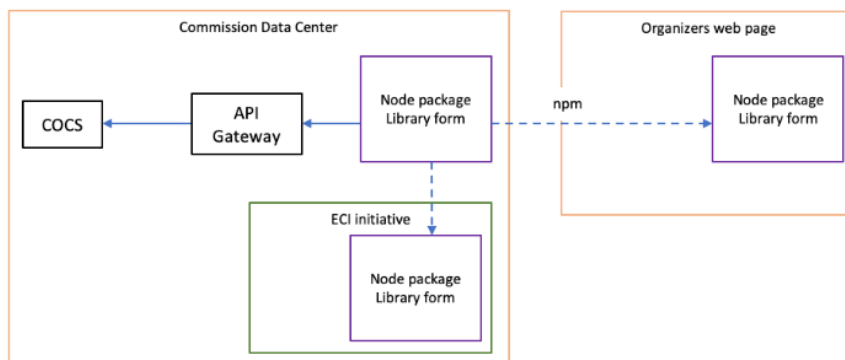


Figure 5: API Gateway solution (TS03)

5.2.3. Operational Management, Auditing, Implementation and Maintenance Costs of the Technical Solutions

This chapter assesses the technical solutions identified for their impacts on operational management, and costs associated with implementation and maintenance. Operational management is based on the impact on the EC internal team to run the embeddable solution, and the profiles needed. It also considers the security plan and the auditing of the embeddable solution. In term of costs associated

with the implementation and maintenance, this chapter assesses costs for the EC and the organisers. In particular, the estimated costs for implementation (development for the EC and integration for the organisers) of the embeddable solution are provided for up to 3 campaign websites. Maintenance estimated costs are also provided for up to 3 campaign websites on a yearly basis. However, for the auditing of the embeddable solution estimated costs are provided for each campaign website and for each initiative. The limitation of the estimated costs for implementation and maintenance to 3 campaign websites was proposed to meet the organisers' needs to decentralise the embeddable solution on more than 1 campaign website, while limiting the costs of the auditing and maintenance, and reducing the exposure to security and data protection risks.

In terms of the linear increase of the estimated costs if the embeddable solution would be decentralised on more than 3 campaign websites, it follows the below:

- For the auditing costs, there is a linear increase, because each campaign website where the embeddable solution is decentralised must be audited as each campaign website will carry security and data protection risks;
- For maintenance costs, there is a linear increase, which is due to the fact that a budget should be allocated for unpredictable situations. In fact, it is not easy to foresee all possible problems/issues/risks in advance and for many campaign websites (e.g., unavailability, responsibility, campaigning sites crash, malfunctioning of the embeddable solution on specific campaign websites, etc.) because there is no clear information about the systems/servers where the organisers will decentralise the embeddable solution, similarly there is no information about the organisers' technical expertise;
- For implementation costs (development and integration), these are mostly one-off costs considering up to 3 campaign websites where the embeddable solution is decentralised. However, if the organisers will integrate the embeddable solutions on more than 3 websites, this in principle will be a repetitive process and would not cost much more. The difficulty and costs are mostly to integrate the embeddable solution the first time. Similarly, the EC can develop the embeddable solution with one-off major costs (first time development), and then some minor costs when the solution is offered to different organisers on different campaign websites.

The major burden for implementation of the embeddable solution beyond 3 campaign websites will be for the auditing and maintenance that will need to be set up for all campaign websites where the embeddable solution is decentralised.

5.2.3.1. OPERATIONAL MANAGEMENT

Operational management impacts the European Commission in terms of the internal team required to implement and maintain the embeddable solution, of the security management associated with the solutions including the necessary auditing of all websites where the embeddable solution is decentralised. Detailed estimates of costs³⁰ are quantified under the following section.

Table 11 below recaps the major areas of impact in operational management.

Table 11: Operational Management

Technical Solutions	Iframe + better UX (TS01)	iframe + Micro frontend (TS02)	API Gateway + form (TS03)
Operations (internal team involved and profiles)	medium	medium-high	high
Security Plan (for the embeddable solution)	Set up by the EC on a yearly basis and for their own system	Set up by the EC on a yearly basis and for their own system	2 security plans: 1 set up by the EC, and 1 set up by the organisers for the frontend part.
Compliance review of audit requirements (Risks, Security, Regulatory per each campaign website)	Yes; audit twice during the collection period. (Once at the beginning and once after 6 months).	Yes; regularly required during the collection process (beginning, then every 4 months until conclusion of collection)	Yes; regularly required during the collection process (beginning, then every 4 months until conclusion of collection)
Complexity of auditing the code (IT solution embedded in campaign site)	low	medium	High

³⁰ Estimate is based on an average rate of a resource of €650 per workday. This rate is only an estimate considering lower and higher rates of the profiles involved from a private company perspective. Real cost for the EC will depend on the specific framework contract used for the implementation and maintenance, if external resources will be used.

A major burden for the operational management would occur in case the embeddable solution will not properly work on the organisers' campaigning site. For example, in the specific case of the API Gateway solution, if the support collection form is developed by the ECI's organisers or a third party, there could be a dispute of responsibility between the support collection form provider and the EC's backend services about who is responsible and for what (ex. unavailability, responsibility, campaigning sites crash, malfunctioning of the embeddable solution on specific campaign websites, etc.) This scenario could become a reality if the organisers' campaigning websites would crash because of the massive visitors' volume. Similarly, it could happen that the EC develops the support collection form, but would face dispute deriving from the poor performances of the hosting campaigning site, especially in case of massive visitors' volume. The costs of such a scenario are difficult to quantify. However, the European Commission should take into consideration the possible extra burden on its internal team in case of a dispute arising on the malfunctioning of the embeddable solution on the campaigning sites.

In terms of risk and security assessment and auditing of the organisers campaigning websites. The EC will have to produce a yearly security plan (which include a risk assessment) specific for the embeddable solution. For the embeddable solution using the API Gateway, the organisers will need to set up their own security plan. The security plan will need to be regularly updated and every time a new risk arises. Organisers should elect a competent data protection and security officer that will cooperate with the EC to safeguard the security of the collection process, and the personal data of EU citizens. Further, the European Commission will need to set up an auditing of the campaigning websites where the embeddable solution will be located. This is not an easy task, as the EC would need to set up an internal team or to outsource this audit mechanisms, because the current ECI Regulation does not foresee a certification process with the Member State authority. The auditing would largely impact the whole operational management, as it would need to be done for each initiative that would choose to deploy an embeddable solution. The auditor will need to check the security of the campaign website requirements, the security of the embeddable solution, and that the organisers will not misuse the embeddable solution. Then, the auditor will prepare a short report for the European Commission.

For the first iframe solution, the auditing will be simplified, and can be done twice during the whole collection process. For the second iframe solution, and the API Gateway solution, the EC (Member States, or a third party) should regularly audit the embeddable solution on any campaigning websites, every 4 months during the 12-month collection process. The first audit of the embeddable solution should be completed before starting the collection of statements of support. The cost of auditing, if outsourced to a private company, would require a security expert to work an average of 5 working days per single audit and per each campaign website (this work is estimated at €3,250). In addition, there are the initial costs of the auditing (or the certification) for the embeddable solution before starting the collection of statements of support, which are estimated at €10,000 (one-off costs). Considering the high risks associated with the API Gateway solution, an audit of the code of this embeddable solution is also important, this kind of audit however is very complex and costly. We estimate that each time that the auditing of the code is necessary it would cost an extra 10 workdays (estimated costs at €6,500). Table 12 below summarises the costs of auditing any of the embeddable solutions presented in the report. These costs should be afforded either by the European Commission or the organisers.

Table 12: Costs for the Auditing and the Certification of embeddable solution

Type of Control	Time	Costs	Impacts of Costs
Initial Auditing/Certification	Before Starting Collection	€ 10,000	(one-off costs for one website/initiative)
Auditing (Regular)	Every 4 months / 3 times per year	€ 3,250	(costs per one audit & for one website/initiative)
Code auditing for API Gateway	on ad-hoc basis	€ 6,500	(costs per each code auditing, per one website/initiative)

However, an audit of the campaigning websites should be limited to a small number of campaigning sites (max 3), first because auditing many websites will be excessively costly for the European Commission if outsourcing is required, second even if Member States are involved, they already stated in interviews that they have limited capacity to conduct a detailed auditing of the organisers campaigning website. Organisers needs to have a secure process and their own security plan in place, especially for the API Gateway solution. They will need to follow several security recommendations that have to be applied in the webpage development and the hosting servers. The EC should prepare in advance this security plan with specific recommendations, which can be added to the joint agreement with a template checklist of the security aspect for the hosting site that organisers have to comply with.

5.2.3.2. TECHNICAL SOLUTIONS: IMPLEMENTATION AND MAINTENANCE COSTS

The three solutions identified impact differently on the difficulty and the costs of implementation and long-term maintenance.

The implementation phase considers the development of the embeddable solution, which is an effort and a cost afforded by the European Commission, and the integration costs of the solution within the organisers' campaigning websites. This latter cost is for the organisers to afford. Maintenance costs are costs mostly afforded by the European Commission to update and maintain the embeddable solution. When a new update is available this will need to be integrated in the campaigning websites and it will generate a cost also for organisers. Maintenance costs also include the interaction between the European Commission and the organisers during the 12-month collection period.

The first iframe solution is easy to implement for the EC and the organisers. In terms of effort, it is medium-costly for the EC and low for organisers. The second iframe solution has a medium-high difficulty of implementation for the European Commission, while it will be relatively easy for the organisers to implement in their campaigning websites. In terms of costs, the second iframe solution, is high-costly for the European Commission, and relatively low for organisers. The API Gateway solution, instead, is hard to implement for both the EC and the organisers, it is also high-costly for the EC and the organisers.

Long term maintenance for the embeddable solutions also requires efforts on both the EC and the organisers. The first iframe solution is easy to maintain for both the EC and the organisers, and it requires low effort of maintenance. The second iframe solution has a medium difficulty to maintain for the EC, and requires a medium effort, while it is easy to maintain for the organisers and has relatively low effort on them. The API Gateway solution, instead, present very high effort, and it is hard to maintain for both the EC and the organisers.

The below table summarises the data presented above.

Table 13: Costs (effort) of Implementation and Maintenance

Technical Solutions	Iframe + better UX (TS01)	Iframe + Micro frontend (TS02)	API Gateway + form (TS03)
Implementation difficulty for EC	low	medium-high	high
Implementation effort for EC	medium	high	high
Implementation difficulty for organisers	low	low	high
Implementation effort for organisers	low	low	high
Long term maintenance difficulty EC	low	medium	high
Long term maintenance effort EC	low	medium	high
Long term maintenance difficulty organisers	low	low	high
Long term maintenance effort organisers	low	low	high

In terms of estimated costs for the implementation (both for the development by the EC and the integration of the organisers of the embeddable solution), these estimates are provided for up to 3 campaign websites.

For the development of the iframe solution (TS01), an effort of between 60 and 90 workdays has been estimated. An IT architect will be necessary to control the technical part of the tasks and a developer to execute the tasks to be carried out. It is estimated that the development will cost between €39,000 and €58,500.

For the development of the iframe + microfrontend (TS02) solution, an effort of between 180 to 240 days has been estimated. In this solution, it will be necessary to create an application and its subsequent implementation, which will require an IT architect to control the technical part of the tasks, code review and support, two developers to execute the tasks at carry out and the participation of a design person to improve the user experience. In addition, the configuration of the work environment and the specific definition of tasks will be necessary. It is estimated that the development of this second iframe solution will cost between €117,000 and €156,000.

For the development of the API Gateway solution (TS03), an effort of between 240 to 300 workdays has been estimated. This solution is the longest one since it requires modification of the existing data collection system and creation of the node library and putting it into production. In this solution, it will be necessary to create an application and its subsequent implementation, which will require an IT architect to control the technical part of the tasks, code review and support, two developers for the frontend part and one developer for the backend part for the development of the tasks to be carried out and the participation of a designer to improve the user experience. In addition, it will be necessary to configure both work environments and the specific definition of tasks in both parts, both frontend and backend. It is estimated that the development of this second iframe solution will cost between €156,000 and €195,000.

The workload to integrate the embeddable solution in the campaign websites would require specific effort depending on the solution implemented.

For the organisers, the effort of integrating the iframe solutions (TS01 and TS02) will be approximately 15 workdays for each solution (estimated costs of €9,750 each), and it consists of adding the line of code with the iframe in the organisers' website. This estimate considers that not all the organisers have the technical knowledge required. The estimate of 15 workdays is a guideline considering the worst-case scenario. The implementation time will depend on how the web page of each organiser is set up and its environment. The organisers will need to have some IT knowledge for the integration of the iframe, and if they do not have it, they may need a developer to integrate the iframe solutions on their campaigning website.

As for the API Gateway solution (TS03), the integration requires an effort for organisers that can range from 30 to 90 workdays (estimated costs between €19,500 and €58,500) depending on the technical knowledge they have, and, if they do not have it, they should have the financial resources necessary for its implementation on the webpage, or the EC should cover these costs. This estimation has been based on the fact that it is not known how the web pages of the organisers are implemented. With a favourable working environment, it could be implemented in 20-30 workdays but in unfavourable environments this period could be increased in the range of 30 to 90 workdays. For this third solution,

the organisers would need either to have technical knowledge for the support collection form integration, or to hire a developer to work on the integration of the embeddable solution.

In terms of maintenance, these costs are mostly afforded by the European Commission to update and maintain the embeddable solution, which require a minimum internal team of an IT architect and a developer. Maintenance costs and efforts are estimated on a yearly basis, for each initiative, and for a maximum of 3 campaign websites where the embeddable solution would be decentralised. For the first iframe solution, effort is estimated at low, between 15 to 20 workdays (estimated costs between €9,750 to €13,000). However, for the second iframe solution in MicroFrontend, if it is developed, the maintenance effort is estimated at medium, requiring one or two experts to maintain it (an IT architect and a developer) with average workdays of 60 to 90 days (estimated costs between €39,000 to €58,500) per year or per signature collection period. The work required is about upgrading and maintaining the embeddable solution, which is part of the COCS. For the API Gateway solution the maintenance effort is estimated at a high level between 90 to 120 workdays (estimated costs between €58,500 to €78,000). It requires a team of three experts to handle such a solution made of different applications: one IT architect and two developers.

For organisers, maintenance effort is mostly related to possible updates of the embeddable solution and the interaction with the EC during the 12-month collection process. Also for organisers, costs are estimated per year/collection period and per initiative and for a maximum of 3 campaign websites where the embeddable solution would be decentralised. We estimate these costs to be low for the first and second iframe at about 10 workdays (estimated costs €6,500). For the API Gateway solution, instead, the required effort is high, and it is estimated at 60 workdays (estimated costs €39,000) per year.

The below table summarises the estimated costs of implementation and maintenance per each actor.

Table 14: Costs (in €) of Implementation and Maintenance

Technical Solutions	iframe + better UX (TS01)	iframe + Micro frontend (TS02)	API Gateway + form (TS03)
Implementation (Development) one time cost for EC	39,000€ to 58,500€	117,000€ to 156.000€	156,000€ to 195,000€
Implementation (Integration) one time cost for organisers	9,750 €	9,750 €	19,500€ to 58,500€
Long term maintenance cost for EC (per year)	9,750€ to 13,000€	39,000€ to 58,500€	58,500€ to 78,000€
Long term maintenance cost for organisers (per year)	6,500 €	6,500 €	39,000 €

In relation to the infrastructure necessary to run the embeddable solution, for the first iframe solution it is not necessary to set up any infrastructure, the solution consists of a button in the current angular system of the EC.

For the second iframe solution in Microfrontend, it is necessary to configure a secured server to host the Angular form application, and Node js to install project dependencies.

For the API Gateway solution for the frontend part, it is necessary to install Node js to run package library and Java to connect with API Rest services.

5.2.3.3. IMPACT ON PERFORMANCE: MOBILE, CHANGE TO COCS, CAMPAIGN WEBSITES

The embeddable solution can have an impact on other variables, like mobile application, change required to the current COCS, and the campaigning site of the organisers. The below Table 15 summarises the key impact on the above variables and assesses them per each technical solution.

Table 15: Impact on Performance

	Technical Solutions	iframe + better UX (TS01)	iframe + Micro frontend (TS02)	API Gateway + form (TS03)
Impact	Mobile solution (customisation with related costs for the EC)	Responsive for mobile (iframe first configuration, but can be editable by organisers)	Responsive for mobile (iframe first configuration, but can be editable by organisers)	Responsive for mobile (relies on organisers to set proper styles)
	Impact on the redesign of the COCS	minimum	medium	high
	Campaign Site Performance Impact	high	high	high

The iframe is responsive for mobile. The dimensions of the iframe can be configured by default but the organiser can change the dimensions of the iframe locally on their websites so that the design is responsive. It can be set up a default width and height for the iframe dimensions on the EC website, but if the organisers want to modify these dimensions, they can do it locally on their website to adapt the iframe visibility to their specific needs and website's layout. In terms of technology, it is HTML coding configuring dimensions. For the style in the organisers' websites, they can also apply the Cascading Style Sheets. The EC can provide a default iframe dimensions, but organisers, if they have the knowledge, can adapt these dimensions according to their needs on their own campaigning websites.

In terms of changes to the current COCS, the first iframe solution will require very minimum change to the current structure. However, both the second iframe solution, and the API Gateway solution will have a more relevant impact to the current infrastructure of the COCS.

The second iframe solution with the micro frontend will require a substantial amount of work as assessed in previous sections. This will have an impact in the current system. The API gateway solution will also impact massively. In terms of performance on the campaigning website, the embeddable solution can have an impact, but this is determined on the basis of the type of hosting service the organisers will use. In particular, if there will be high volume visitors the campaigning site can crash if their hosting provider does not have the capability to handle thousands of visits per day. This happened in the case of Stop Finning, where their campaigning site crashed when visitors' numbers increased. They were able to continue to collect statements of support only because they relied on the current redirection option offered by the COCS. Therefore, if the campaigning site will crash because of the high volume of visitors, the embeddable solution will not be able to collect statements of support, therefore, there could be a dispute of responsibility between the support collection form provider and the EC's backend services about who is responsible and for what (ex. unavailability, issues, campaigning sites crash, etc.)

As supporters and organisers will turn to the EC to solve problem for which the EC would not be responsible, as website performance will be dependent on the hosting provider that the organisers will choose.

In terms of the iframe impact on the performance of the COCS, the iframe solution does not have an impact on the COCS in terms of performance. It will not be impacted in terms of speed as the iframe displays the content of the EC website on the organisers' website.

5.2.4. Data Protection and the Current ECI's Regulation

5.2.4.1. THE LEGISLATIVE FRAMEWORK

The ECI is governed by Regulation (EU) 2019/788 ("ECI Regulation") and, on the data protection side, particularly by its Article 19.

Articles 10 and 11 describe respectively the two different systems of the Central Online Collection System ("COCS" or "centralised system") and the Individual Online Collection System ("IOCS" or "individual system"). However, the IOCS can no longer be used as of 1 January 2023, for initiatives registered as of then. Today for initiatives registered as of 1 January 2023, the online collection is only possible via the centralised system.

According to Article 11(5), the European Commission must define the technical specifications for the individual online collection systems. These are laid down in the Implementing Regulation (EU) 2019/1799 and provide also in the context of this study useful reference as some of the security and data protection risks identified for the embeddable solutions are similar to the IOCS.

Regulation (EU) 2018/1725 applies to the processing of personal data by European institutions such as the European Commission, while Regulation (EU) 2016/679 ("GDPR") applies to any personal data processing, so including the one by the organisations taking the initiative.

5.2.4.2. DEFINITION OF COCS

Since 1 January 2023, the online collection of statements of support for an ECI can only be done through the COCS, with its redirection option.

Below follow some extracts about the COCS from the ECI Regulation which give an idea of the role of the European Commission on the COCS.

Recital 21: “(...) *the Commission should set up and operate a central system for the online collection of statements of support. That system should be made available free of charge to groups of organisers and should comprise the necessary technical features enabling online collection, including the hosting and software.*”

Article 10(1): “*The Commission shall set up and operate a COCS.*”

Article 10(2): “*The data obtained through the COCS shall be stored in the servers made available by the Commission for that purpose.*”

Both iframe solutions seem to be compatible with the definition of COCS (Art. 10). Because (i) the frontend part would look like an iframe of the official European Commission’s website; (ii) the personal data filled in the iframe are filled in on the campaigning website, which will provide a “view” on the collection form hosted on the servers of the European Commission. As a consequence, the frontend part embedded on the website of the organisers would still belong to the COCS operated by the European Commission.

Different is the assessment for the API Gateway solution, which, would hardly fall under the definition of a COCS, because the European Commission would not fully operate the most external component, namely the support collection form included in the hosting website. In the case of the API Gateway solution, the ECI Regulation should be amended with the definition of a new system alternative to COCS.

The below table summarises the technical solutions’ impact on the ECI Regulation.

Table 16: Impact on the ECI Regulation

	Technical Solutions	iframe + better UX (TS01)	iframe + Micro frontend (TS02)	API Gateway + form (TS03)
Impact: Regulatory	Regulatory impact	Medium (joint controllership agreement - temporary and/or amendment)	Medium (joint controllership agreement - temporary and/or amendment)	High (amendment required)

5.2.4.3. DATA PROTECTION RELEVANCE AND THE CERTIFICATION PROCESS

The European Commission and the organisations need to process different type of personal data for the collection of a given ECI. Not only those necessary to identify the citizens but, most importantly, with the personal support the citizen also expresses its opinion. In combination, these personal data qualify as special personal data according to the definition of Article 9 GDPR and Article 10 of Regulation (EU) 2018/1725, because they are very likely to reveal “*political opinions, religious or philosophical beliefs*”.³¹

Besides, the personal data are processed in the order of thousands and sometimes millions of figures, making the overall risks higher and the initiative more vulnerable to such risks.

In terms of security, the first and the second iframe solution propose the creation of an iframe within the website of the organisation so there is no reason to differentiate between the two for the purpose of assessing the data protection aspects. As exposed in the previous paragraphs, both pose a higher security risk, and therefore a higher data protection risks for the personal data of the citizens than the current COCS. A malicious actor could threaten the confidentiality, integrity and availability of the personal data on the websites of the organisations if they are insecure websites. According to the technical assessment, the third solution, API Gateway, would be even riskier for security.

If an embeddable solution is eventually implemented, the EC needs to ensure a certain level of security and data protection. Since Article 11 on IOCS is not effective anymore, there is currently no

³¹ Recital 43, Regulation (EU) 2018/1725.

legal basis for the certification scheme of the campaigning websites by the competent authority of the Member States.

For all three solutions the most effective way of verifying security and data protection would be to amend the ECI Regulation and set up a new auditing and certification scheme with a set of technical requirements.

In the case of the iframe solution, the European Commission could consider a personal data joint controllership agreement, as a temporary measure before the full amendment of the legislation. For the API Gateway solution an amendment of the Regulation would be compulsory.

For certification purposes, the national solution adopted for the IOCS under Article 11(3) of the ECI Regulation would ensure the organisers more easiness in reaching out to the certification authority. Moving this task from the national authority to the European Commission would ensure more coherence in the application of the criteria throughout the EU territory. Therefore, speaking strictly from the point of view of data protection, this second option seems to be preferable. The certification of campaigning websites could also be outsourced.

5.2.5. Risk and Security Assessment

This section details the risks and security concerns of each embeddable solution identified, including the mitigation strategies to put in place to reduce the risks of data breach.

Threats are in constant change and therefore security risk management needs to be in place with a specific security plan and regularly updated with the challenges of tomorrow. Security risk management includes risk and security assessment. A Risk Assessment is a process to identify potential hazards and analyse what could happen if a hazard occurs.³² A Security Assessment is the practice of testing or the evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.³³ A Security Risk Assessment (or SRA) is an assessment that involves identifying the risks the technology used, and in the processes to verify that controls are in place to safeguard against security threats.³⁴

In general, the main concerns in security are phishing and ransomware, other security concerns are misconfiguration, poor passwords, lack of patching, orphaned accounts or lost/stolen devices.

In the ECI case, the main risks are related to the life cycle deployment of the iframe solutions and the API Gateway solution.

To prevent the risks in the life cycle deployment, there exist best practices to attain when the solution is built. It places emphasis on security concerns during the production or application development process. From requirements to design, coding to test, these best practices strive to build security into a product or application at every development step.

The most common best practices used to secure an application are listed every year by the Open Worldwide Application Security Project (OWASP).³⁵ The OWASP is a non-profit foundation dedicated to improving software security. It operates under an “open community” model, which means that anyone can participate in and contribute to OWASP-related online chats, projects, and more.

The OWASP has maintained its Top 10 list since 2003, updating it every two or three years in accordance with advancements and changes in the AppSec market. The list’s importance lies in the actionable information it provides in serving as a checklist and internal web application development standard for many of the world’s largest organisations.

³² Ready Campaign. “*Risk Assessment*”. Accessed on 5 April 2023. <https://www.ready.gov/risk-assessment>

³³ NIST. “*Security Control Assessment*”. Accessed on 5 April 2023. https://csrc.nist.gov/glossary/term/security_control_assessment

³⁴ Adsero Security. “*So what exactly is a security risk assessment*”. Accessed on 5 April 2023. <https://www.adserosecurity.com/security-learning-center/what-is-a-security-risk-assessment/>

³⁵ The Open Worldwide Application Security Project. “*OWASP Top Ten*”. Accessed on 16 March 2023. <https://owasp.org/www-project-top-ten/>

In detail there exists a series of instructions that help to provide a concise collection of high value information on specific application security topics. These are the OWASP Cheat Sheets³⁶ that were created by various application security professionals who have expertise in specific security topics.

The below figures and tables summarise the risks associated to the three embeddable solutions identified.

Table 17 provides a general assessment of security and data protection risks, including the risks common to all three solutions identified. In this table a risk value from low to medium to high is assigned to each variable. Figure 6 provides a graph of the number of risks per each solution.

These **risks are associated with the decentralisation of the embeddable solution on any other external website**, and therefore they apply to each campaigning website. Decentralisation increases the risks of data breach when the support collection form is distributed in many other websites that are not audited. Organisers that were interviewed do not seem to be aware of these risks. Interviews revealed that some organisers have also decentralised the IOCS support collection form in the websites of partners organisations which were not covered by the certification process. Organisers indicated that they trusted the private collection software provided to them, and the fact that the same software has been initially certified by the German certifying authority (BSI), and that their main campaigning website was also certified. However, that certification was issued by the national authority based on the submitted information that the IOCS support collection form would only be hosted on one campaigning website. The national authority was not informed that organisers decentralised the support collection form on other websites.³⁷ Therefore, the decentralisation of an embeddable solution will require the application of risks mitigation strategies on each campaigning website.

Table 18 lists the risks and the mitigation strategies for each solution, including the residual risks. These risks and mitigation strategies are explained in detail in the following paragraphs. Nevertheless, it is important to highlight that **there are no mitigation strategies that can offer the same level of security as the current redirection option of the centralised COCS**, which provides citizens with the possibility of filling in the form with their personal data on the highly secure server of the European Commission. Mitigation strategies, if properly applied, only reduce the risks identified, however, the overall conclusion is that in any of the solutions **the residual risk after mitigation remains high**, because most **organisers have limited technical and security expertise on the risks associated with an embeddable solution**. In addition, most organisers will not be experts, and as seen in interviews, they have limited understanding of the risks associated with the collection of personal data via an embeddable solution. Therefore, the European Commission cannot base its risk mitigation strategies on trust of the organisers' compliance with the rules.

Table 17: General assessment of security and data protection risks

	Technical Solutions	Iframe + better UX (TS01)	Iframe + Micro frontend (TS02)	API Gateway + form (TS03)
Security and Data Protection	Security risks	medium-high	medium-high	high
	Data protection risks	medium-high	medium-high	high
	Phishing	high	high	high
	Cross-site scripting	high	high	high
	Code Injection	high	high	high
	Security misconfiguration	medium-high	medium-high	high
	Excessive data exposure	medium-high	medium-high	high
	Mass assignment	medium-high	medium-high	high

³⁶ The OWASP Cheat Sheet Series was created to provide a concise collection of high value information on specific application security topics. These cheat sheets were created by various application security professionals who have expertise in specific topics. OWASP. "OWASP Cheat Sheet Series". Accessed on 18 March 2023. <https://cheatsheetseries.owasp.org/>

³⁷ Email sent from the BSI, German Federal Office for Information Security (ECI websites' certification authority) to the Secretariat General on 31 January 2023. (Annex V)

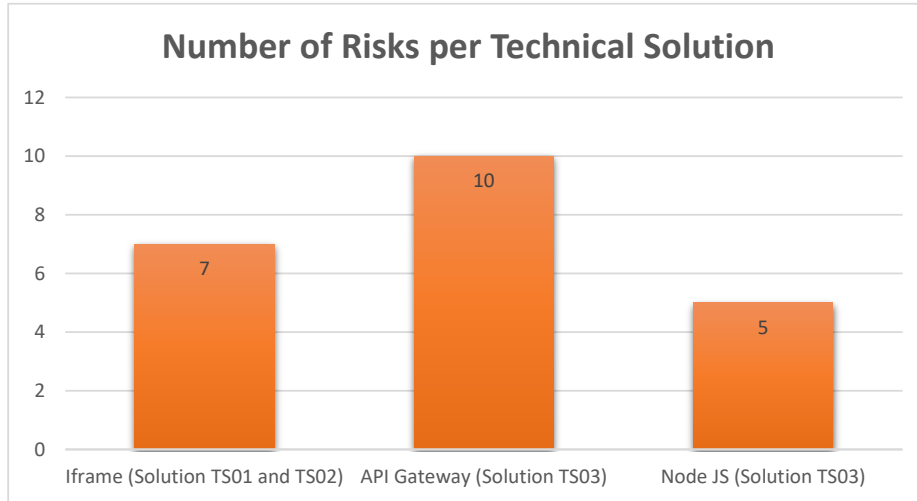


Figure 6: Number of Risks

Table 18: Risks³⁸ for each Embeddable Solution

	Risk	Likelihood	Impact	Risk Level	Risk Response Strategy reduced with Technical Mitigation	Residual Risk
Iframe (TS01 and TS02)	Phishing	4	4	16	Content Security Policy	medium-high
	Clickjacking	3	5	15	Client-side methods Server-side methods	medium-high
	Cross Site Scripting - Cross Frame Scripting	4	5	20	Secure frameworks Applying context sensitive coding Content Security Policy Sandbox attribute	high
	Security Misconfiguration	4	5	20	Specified HTTP verbs Cross-Origin Resource Sharing Policy	high
	Excessive Data Exposure	3	5	15	Filter Sensitive Data Classify sensitive and personally identifiable information Implement a schema-based response validation mechanism	medium-high
	Mass Assignment	4	4	16	Whitelist Built-in features to blacklist	medium-high

³⁸ Risk Matrix is based on the PM² Methodology and it is attached in Chapter 8 of this report.

Final Report

					Enforce schemas for the input data payloads	
	Code Injection	4	5	20	<ul style="list-style-type: none"> Whitelist Encode HTML outputs Use a static type of system Use the HttpOnly flag for cookies Avoid Javascript code serialization 	high
API gateway (TS03)	Security Misconfiguration	4	5	20	<ul style="list-style-type: none"> API life cycle API response payload schemas Specified HTTP verbs Cross-Origin Resource Sharing Policy 	high
	Broken Object Level Authorization	4	5	20	<ul style="list-style-type: none"> Authorization Mechanism Random and unpredictable values as GUIDs Tests to evaluate the authorization mechanism 	high
	Broken User Authentication	3	5	15	<ul style="list-style-type: none"> Authentication Mechanisms Multi-factor authentication. Anti brute force mechanisms <u>Account Lockout / Captcha Mechanism</u> 	medium-high
	Excessive Data Exposure	3	5	15	<ul style="list-style-type: none"> Filter Sensitive Data Classify sensitive and personally identifiable information Implement a schema-based response validation mechanism 	medium-high
	Lack of Resources & Rate Limiting	3	5	15	<ul style="list-style-type: none"> Use Docker Limit calls to API Server-side validation Maximum size of data 	medium-high
	Broken Function Level Authorization	4	5	20	<ul style="list-style-type: none"> Deny all access by default Review your API endpoints Check user's group/role 	high
	Mass Assignment	4	4	16	Whitelist	

Final Report

					Built-in features to blacklist Enforce schemas for the input data payloads	medium-high
	Injection	5	5	25	Validate incoming data Specific syntax Limit the number of returned records Data types and strict patterns	very-high
	Improper Assets Management	4	5	20	Inventory all API Document all aspects of your API API documentation available	high
	Insufficient Logging & Monitoring	4	4	16	Log all failed authentication attempts Logs should be handled as sensitive data Security Information and Event Management (SIEM) Configure custom dashboards	medium-high
Node Package Library (TS03)	Cross Site Scripting	4	5	20	Keep Software Up to Date Scan For Vulnerabilities Encode And Sanitize User Input Web Application Firewall	high
	Cross Site Request Forgery	4	5	20	Synchronizer Token Pattern Double submit cookie technique Verifying Origin With Standard Headers Same-Site Cookies Enabling User Interaction	high
	Code Injection	4	5	20	Whitelist Encode HTML outputs Use a static type of system Use the HttpOnly flag for cookies Avoid Javascript code serialization	high
	Distributed Denial Of Service	5	5	25	Design a Robust Architecture	very-high

					Use Cloud-Based Hosting from Major Providers Have a DDoS Response Plan Have a Static Version of Your Website Incorporate AI into your security stack	
	Regular Expression Denial Of Service Attacks	5	5	25	Implement a strict time cut-off on search Preformat/validate your regular expressions Have the regex operation does not happen on the user thread	very-high

5.2.5.1. IFRAME SOLUTIONS

The iframe solutions carry risks of data protection that will be addressed in this section. Previous figures list a total of seven risks. Of these risks, the below are considered the major risks:

- Phishing
- Clickjacking
- Cross site scripting (XSS)
- Cross frame scripting (XFS)

Nevertheless, iframe is also exposed to security misconfiguration, excessive data exposure, mass assignment and code injection, which are all threats common to the API Gateway solution as well. These threats and their mitigation strategies are described in the paragraphs below dedicated to the API Gateway solution.

Concerning security, the iframe solutions seem to be a less risky option comparing to the API Gateway solution. With the iframe solution, the support component can be hosted in a controlled and secured European environment. Moreover, there are many ways to secure an iframe: a) from preventing not allowed websites to use the iframe; b) to completely blocking the host to access the iframe content. For the first point, the iframe can be secured from cross-frame scripting, iframe phishing, iframe injection, clickjacking, malicious forms and malware download by using trusted third-party libraries, trusted plugins, by handling XSS in the website to prevent iframe injection, by using trusted Iframes source, by using proper Content-Security-Policy.

For the second point, if the iframe is properly secured, the iframe will not leak information. Also, the host websites will not be able to parse information in the iframe because the iframe is seen has a completely different website isolated from the host one. All current browsers strictly restrict access to iframe elements from host website scripts.

5.2.5.2. PHISHING

Phishing attack vector in iframe is important to discuss because some famous social networking websites, like Facebook, allow users and developers to integrate the third-party web page to their fan pages and other applications by using iframe. So, the iframe is dangerous because an attacker might use it for phishing purposes.

How to prevent it?

- Include Content-Security-Policy: frame-ancestors configurations.
- Use X-Frame-Options for older browser compatibility. These setups will make the website not allowed to be rendered by other sites other than included in the configurations.

5.2.5.3. CLICKJACKING

Clickjacking is an attack that tricks a user into clicking on a button or link that performs a malicious action such as installing malware or stealing sensitive information. The user clicks a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

There are several variations of the clickjacking attack, such as:

- Likejacking – a technique in which the Facebook “Like” button is manipulated, causing users to “like” a page they did not intend to like.
- Cursor jacking – a UI redressing technique that changes the cursor for the position the user perceives to another position.
- Cursor jacking relies on vulnerabilities in Flash and the Firefox browser, which has now been fixed.

How to prevent it?

There are two general ways to defend against clickjacking:

- Client-side methods: the most common is called Frame Busting. Client-side methods can be effective in some cases, but are considered not to be a best practice, because they can be easily bypassed.
- Server-side methods: the most common is X-Frame-Options. Server-side methods are recommended by security experts as an effective way to defend against clickjacking.

5.2.5.4. IFRAME INJECTION XSS (CROSS-SITE-SCRIPTING)

An iframe injection, Cross-Site scripting (XSS) is a common cross-site scripting attack that combines malicious JavaScript with an iframe that loads a legitimate page to steal data from an unsuspecting user. This attack is usually only successful when combined with social engineering. An example of an iframe injection XSS attack would consist of an attacker convincing the user to navigate to a web page the attacker controls. The attacker’s page then loads malicious JavaScript and an HTML iframe pointing to a legitimate site. Once the user enters credentials into the legitimate site within the iframe, the malicious JavaScript steals the keystrokes.

Cross-Frame Scripting (XFS) combines Iframes with malicious JavaScript to steal data from users.

XFS attackers persuade a user to visit a web page regulated by the attacker and loads an iframe combined with malicious JavaScript referring to a legitimate site. The malicious JavaScript code keeps track of the user’s keystrokes after inserting credentials into the legitimate site within the iframe.

XFS attacks can be prevented by including Content-Security-Policy: frame-ancestors and X-Frame-Options headers in web server configuration.

Cross-site scripting (XSS) and cross-frame scripting (XFS) are both security vulnerabilities that can be exploited by attackers to inject and execute malicious code in a victim's browser. However, there are some differences between these two types of attacks:

1. **Scope:** XSS attacks occur when an attacker injects malicious code into a website that is then executed in the victim's browser, usually as a result of the victim clicking on a link or visiting a page. Cross-frame scripting, on the other hand, occurs when an attacker injects malicious code into an iframe or a frame on a different domain that is then executed in the context of the victim's browser.
2. **Target:** XSS attacks typically target web applications that accept user input, such as search boxes, comment fields, or contact forms. Cross-frame scripting, on the other hand, targets websites that use iframes or frames to display content from other domains.
3. **Prevention:** both XSS and cross-frame scripting can be prevented by implementing proper security measures such as input validation, Content Security Policy (CSP), and X-Frame-Options headers. However, preventing XSS attacks is generally more complex and requires more security measures due to the nature of the attack and the wide range of vulnerable web applications.

Overall, while XSS attacks and cross-frame scripting attacks have some similarities, they differ in terms of scope, target, and prevention measures. Web developers should be aware of both types of attacks and take appropriate security measures to prevent them.

How to prevent it?

- Use secure frameworks that, by design, automatically encode content to prevent XSS, such as Ruby 3.0 or React JS.
- Encoding unreliable HTTP request data in HTML output fields (body, attributes, JavaScript, CSS, or URL) resolves Reflected XSS and Stored XSS. The OWASP Cheat Sheet for Avoiding XSS has details of the required data encryption techniques.
- Applying context sensitive coding, when the document is modified in the client's browser, helps prevent XSS DOM. When this technique cannot be applied, similar coding techniques can be used, as explained in the OWASP cheat sheet to avoid XSS DOM.
- Enabling a Content Security Policy (CSP) supposes a deep defence for the mitigation of XSS vulnerabilities, assuming that there are no other vulnerabilities that allow placing malicious code via inclusion of local files, vulnerable libraries in known sources stored in Content Distribution Networks (CDN) or locally.

5.2.5.5. TECHNIQUE TO SECURE IFRAME

Here are some ways to secure an iframe:

1. **Use the "sandbox" attribute:** The "sandbox" attribute can be added to an iframe to restrict its behaviour and prevent it from accessing the parent page or performing certain actions such as running scripts or submitting forms. This can help prevent clickjacking and other attacks.
2. **Set the "X-Frame-Options" header:** The "X-Frame-Options" header can be set in the server's HTTP response to restrict which sites are allowed to embed the iframe. This can help prevent clickjacking and other attacks by ensuring that the iframe is only embedded on trusted sites.
3. **Use Content Security Policy (CSP):** CSP allows web developers to specify which sources of content are trusted for a given web page. By using CSP directives to restrict the sources of content that can be loaded within an iframe, web developers can prevent XSS attacks and other code injection attacks.

4. Use secure protocols: Iframes should be loaded over secure protocols such as HTTPS to prevent data interception and tampering.
5. Validate inputs: If an iframe is used to display user-generated content, it's important to validate the input to prevent XSS and other attacks.
6. Check for vulnerabilities: Regularly scan the site for vulnerabilities, including those that may affect iframes.

By implementing these measures, web developers can help secure iframes and prevent them from being used in malicious attacks.

5.2.5.6. CONTENT SECURITY POLICY FOR IFRAME

Content Security Policy (CSP) is a security mechanism that helps prevent cross-site scripting (XSS) attacks and other code injection attacks by allowing website owners to specify which source of content are trusted for a given web page.

A Content Security Policy is a set of directives that is sent to the user's web browser, instructing it to only load resources from trusted sources such as the website itself or specified domains. This can help prevent malicious content from being loaded onto a web page and from being loaded onto a web page and executed in the user's browser.

CSP can be implemented using an HTTP response header, or through a meta tag in the HTML or a web page. The directives specified in the policy can control what types of resources are allowed to be loaded, such as scripts, stylesheets, images, and fonts.

CSP can also help protect against clickjacking attacks by allowing website owners to specify which domains are allowed to embed their content on a given page. Additionally, CSP reports can be used to monitor and analyse security issues and threats on a website.

That said, it is useful to be able to place restrictions upon iframed support collection form. A specific mechanism, which relies on an explicit opt-in from the embedded content, ought to make it possible for support collection forms to cooperate with their embedders to negotiate a reasonable set of restrictions.

In short, the embedder proposes a Content Security Policy by setting an attribute on an iframe element. This policy is transmitted along with the HTTP request for the framed content in an HTTP request header (Sec-Required-CSP). If the embedded content can accept that policy, it can enforce it by returning a Content-Security-Policy or Allow-CSP-From header along with the response. If the response contains a policy at least as strict as the policy which the embedder requested, or accepts the embedder-provided policy, then the user agent will render the embedded content. If no such assertion is present, the response will be blocked.³⁹

5.2.5.7. API SECURITY

Many threats face modern software applications. Having benchmarks for such vulnerabilities is paramount to ensure application security before an attack occurs.

³⁹ West, Mike. (2021, March 23). "Content Security Policy: Embedded Enforcement". W3C. Accessed on 19 March 2023. <https://w3c.github.io/webappsec-cspee/#:~:text=Content%20Security%20Policy%20is%20a,content%20loaded%20in%20via%20iframe%20>.

As the value of APIs increases in our daily lives, these touchpoints become more vulnerable to attack. Below, we highlight the latest OWASP top 10 API security vulnerabilities list and expand on what actions an API provider can take to address each insecurity.

The OWASP API Security Project is updating its Top 10 API Security Risks for 2023. Last updated in 2019, the new list acknowledges many of the same risks, adds a few new ones, and drops a couple off the list. For example, logging and monitoring, and injection no longer make the top 10 risks, although they are still significant factors. New to the list are server-side request forgery (SSRF) and unsafe consumptions of APIs.

The list is not finalized yet, but it is available on the OWASP GitHub site for review and comment. As it stands, here are the items that made the 2023 list:⁴⁰

1. Broken object level authorization
2. Broken authentication
3. Broken object property level authorization
4. Unrestricted resource consumption
5. Broken function level authorization
6. Server side request forgery
7. Security misconfiguration
8. Lack of protection from automated threats
9. Improper asset management
10. Unsafe consumption of APIs

These actions boil down to a few basic security strategies. Most of these vulnerabilities can be mitigated by implementing the following approaches:

- Use an API gateway.
- Use access tokens and make sure to audit them rigorously.
- Use claims to simplify authorisation. If the token has enough data to authorize on, then the logic becomes simpler in the API.
- Use Pairwise pseudonymous identifiers (PPIDs) to avoid leaking personally identifiable information to external parties, even in the tokens.

The main vulnerabilities and risk in API are:

5.2.5.8. BROKEN OBJECT LEVEL AUTHORIZATION

APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object level authorization checks should be considered in every function that accesses a data source using an input from the user.

Object level authorization is an access control mechanism that is usually implemented at the code level to validate that one user can only access objects that they should have access to.

Every API endpoint that receives an ID of an object, and performs any type of action on the object, should implement object level authorization checks. The checks should validate that the logged-in user does have access to perform the requested action on the requested object.

Failures in this mechanism typically leads to unauthorised information disclosure, modification, or destruction of all data.

How to prevent it:

⁴⁰ Github. "API Security – Top Ten". Accessed on 20 March 2023. <https://github.com/OWASP/API-Security/tree/master/2023/en/src>

- Implement a proper authorization mechanism that relies on the user policies and hierarchy.
- Use an authorization mechanism to check if the logged-in user has access to perform the requested action on the record in every function that uses an input from the client to access a record in the database.
- Prefer to use random and unpredictable values as Globally Unique Identifier (“GUIDs”) for records’ IDs.
- Write tests to evaluate the authorization mechanism. Do not deploy vulnerable changes that break the tests.

5.2.5.9. BROKEN USER AUTHENTICATION

Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user’s identities temporarily or permanently. Compromising a system’s ability to identify the client/user, compromises API security overall.

Authentication endpoints and flows are assets that need to be protected. “Forgot password / reset password” should be treated the same way as authentication mechanisms.

An API is vulnerable if it:

- Permits credential stuffing whereby the attacker has a list of valid usernames and passwords.
- Permits attackers to perform a brute force attack on the same user account, without presenting captcha/account lockout mechanism.
- Permits weak passwords.
- Sends sensitive authentication details, such as auth tokens and passwords in the URL.
- Doesn’t validate the authenticity of tokens.
- Accepts unsigned/weakly signed JWT tokens⁴¹ (“alg”:“none”)/doesn’t validate their expiration date.
- Uses plain text, non-encrypted, or weakly hashed passwords.
- Uses weak encryption keys.

How to prevent it:

- Know all possible flows to authenticate to the API (mobile/web/deep links that implement one-click authentication/etc.).
- Check which flows it is missed.
- Read about authentication mechanisms. Understand what and how they are used. OAuth is not authentication, and neither is API keys.
- Don't reinvent the wheel in authentication, token generation, password storage. Use the standards.
- Credential recovery/forgot password endpoints should be treated as login endpoints in terms of brute force, rate limiting, and lockout protections.
- Use the OWASP Authentication Cheatsheet.
- Where possible, implement multi-factor authentication.
- Implement anti brute force mechanisms to mitigate credential stuffing, dictionary attack, and brute force attacks on the authentication endpoints. This mechanism should be stricter than the regular rate limiting mechanism on the API.
- Implement account lockout / captcha mechanism to prevent brute force against specific users. Implement weak-password checks.
- API keys should not be used for user authentication, but for client app/ project authentication.

⁴¹ JSON Web Token (JWT) is a compact URL-safe means of representing claims to be transferred between two parties.

5.2.5.10. EXCESSIVE DATA EXPOSURE

Looking forward to generic implementations, developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user.

The API returns sensitive data to the client by design. This data is usually filtered on the client side before being presented to the user. An attacker can easily sniff the traffic and see the sensitive data.

How to prevent it:

- Never rely on the client side to filter sensitive data.
- Review the responses from the API to make sure they contain only legitimate data.
- Backend engineers should always ask themselves "who is the consumer of the data?" before exposing a new API endpoint.
- Avoid using generic methods (e.g. `to_json()` and `to_string()`).
- Classify sensitive and personally identifiable information (PII) that an application stores and works with, reviewing all API calls returning such information to see if these responses pose a security issue.
- Implement a schema-based response validation mechanism as an extra layer of security. As part of this mechanism, it is defined and enforced data returned by all API methods, including errors.

5.2.5.11. LACK OF RESOURCES & RATE LIMITING

Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force.

API requests consume resources such as network, CPU, memory, and storage. The number of resources required to satisfy a request greatly depends on the user input and endpoint business logic. Also, consider the fact that requests from multiple API clients compete for resources. An API is vulnerable if at least one of the following limits is missing or set inappropriately (e.g., too low/high):

- Execution timeouts
- Max allocable memory
- Number of file descriptors
- Number of processes
- Request payload size (e.g., uploads)
- Number of requests per client/resource
- Number of records per page to return in a single request response

How to prevent it:

- Docker makes it easy to limit memory, CPU, number of restarts, file descriptors, and processes.
- Implement a limit on how often a client can call the API within a defined timeframe.
- Notify the client when the limit is exceeded by providing the limit number and the time at which the limit will be reset.
- Add proper server-side validation for query string and request body parameters, specifically the one that controls the number of records to be returned in the response.
- Define and enforce maximum size of data on all incoming parameters and payloads such as maximum length for strings and maximum number of elements in arrays.

5.2.5.12. BROKEN FUNCTION LEVEL AUTHORIZATION

Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By

exploiting these issues, attackers gain access to other users' resources and/or administrative functions.

The best way to find broken function level authorization issues is to perform deep analysis of the authorization mechanism, while keeping in mind the user hierarchy, different roles or groups in the application, and asking the following questions:

- Can a regular user access administrative endpoint?
- Can a user perform sensitive actions (e.g., creation, modification, or erasure) that they should not have access to by simply changing the HTTP method (e.g., from GET to DELETE)?
- Can a user from group X access a function that should be exposed only to users from group Y, by simply guessing the endpoint URL and parameters (e.g., /api/v1/users/export all)?

Don't assume that an API endpoint is regular or administrative only based on the URL path. While developers might choose to expose most of the administrative endpoints under a specific relative path, like api/admins, it's very common to find these administrative endpoints under other relative paths together with regular endpoints, like api/users.

How to prevent it:

The application should have a consistent and easy to analyse authorisation module that is invoked from all business functions. Frequently, such protection is provided by one or more components external to the application code:

- The enforcement mechanism(s) should deny all access by default, requiring explicit grants to specific roles for access to every function.
- Review the API endpoints against function level authorization flaws, while keeping in mind the business logic of the application and groups hierarchy.
- Make sure that all administrative controllers inherit from an administrative abstract controller that implements authorization checks based on the user's group/role.
- Make sure that administrative functions inside a regular controller implement authorization checks based on the user's group and role.

5.2.5.13. MASS ASSIGNMENT

Binding client provided data (e.g., JSON) to data models, without proper properties filtering based on an allowlist, usually leads to Mass Assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads, allows attackers to modify object properties they are not supposed to.

Objects in modern applications might contain many properties. Some of these properties should be updated directly by the client (e.g., user.first_name or user.address) and some of them should not (e.g., user.is_vip flag).

An API endpoint is vulnerable if it automatically converts client parameters into internal object properties, without considering the sensitivity and the exposure level of these properties. This could allow an attacker to update object properties that they should not have access to.

How to prevent it:

- If possible, avoid using functions that automatically bind a client's input into code variables or internal objects.
- Whitelist only the properties that should be updated by the client.
- Use built-in features to blacklist properties that should not be accessed by clients.
- If applicable, explicitly define and enforce schemas for the input data payloads.

5.2.5.14. SECURITY MISCONFIGURATION

Security misconfiguration is commonly a result of unsecure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information.

The API might be vulnerable if:

- Appropriate security hardening is missing across any part of the application stack, or if it has improperly configured permissions on cloud services.
- The latest security patches are missing, or the systems are out of date.
- Unnecessary features are enabled (e.g., HTTP verbs).
- Transport Layer Security (TLS) is missing.
- Security directives are not sent to clients (e.g., Security Headers).
- A Cross-Origin Resource Sharing (CORS) policy is missing or improperly set.
- Error messages include stack traces, or other sensitive information is exposed.

How to prevent it:

The API life cycle should include:

- A repeatable hardening process leading to fast and easy deployment of a properly locked down environment.
- A task to review and update configurations across the entire API stack. The review should include: orchestration files, API components, and cloud services (e.g., S3 bucket permissions).
- A secure communication channel for all API interactions access to static assets (e.g., images).
- An automated process to continuously assess the effectiveness of the configuration and settings in all environments.

Furthermore:

- To prevent exception traces and other valuable information from being sent back to attackers, if applicable, define and enforce all API response payload schemas including error responses.
- Ensure API can only be accessed by the specified HTTP verbs. All other HTTP verbs should be disabled (e.g. HEAD).
- APIs expecting to be accessed from browser-based clients (e.g., WebApp frontend) should implement a proper Cross-Origin Resource Sharing (CORS) policy.

5.2.5.15. INJECTION

Injection flaws, such as SQL, NoSQL, Command Injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

The API is vulnerable to injection flaws if:

- Client-supplied data is not validated, filtered, or sanitized by the API.
- Client-supplied data is directly used or concatenated to SQL/NoSQL/LDAP queries, OS commands, XML parsers, and Object Relational Mapping (ORM)/Object Document Mapper (ODM).
- Data coming from external systems (e.g., integrated systems) is not validated, filtered, or sanitized by the API.

How to prevent it:

- Preventing injection requires keeping data separate from commands and queries.
- Perform data validation using a single, trustworthy, and actively maintained library.
- Validate, filter, and sanitize all client-provided data, or other data coming from integrated systems.
- Special characters should be escaped using the specific syntax for the target interpreter.
- Prefer a safe API that provides a parameterized interface.
- Always limit the number of returned records to prevent mass disclosure in case of injection.
- Validate incoming data using sufficient filters to only allow valid values for each input parameter.

- Define data types and strict patterns for all string parameters.

5.2.5.16. IMPROPER ASSETS MANAGEMENT

APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints.

The API might be vulnerable if:

- There is no documentation, or the existing documentation is not updated.
- There is no retirement plan for each API version.
- Hosts inventory is missing or outdated.
- Integrated services inventory, either first- or third-party, is missing or outdated.
- Old or previous API versions are running unpatched.

How to prevent it:

- Inventory all API hosts and document important aspects of each one of them, focusing on the API environment (e.g., production, staging, test, development), who should have network access to the host (e.g., public, internal, partners) and the API version.
- Inventory integrated services and document important aspects such as their role in the system, what data is exchanged (data flow), and its sensitivity.
- Document all aspects of the API such as authentication, errors, redirects, rate limiting, cross-origin resource sharing (CORS) policy and endpoints, including their parameters, requests, and responses.
- Generate documentation automatically by adopting open standards. Include the documentation build in the CI/CD pipeline.
- Make API documentation available to those authorized to use the API.
- Use external protection measures such as API security firewalls for all exposed versions of the APIs, not just for the current production version.
- Avoid using production data with non-production API deployments. If this is unavoidable, these endpoints should get the same security treatment as the production ones.
- When newer versions of APIs include security improvements, perform risk analysis to make the decision of the mitigation actions required for the older version: for example, whether it is possible to backport the improvements without breaking API compatibility or need to take the older version out quickly and force all clients to move to the latest version.

5.2.5.17. INSUFFICIENT LOGGING & MONITORING

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems to tamper with, extract, or destroy data. Most breach studies demonstrate the time to detect a breach is over 200 days⁴², typically detected by external parties rather than internal processes or monitoring.

The API is vulnerable if:

- It does not produce any logs, the logging level is not set correctly, or log messages do not include enough detail.
- Log integrity is not guaranteed (e.g., Log Injection).
- Logs are not continuously monitored.
- API infrastructure is not continuously monitored.

How To Prevent it?

⁴² Sobers, Rob. (2022, June 22). "Data Breach Response Times: Trends and Tips". Accessed on 18 March 2023. <https://www.varonis.com/blog/data-breach-response-times>

- Log all failed authentication attempts, denied access, and input validation errors.
- Logs should be written using a format suited to be consumed by a log management solution and should include enough detail to identify the malicious actor.
- Logs should be handled as sensitive data, and their integrity should be guaranteed at rest and transit.
- Configure a monitoring system to continuously monitor the infrastructure, network, and the API functioning.
- Use a Security Information and Event Management (SIEM) system to aggregate and manage logs from all components of the API stack and hosts.
- Configure custom dashboards and alerts, enabling suspicious activities to be detected and responded to earlier.

5.2.5.18. NODE JS DEPLOYMENT

The Node.js platform is inherently secure, but because it uses third-party open-source packages through its package management system (npm), it is vulnerable to cyber-attacks. Companies must implement the best practices like those outlined in this article to maintain the security of Node.js.

Node.js can be secured by establishing practices like validating user input, implementing authentication, limiting request sizes, and setting up logging and monitoring are good first steps to securing Node.js. For specific concerns about code injection attacks, here are five ways to prevent code injection in Node.js.

Like any application, those built with Node.js come with security risks.

The following top five security risk:

CROSS-SITE SCRIPTING (XSS)

If a web application fails to adequately validate user input, malicious actors can inject modified JavaScript code into the web pages users are viewing. Because the browser can't determine the trustworthiness of the code, it executes the script by default, potentially giving the attacker access to cookies, tokens, user information, and more.

How to prevent it:

- **Keep Software Up to Date.** Software should always be kept up to date for many reasons, including fixing bugs, improving performance, installing new features and patching security vulnerabilities. Regularly updating software will greatly reduce the vulnerabilities that leave a site or application open to XSS vulnerabilities.
- **Scan For Vulnerabilities.** A scan should be regularly done for all web-facing infrastructure for vulnerabilities. Many vulnerability scanning tools can identify applications and web sites that are vulnerable to XSS attacks.
- **Encode And Sanitize User Input.** Input fields are the most common point of entry for XSS attack scripts. Therefore, it should always be screened and validated any information input into data fields. This is particularly important if the data will be included as HTML output to protect against reflected XSS attacks.
- **A web application firewall (WAF)** can be a powerful tool for protecting against XSS attacks. WAFs can filter bots and other malicious activities that may indicate an attack. Attacks can then be blocked before any script is executed.
- **Implement A Content Security Policy.** A content security policy (CSP) is a http response header that can define the functions a website is allowed to perform. They can be used to prevent a website from accepting any in-line scripts. This may be the strongest method at disposal as it can completely block XSS attacks or at least greatly reduce the possibility of them.

CROSS-SITE REQUEST FORGERY (CSRF)

A cross-site request forgery attack hijacks user sessions by hiding malicious code under seemingly trustworthy HTML elements. Because the user is already logged in and authenticated, clicking one of these masked links gives the hacker the ability to execute changes in the underlying systems.

How to prevent it:

- Token Synchronization. CSRF tokens help prevent CSRF attacks because attackers cannot make requests to the backend without valid tokens.
- Double-Submitting Cookies. The double-submit cookie method is an alternative to maintaining the CSRF token state on the server-side, which can be problematic.
- Same-Site Cookies. Same-site cookies help defend against CSRF attacks by restricting the cookies sent alongside each request.
- Enabling User Interaction. While most CSRF techniques do not involve user interaction, users can help secure transactions in some cases.
- Custom Headers for Requests. Adding custom request headers is an especially effective defence for API and AJAX endpoints.
- Conduct Regular Web Application Security Tests to Identify CSRF. Even if vulnerabilities in web applications with CSRF attacks are successfully addressed, application updates and code changes may expose the application to CSRF in the future.

CODE INJECTION

Attackers can use an input validation flaw to inject malicious code into the codebase, changing the way the application executes. Code injection can give them access to sensitive data, provide information about the environment, or infect the system with malware.

How to prevent it:

- Utilise Whitelisting for input validation – Whitelisting is simpler to set up and gives security teams stricter control over what data or types of input the application can process, thereby helping to reduce the risk of an attacker executing malicious code.
- Encode HTML outputs – Security teams should leverage contextual output encoding to convert malicious input into safer representatives, where user data can be displayed but not executed as code.
- Use a static type of system to enforce language separation – With static type systems, teams can develop declarative control checks without the additional run-time overhead.
- Leverage Parameterized Queries and Criteria-Based APIs to interpret user data strings – This is done to ensure that APIs do not accept any string values other than those specified. Additionally, parameterized queries consider inputs of malicious commands as a string instead of an SQL command.
- Avoid using unsafe functions in source code – It's important to avoid all vulnerable code evaluation constructs when developing source code. Developers should instead use secure, dedicated, language-specific features to process user-supplied inputs.
- Use the HttpOnly flag for cookies to disable client-side script interaction – If the server sets the HttpOnly flag on every cookie it creates, it indicates that the cookie should not be accessible from the client side. Even with HTML injection flaws, the cookies cannot be revealed to third parties.
- Use SCA Tools to find and fix issues – Teams should set up automatic static code checking tools to find and eliminate injection vectors in source code
- Avoid Javascript code serialization – Developers use code serialization to rearrange input data into a set of regular functions and expressions.

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

In a DDoS attack, an attacker floods production servers with internet traffic to disrupt their normal function. This traffic can overwhelm the system and cause significant damage and outages. Versions 4-4.1.1 of Node.js that contained a bug with the HTTP handling are one example of this.

How to prevent it:

- Design a Robust Architecture
- It is crucial to ensure that the IT infrastructure doesn't have any single points of failure that a cyber-attacker could exploit. This could mean ensuring that data servers have different networks and paths, locating servers in separate data centres in different geographical points and securing the diversity of service providers.
- Use Cloud-Based Hosting from Major Providers
- Closely related to designing a robust architecture, cloud-based hosting typically uses multiple servers to store files. Suppose one of those servers goes down because of a DDoS attack. In that case, other servers can offer reprieve, ensuring that there is not any downtime because resources will be shared across multiple servers. When deciding on a hosting provider, consider whether the provider hosts websites through major providers or using their own servers.
- Have a DDoS Response Plan
- What will the European Commission do when a DDoS attack happens? What are the notification and escalation procedures? By ensuring the European Commission has a plan in place, it will be able to respond promptly and effectively when attackers target the network. The challenge here is that the more complicated the infrastructure, the more intricate the DDoS plan will have to be.
- Having a static version of the website can help remediate DDoS attacks since there is a place to send the traffic if the website does go down. A static version of the website requires significantly less processing power and bandwidth to lower some of the load on the backends' servers.
- Incorporate AI into the security stack.
- Given the scale and speed at which attackers launch DDoS attacks, humans are just not effective responders. Types of security systems leveraging artificial intelligence (AI) can learn what "normal" for a business is. AI can even respond to a DDoS attack — when an "abnormal" uptick in traffic occurs, AI can analyse the traffic and block access from suspicious locations, to enforce the "normal."

REGULAR EXPRESSION DENIAL OF SERVICE ATTACKS (REDOS)

This type of denial-of-service (DoS) attack can take a system down by providing an input that makes it time-consuming for the program to evaluate a regular expression. This slows or even halts the program and produces a DoS to legitimate users.

How to prevent it:

- Implement a strict time cut-off on search. If a regular expression takes too long, kill it at once, and inform the user that the regular expression was taking too long.
- Preformat/validate the regular expressions. In other words, let people search for text directly, rather than input a regular expression directly. Provide UX options that give organisers the chance to narrow down their focus.
- Have the regex operation *does not happen* on the user thread - instead, spawn a separate thread, implement a good time cut-off for operations to complete in, and handle it asynchronously. Potentially malicious operations should always be isolated from users and be easily killed if necessary.

5.2.5.19. HOW TO SECURE THE COLLECTION PROCESS WITH AN API GATEWAY SOLUTION IN PLACE

The collection of personal data of EU citizens demand attention during the whole process. This process needs to be secure in full if an embeddable solution is implemented. Therefore, it seems crucial to identify and set up the boundaries of the online support collection process. These boundaries should consider the whole process from the moment in which the data are inserted in the embeddable solution (Step 1), passing through the communication with the COCS when data are sent after a supporter will click the submit button (Step 2), until the time the data reach and are stored on the European Commission servers (Step 3). Figure 7 below shows the three steps of the personal data collection process under an ECI. This process therefore will need to be secured from step 1 to step 3 if an embeddable solution, in particular an API Gateway solution, is eventually offered.

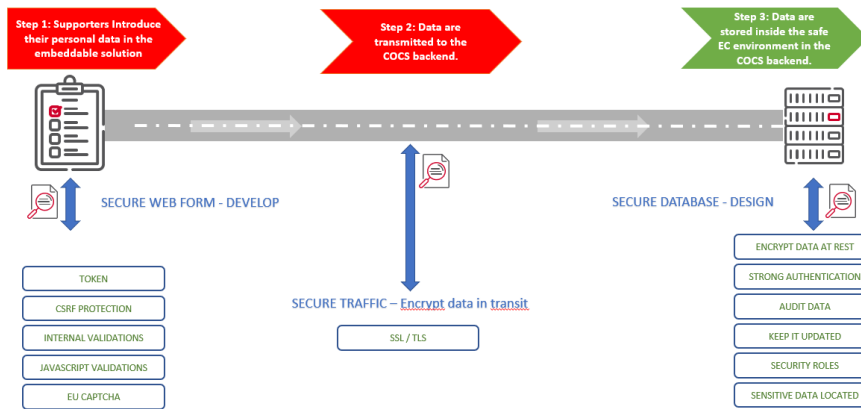


Figure 7: Securing the 3-Step Pathway of the Personal Data Collection Process

At Step 2 also the communication between the embeddable solutions on the organisers' websites and the COCS should be secured. At this level there should be a security plan in place from a technical point of view. The data transfer to the COCS servers can be encrypted with Secure Sockets Layer⁴³ (SSL) throughout, and Transport Layer Security (TLS).

To secure the transfer, data can be encrypted. Encryption is about keeping the online activities and the accompanying personal and business-related information safe from the eyes of third parties, who would just love to be able to steal personal information. The Electronic Frontier Foundation (EFF) has developed a browser extension called "HTTPS Everywhere", which automatically enables an HTTPS connection for websites that support HTTPS. This protects in full the connection.

At Step 3, the data will be stored in the COCS backend, which is a secure environment on the European Commission servers. Therefore, if an embeddable solution is implemented, Step 1 and 2 will need to be secured.

One critical challenge in fact would be how to prevent the embeddable solution (support collection form or iframe) to be replicated on non-certified websites, and specifically on how to limit their use to websites located within the European Union territory. Furthermore, organisers should be prevented from modifying the code of the embeddable solution.

⁴³ SSL is a standard security technology for establishing an encrypted link between a server and a client.

6. Phase III: Recommendations

The third and last phase of the study aims at providing the key takeaways from what was presented and analysed in Phase I and Phase II and provide final recommendations to the European Commission.

6.1. Key Takeaways on the Technical Solutions' Main Elements and Benefits

In the SWOT⁴⁴ analysis this study identified three possible technical solutions that could provide an answer to the research questions. The first technical solution identified is named *'iframe'*. An iframe is an in-line frame and it is commonly used to embed specific content like external ads, videos, tags, or other interactive elements into a page. The main advantage of iframe is that it can be easily placed almost anywhere within a website. This first Iframe solution provides organisers with a 'view' within their campaigning website on the whole COCS frontend part located on the European Commission servers. The second technical solution identified is *'iframe + Micro Frontend Application'*. Micro Frontend permits to decompose the COCS of the European Commission website into independent 'microapps' working loosely together. This second solution would provide organisers with a 'view', within their campaigning website, on the support collection form of the COCS frontend part located on the European Commission servers. This is different from the first iframe solution, where the whole COCS frontend website of the European Commission would be loaded within the campaigning website. The third technical solution identified is *'API Gateway solution'*. The European Commission will have to set up an API Gateway for the ECI, which can be used together with a support collection form developed by the European Commission, a third party, or the ECI organisers themselves. If the API Gateway will not be available for the ECI, as an alternative, the support collection form could be decentralised via web services, which also offer customisable opportunities. **All three solutions would only partially meet the organisers' needs**, because these solutions will not easily allow the customisation of the collection form, or the collection of analytics, or the decentralisation on third parties' websites.

6.2. Key Takeaways on Technical Implementation, Operational Management and Costs

Operational management impacts the European Commission and the organisers in terms of the team required for the implementation and maintenance of the embeddable solution.

In terms of technical implementation, all solutions identified are viable and can be implemented for the frontend part of the COCS. As regards to the complexity of implementation and estimated costs, all solutions require substantial effort and costs for their implementation and yearly costs for maintenance. The estimated costs are one-off costs for the development of the solution by the European Commission and the organisers' integration of the embeddable solution on maximum three campaign websites.

The first iframe solution is easy to implement for the EC and the organisers. In terms of costs, it is medium-costly for the European Commission (€39,000 to €58,500 one-off) and low for organisers (€9,750). The second iframe solution has a medium-high difficulty of implementation for the European Commission, while it will be relatively easy for the organisers to integrate in their campaigning websites. In terms of costs, the second iframe solution, is high-costly for the European Commission (€117,000 to €156,000), and relatively low for organisers (€9,750). The API Gateway solution, instead, is hard to implement and high-costly for both the European Commission (€156,000 to €195,000) and the organisers (€19,500 to €58,500).

⁴⁴ SWOT stands for Strengths, Weaknesses, Opportunities, and Threats. A SWOT analysis is a technique for assessing these four aspects of a project. The analysis can help to understand different scenarios and options, and in particular what is the best option for a successful strategy for the future.

Long term maintenance for the embeddable solutions also requires efforts on both the EC and the organisers. Maintenance costs are estimated on a yearly basis, for each initiative and for a maximum of three campaign websites where the embeddable solution is decentralised. The first iframe solution is easy to maintain and requires low costs for both the EC (€9,750 to €13,000 per year) and the organisers (€6,500 per year). The second iframe solution has medium difficulty and requires medium maintenance costs for the European Commission (€39,000 to €58,500 per year), while it is easy to maintain for the organisers and has relatively low costs (€6,500 per year) on them. The API Gateway solution, instead, is hard to maintain and requires very high maintenance costs for both the European Commission (€58,500 to €78,000 per year) and the organisers (€39,000 per year). Detailed estimate of costs for the implementation and maintenance are provided in [section 5.2.3.2](#) below.

6.3. Key Takeaways on the Technical Solutions: Security, Data Protection Risks and Mitigation Strategies

All solutions identified present high security and data protection risks, which should be carefully considered by the European Commission before deciding on their potential implementation. **These risks are associated with the decentralisation of the embeddable solution on any other external website.** For all three solutions, supporters will physically insert their personal data on the organisers' campaigning websites. A malicious actor could threaten the confidentiality, integrity and availability of the personal data when EU citizens fill in the support form via the organisers' campaigning websites if these are insecure websites.⁴⁵ By decentralising the collection of personal data, there is an increased risk of data breach in comparison to the, currently offered, redirection option to the COCS on the European Commission secure servers. However, there is a substantial technical difference with the three solutions identified (which affects and increases risk) and it relates to location of the source code of the support collection form. The source code of the API Gateway collection form would be located on the campaigning websites; this will further increase the risk that the European Commission will lose control of the process of collection of statements of support. Furthermore, the decentralised source code is vulnerable to manipulation as the frontend part of this solution will be independent from the COCS backend, and it will only transmit the supporters' personal data to the European Commission storage, or potentially to another data storage set up by the organisers or other malicious actors. The iframe, instead, provides organisers with a 'view' on the COCS frontend part located on the European Commission servers. In this latter case, the source code of the collection form will still be located only on the European Commission servers, and as such there is no transmission of data involved. For all three solutions, personal data collected will still be stored within the COCS backend on the European Commission servers.

The iframe solutions pose a medium-high security risk, while the API Gateway solution poses a high security risk to the personal data of the EU citizens. This study has identified seven major risks for the iframe solutions, while the API Gateway solution presents fifteen major risks. Main security and data protection breaches could be caused by phishing, cross-site scripting, code injection, security misconfiguration, excessive data exposure, mass assignment, etc. These types of risks are explained and detailed in [section 5.2.5](#) above. For all these risks, the study suggests specific mitigation strategies (see [section 5.2.5](#)). Nevertheless, it is important to highlight that **there are no mitigation strategies that can offer the same level of security as the current redirection option of the centralised COCS**, which provides citizens with the possibility of filling in the form with their personal data on the highly secure server of the European Commission. Mitigation strategies, if properly applied, only reduce the risks identified, however, the overall conclusion is that in any of the solutions **the residual risk after mitigation remains high**, because most **organisers have limited technical and security expertise on the risks associated with an embeddable solution**. In addition, most organisers will not be experts, and as seen in interviews, they have limited understanding of the risks associated with the collection of personal data via an embeddable solution. Therefore, the European

⁴⁵ Art. 33 of the Regulation (EU) 2018/1725, on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

Commission cannot base its risk mitigation strategies on trust of the organisers' compliance with the rules.

In addition to the above risks, interviews revealed that some organisers have also decentralised the IOCS support collection form in the websites of partners organisations which were not covered by the certification. Our study has found that risks of data breach increase when the support collection form is decentralised in many other websites that are not audited; these risks also apply to the embeddable solutions identified in this study. Organisers that were interviewed do not seem to be aware of these risks, as they indicated that they trusted the private collection software provided to them, and the fact that the same software has been initially certified by the German certifying authority (BSI), and that their main campaigning website was also certified. However, that certification was issued by the national authority based on the submitted information that the IOCS support collection form would only be hosted on one campaigning website. The national authority was not informed that organisers decentralised the support collection form on other websites.⁴⁶ Further security risks derive from potential misuse and mishandling of the support collection form by organisers, other malicious actors, and the possibility of data being collected in private data storages, a risk that can only to a limited extent be mitigated through an auditing or a certification process. There is also a risk that the other websites, where the support collection form was embedded, were not located within the European Union territory (as mandated by the ECI Regulation⁴⁷) but outside.

One of the organisers has also indicated that the embeddable solution could provide them with the possibility of obtaining, harvesting, and saving supporters' emails, not only to be used in the context of their ECI but also for future and/or other long-term activities. Given the scope limitation in the ECI Regulation, the collection of email addresses for such broader purpose is not allowed as part of the collection of statements of support within the ECI context. It would also require a separate additional consent under the GDPR.

Considering that any of the embeddable solutions will imply a technical change to the current COCS, and personal data/statements of support will be collected via the campaigning websites, if the European Commission would consider implementing one of the embeddable solutions, it will have to produce a yearly security plan (which includes a risk assessment) specific for the embeddable solution to cover the identified risks and mitigation measures needed to address those risks. It will also need to ensure auditing of the embeddable solution decentralised on any campaigning website. Furthermore, for the embeddable solution using the API Gateway, the organisers will need to produce their own security plan, which will need to be regularly updated as well as every time a new risk arises.

6.4. Key Takeaways on the Impact of the Embeddable Technical Solutions on UX

There are three points to keep in mind about UX with embeddable solutions. First, they can be imported in any size. Second, the support collection form can be styled and modified by the organiser while the Iframes are limited to what we allow to. Third, the end user should believe it is part of the website.

First, both the support collection form and the iframe should be able to adapt to most of the current devices. So, the embeddable solution should adapt to computer screens, tablets and the most important one: mobile phones. As a matter of fact, smartphone is currently the most used device in terms of internet browser usage. Almost 50% of website navigations in Europe in January 2023 are done on a mobile device⁴⁸, and that increases every year. This means the solution should be firstly designed for smartphones, then for the other devices, and that's what it is called mobile first design.

⁴⁶ Email sent from the BSI, German Federal Office for Information Security (ECI websites' certification authority) to the Secretariat General on 31 January 2023. (Annex V)

⁴⁷ Art.11 of the Regulation (EU) 2019/788.

⁴⁸ StatCounter. "Desktop vs Mobile Tablet Market Share Europe". Accessed on 31 March 2023. <https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/europe>.

Also, as organiser can choose to implement the embeddable solution in any size. This means that the embeddable solution should be designed in a way that can match the most common scenarios that a web designer would use to implement it in its website. To do that, it would be necessary to interview some organisers (and web designers working for them) and then also compare the embeddable solution with the most popular websites which use forms that look like the support collection form. In this way, it is possible to know the minimum size the embeddable solution should adapt to and the most used size ratio to design the solution.

Finally, it is important to explicitly expose minimum size requirement and best size recommendations to the developers through the solution documentation.

Second point, the support collection form (in the API Gateway solution) can be styled and modified by the organiser and the Iframes are limited to what we allow to. Because the support collection form is part of the organiser website in the API Gateway solution, that means they can do whatever they want to its style and behaviour and that is another reason why we do not recommend this solution.

It is relevant to say that the general design of the solution will define its identity and that identity will be recognised by the final users. At some point, they will be more reassured and confident about using the embeddable solution and to give sensitive information if they recognise it as the one that has been designed by the European Commission.

With the iframe solution, limit can be imposed on the style to the parameters previously defined. In this way the EC will be able to control its visual identity and, at the same time, allow organisers to adapt it a bit to their website's graphic charts. Again, to define which style parameter can be customised, the best approach is to interview some organisers and build a graphic chart for the solution defining how far graphic elements can be changed.

Third point, the end user should believe it is part of the campaigning website. This is the last point to consider, and which may apparently contradict the previous one, is that the end user should not feel like the embeddable solution is suspicious by not fitting well to the rest of the organiser website.

As we saw in the previous point, it is necessary to make the solution customisable enough so it can fit in the most common's website designs. But it should also keep a style and element organisation which keep a certain visual identity.

Everything is about getting the user to easily use the solution and, because it is treating sensitive data, the most safely possible. Here, we are not talking about effective security but the end user's feeling that the solution is safe to use.

6.5. Recommendations on the UX Approach to Succeed in the Implementation

User experience is not only about graphic design of a solution. As defined by ISO 9241-210:2010, UX is "*person's perceptions and responses that result from the use or anticipated use of a product, system or service*". That means UX takes care of everything about the aspect, usage and usability of a product.

To design a great user experience, we must:

- Search about the people who will interact with the embeddable solution;
- Know how they interact with the current solution;
- Find how to improve their experience;
- And finally, co-design the final solution with them.

This is why it is crucial to follow a good UX approach to succeed in the design of the embeddable solution. To do so the following steps are required:

- Define personas and scenarios

A persona represents a group of users who will interact with the embeddable solution. They have needs, they encountered some problems, they may have some contacts with other people, they've got actions and tasks to do, etc. And they follow some steps when they use the embeddable solution. We define all those aspects by interviewing those users.

For the support process, we already identified 2 personas to define:

- The organiser who should integrate the embeddable solution in its website;
- The end user who will use the embeddable solution in the organiser's website.

- Make an experience map by persona

Now that we have identified the personas, we have to understand their interaction with the embeddable solution:

- What are the actions they should do?
- What do they think and feel when doing them?
- The pros and cons of doing it like this
- Is the experience of doing each action positive or not?
- What improvement opportunities do we have to improve each action?

To define all of the above, we use a tool named experience map. It is a document which resumes the interaction of a persona with a product (in this case the embeddable solution) and give a global understanding on what should / can be improved.

- Co-design and sketches

Finally, UX designer will sketch some screen to answer the different problematics encountered by the personas.

This is done during workshops with the users where the idea is to re-think the process through storyboards and then sketch the new solution through an iterative approach.

6.6. Recommendations on the Embeddable Solutions' Auditing Mechanism and Estimated Costs

For all three solutions, in terms of security risk management, the most effective way of controlling security and data protection risks would be to set up a new certification/auditing mechanism conducted by the Member States authorities or by the European Commission, and with a set of technical requirements comparable (but stricter) to the ones previously provided for the IOCS under Implementing Regulation (EU) 2019/1799. As mentioned above, it is important to stress that most organisers have limited technical and security expertise on the risks associated with an embeddable solution. In addition, the European Commission cannot base its security risk management on trust of the organisers' compliance with the rules, therefore, on these premises, we strongly recommend setting up an audit mechanism if an embeddable solution is implemented. The auditing of the organisers' websites and the embeddable solution should be performed every 4 months, during the 12-month collection process (including the initial auditing/certification of the system). However, as indicated by the national certifying authority during the interview, Member States may not have the necessary resources/budget to perform regular audits and/or the certification process if this involves several websites, because the process is very time consuming and costly. These costs, if outsourced to a private company, would require a security expert to work an average of 5 working days per single audit and for each campaign website (this work is estimated at €3,250). In addition, there are the initial costs of the auditing (or the certification) for the embeddable solution before starting the collection of statements of support, which are estimated at €10,000 (one-off costs). The complexity of the auditing and its costs could put an excessive burden on national authorities.⁴⁹ As to contain those costs, it is recommended to allow the embeddable solution only for a limited number of campaigning websites

⁴⁹ Interview with the Luxembourg Government authority, held on 10 February 2023. Evidence attached to Annex IV.

(1 to 3). This limit may however only partially meet the business needs of the organisers. Given that the ECI Regulation currently does not contain such audit and certification mechanism, an amendment of the regulation through the ordinary legislative procedure would be necessary. As a temporary solution, and only for the Iframes' technology, the organisers could sign a personal data joint controllership agreement with the European Commission that specifies the technical, security and organisational measures, as pre-conditions for obtaining the solution. The joint controllership agreement would also contain provisions regarding the regular auditing by the Commission of the organisers' websites. Further, the joint agreement should also tackle the organisers' compliance with the principles laid down in the Decision (EU, Euratom) 2017/46⁵⁰. For the API Gateway solution an amendment of the ECI Regulation would be compulsory before considering any possible implementation. This is a high-risk solution which impacts and drastically change the current COCS, as the source code of the support collection form will be located on the organisers' websites, and not anymore on the European Commission secure servers.

6.7. General Recommendations and Scenarios to Consider for the European Commission

From the above discussion and analysis of the operational management, implementation, costs, security and data protection risks, we have come to the following recommendations in relation to the embeddable solutions identified, in order of preference:

- a) First-best option: Do Nothing;
- b) Second-best option: Consider Implementing the iframe + MicroFrontend;
- c) Third-best option: Do not implement the API Gateway.

Our first recommendation is that "Do Nothing" (hence not offering any embeddable solution), is the best defensible option under this assessment. Maintaining the current system as-is has important benefits, notably that the critical risks associated with the embeddable options are avoided. The European Commission can continue to offer and improve the user-friendliness of the current COCS in its centralised and secure form on its servers. No certification and auditing by a dedicated authority is required. There are no additional associated costs for the European Commission or organisers as the COCS will continue to be offered as a free-of-charge turnkey solution to organisers. The COCS has proven already in its three years of operation to be effective, as two initiatives collected over 1 million statements of support with the current redirection option. Supporters have expressed a high satisfaction rate for the current COCS. Emails and personal data of EU citizens are well protected on the European Commission servers. Following this recommendation would mean that the European Commission would not need to spend substantial costs for implementing and maintaining a very costly solution. "Do nothing" however presents the weakness that no alternative is offered to those organisers that would like to have an embeddable solution on their website to address their needs. This study has not considered alternative options to address those needs, as the research questions strictly focussed on the embeddable solutions as advocated by the stakeholders concerned.

As a second-best option, we recommend the European Commission to consider implementing the iframe with the Microfrontend application solution. It would help to maintain the supporters on the campaigning websites; they can provide their support without being redirected to the European Commission website. Organisers can collect emails at the end of the collection process in compliance with the ECI Regulation. This solution will provide an alternative to the existing redirection option of the COCS. It is a less risky solution than the API Gateway solution. As a matter of fact, given that, as of January 2023, almost 50% of website navigations in Europe are done on a mobile device (and that increases every year), if the European Commission will implement the iframe, we recommend that this solution is designed in first instance for smartphones, and later then for the other devices (mobile first design). Iframes are responsive for mobile, and the iframe first configuration would be organised

⁵⁰ Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission.

by the European Commission on the COCS, but these settings could be edited and adjusted by the organisers according to their campaigning websites.

We have excluded from our recommendations the first iframe solution as it would not bring any benefit in framing the whole COCS within the organisers' campaigning websites, while the iframe solution with the Microfrontend allows only the support collection form to be iframed in the organisers' websites, however, with this solution the organisers cannot gather data analytics, as they could have done with the IOCS or with an API Gateway solution. This iframe solution is costly for the European Commission, which should cover the implementation, maintenance, and auditing on top of the management costs of the COCS. Auditing would also introduce a new role and activity for the European Commission and/or national authorities, and possibly costs for the organisers. However, this solution is less costly than the API Gateway solution, because with this Microfrontend, the European Commission would maintain one application, instead of maintaining several applications like for the API (the API gateway solution requires very technical components like libraries, middlewares, transmission between frontend and backend).

As a third-best option we do not recommend the European Commission to implement the API Gateway solution, because the drawbacks outweigh the benefits of its implementation. First, it will be difficult and very costly for both the European Commission and the organisers to implement and maintain. It is a high-risk technical solution prone to the risk of security and data protection breaches. It presents relevant challenges for the dedicated authorities (Commission or potentially the Member States' authorities) as the solution's source code must be regularly audited to mitigate the most important risks.

This solution also does not meet the expressed needs of organisers that stated that an embeddable solution should be kept as easy as possible to accommodate those organisers with limited knowledge of IT. Of all embeddable solutions, the transmission of personal data via an API Gateway allows the least control by the European Commission before the data reach the European Commission's data storage, thus presenting substantial risks. The purpose of a "transmission" API is to transfer personal data collected by the campaigning sites to the central storage. This solution would pose risks comparable to the ones of an IOCS. A malicious actor could target not only the embeddable solution, the campaigning website of the organisation, but also take control of the personal data of the EU citizens before they are sent to the European Commission servers. In addition, there is a risk that organisers would be able to re-build a new individual collection system just by using the API endpoint as a transmission interface to send the data to the central system; nothing would prevent the organisers to store the data locally before transmitting the information to the central system.

6.8. Recommendations for a Future Viewpoint

In conclusion, while from a technical perspective all solutions are feasible, from a security and data protection risks perspective, **a direct answer to the research questions is that there is not an embeddable solution that can be offered to ECI's organisers that ensures the current level of security and data protection currently offered by the COCS solution with the redirection option.** The COCS ensures that the personal data of EU citizens are collected, transferred and stored directly on the secure servers of the European Commission without any third-party interference.

Further, some of the organisers' business needs, like the need to harvest supporters' emails for other purposes than defined under the ECI Regulation, raise concern about the possible misuse of data, and the embeddable solution itself increases the risks of data mishandling and data breach. If the embeddable solution would lead to a data breach, it could also lead to reputational damage for the European Commission and the ECI instrument. Although there are mitigation strategies for the risks reported, it is very unlikely that organisers will have the necessary skills and the capacity to set up and implement proper mitigation strategies, and acquiring them through external providers will involve substantial costs. Therefore, we estimate that the residual risks, even with the mitigation strategies in place, will be still high. Consequently, an embeddable solution is unlikely to be as secure as the current COCS fully hosted in the European Commission premises.

If an embeddable solution is offered to organisers, the European Commission will need to bear (most of) the high costs associated with the development, the maintenance, the operation, and the auditing of the embeddable solution.

On a cost-benefit analysis, major red flags not to implement an embeddable solution would be the risks of data breach, the high costs to mitigate these risks, the reputational damage resulting from a data breach, the significant cost for the European Commission in financial terms and in terms of operational resources necessary to implement and maintain the embeddable solution. Furthermore, the embeddable solution may also have a limited impact and benefit on the supporters' journey to provide their support.

Given the above considerations, if the European Commission would decide to bear the risks and the costs associated with the offering of an embeddable solution, our recommendation would be to consider implementing the "iframe" solution in the format of the Micro Frontend, because it will be a compromise option between the organisers business needs, and the European Commission's concern for security and personal data protection risks. **This solution, however, poses a medium-high security risk of a data breach, and only offers limited security** under the pre-condition that proper security risk management is in place for both parties, the European Commission and the organisers. Therefore, **this solution should be implemented only after a careful consideration and a full cost-benefit analysis.**

Bibliography

Books

- (2008). Pearson's Correlation Coefficient. In: Kirch, W. (eds) *Encyclopedia of Public Health*. Springer, Dordrecht.
- Boslaugh, Sarah. (2012). The Pearson Correlation Coefficient. In S. Boslaugh. *Statistics in a Nutshell* (Chapt. 7). O'Really Media.
- Chin-Chung, Chao. (2018). Correlation, Point-Biserial. In Mike Allen (ed.) *The SAGE Encyclopedia of Communication Research Methods*. (pp 270-272) SAGE Publications.
- Daniel, Johnnie. (2012). Sampling Essentials: Practical Guidelines for Making Sampling Choices. (pp 87-92). SAGE Publications.
- Saldana, Johnny, (2015). *The Coding Manual for Qualitative Researchers*, 3rd ed. Arizona State University, USA: Sage Publications.
- Yuen, P.K. and Vincent Lau. (2003). *Practical Web Technologies*. (pp. 34). Addison Wesley.

EU Law

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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.
- Regulation (EU) 2019/788 of the European Parliament and of the Council of 17 April 2019 on the European citizens' initiative,
- Implementing Regulation (EU) 2019/1799 of 22 October 2019 laying down technical specifications for individual online collection systems pursuant to Regulation (EU) 2019/788 of the European Parliament and of the Council on the European citizens' initiative

Websites

- Adsero Security. "So what exactly is a security risk assessment". Accessed on 5 April 2023. <https://www.adserosecurity.com/security-learning-center/what-is-a-security-risk-assessment/>
- Angular. "Introduction to Angular concepts". Accessed on 14 March 2023. <https://angular.io/guide/architecture>
- Github. "API Security – Top Ten". Accessed on 20 March 2023. <https://github.com/OWASP/API-Security/tree/master/2023/en/src>
- Mozilla. "<iframe>: the inline frame element". Accessed on 23 February 2023. <https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe>

NIST. "Security Control Assessment". Accessed on 5 April 2023. https://csrc.nist.gov/glossary/term/security_control_assessment

NpmDocs. "About npm". <https://docs.npmjs.com/about-npm>

OWASP. "OWASP Top Ten". Accessed on 16 March 2023. <https://owasp.org/www-project-top-ten/>

OWASP. "OWASP Cheat Sheet Series". Accessed on 18 March 2023. <https://cheatsheetseries.owasp.org/>

Ready Campaign. "Risk Assessment". Accessed on 5 April 2023. <https://www.ready.gov/risk-assessment>

Sobers, Rob. (2022, June 22). "Data Breach Response Times: Trends and Tips". Accessed on 18 March 2023. <https://www.varonis.com/blog/data-breach-response-times>

StatCounter. "Desktop vs Mobile Tablet Market Share Europe". Accessed on 31 March 2023. <https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/europe>.

The ECI Campaign. "OpenECI software". Accessed on 8 February 2022. <https://citizens-initiative.eu/openeci/>.

Tutorialspoint. "Node.js – Introduction". https://www.tutorialspoint.com/nodejs/nodejs_introduction.htm

W3C. "HTML & CSS". Accessed on 22 February 2023. <https://www.w3.org/standards/webdesign/htmlcss>

West, Mike. (2021, March 23). "Content Security Policy: Embedded Enforcement". W3C. Accessed on 19 March 2023. <https://w3c.github.io/webappsec-cspee/#:~:text=Content%20Security%20Policy%20is%20a,content%20loaded%20in%20via%20iframe%20>

Communication

Email sent from the BSI, German Federal Office for Information Security, certification body, authority to the Secretariat General on 31 January 2023

Research Team - Biography

Project Director: Edouard Dumonceau

Edouard is the Director Consulting & Cybersecurity for EU and Public Sector at Sopra Steria Benelux. He has more than 15 years of professional experience as Project Director and Project Manager for EU and International Organisation projects covering public policy, finance, and digital transformation domains. Edouard acted as a Project Director in this study, supported the Project Manager in securing resource availability, sponsorship, and interactions with the customer. He has performed countless assignments for the European Institutions, according to relevant project management and reporting methodologies, through which he has acquired a solid understanding of the project cycle management of Commission services. He has experience in project and portfolio management, product/service planning, risk management, and stakeholder management. He has overseen several projects in the interoperability domain by working with different DGs of the Commission and can confidently manage project forecasts, ensure quality of deliverables, and mitigate risks through his expertise in PM² methodology and project management of similar projects.

Project Manager/Business Analyst: Cristian Talesco

Cristian has expertise as Project Manager in academic and public sector - digital transformation in the EU and Asia. He is a core team member of the EHDS study, DG SANTE. In addition, he has recently successfully delivered the Study on Technical solutions for the European Citizens Initiative for DG DIGIT. Cristian has worked for the ISA² Monitoring and Evaluation Action of DG DIGIT, where he was responsible for monitoring the budget expenditure of the 54 ISA² actions by applying the earned value management method and has also delivered perceived quality and utilities reports. Cristian holds a PhD in Social Development and International Relations from the Hong Kong Polytechnic University (Hong Kong).

IT Architect: Antonio Marco Monteagudo

Antonio has 6 years of experience as a software developer in the Digital Service Centre in Sopra Steria Spain (DSC) of which the last two years he has been IT Architect supporting projects in various sectors such as insurance, banking and retail giving technical support and creation of project's architectures especially in the frontend part of the applications. He has specialized in programming languages such as Angular, React and Ionic for the frontend part of applications and for the backend part he has worked with Java and NodeJs.

Security Expert: Arsenio Perez Gavira

Arsenio is Head of Cybersecurity in Sopra Steria Spain and has cumulated 15 years of experience in security/cybersecurity. He did a Security Audit for certification in National Security Spanish Scheme and ISO27001. Before that, as a Security Consultant and then as a Vulnerability Service Manager and Identity Service Manager, he controlled and managed the vulnerabilities of systems and secured PCs in Telefonica Spain. Moreover, he has certifications on encryption. He has also done scouting cybersecurity startups to "fill in gaps" to update actual product/services. He was responsible for evaluating the security of the As-Is ECI solution infrastructure and ensure that the To-Be state was secured.

Data Protection Expert: Domenico Orlando

Domenico has five years of experience as a legal consultant in data protection law and cybersecurity matters. He obtained an LLM in ICT Law from the University of Oslo and wrote his dissertation on the emerging principle of Security by Design in the EU legal framework. Before joining Sopra Steria, he worked as an associate researcher at the Centre for IT and IP Law, KU Leuven, where he conducted research on legal requirements, data protection impact assessments (DPIA), and Privacy and Security by Design. He is a Certified International Privacy Professional (CIPP/E) and an ISO 27001 Lead Implementer.

In this project, Domenico supported the IT architect and security expert in web applications to ensure compliance with GDPR, Regulation (EU) 2019/788, and the general EU legal framework on security

and data protection. He assessed data protection and operational risks, taking into consideration the personal data processed throughout the life cycle of an ECI.

Frontend Developer/UI Designer: Cyril Lefebvre

Cyril has strong knowledge of frontend development and frontend frameworks evidenced by his involvement in numerous projects for the EC including the ECHA. Cyril, as a senior frontend profile, with proven experience in the use of front ends technologies will support Tim to analyse the advantages and limitations for embedding the technical solution to partner websites.

List of Annexes

Annex I - Work Plan and Project's Objectives

The project was organised around the following two tasks with project management as a horizontal task as illustrated in the Figure 8 below:

- Task-01: Project Management;
- Task-02: Produce the Study.

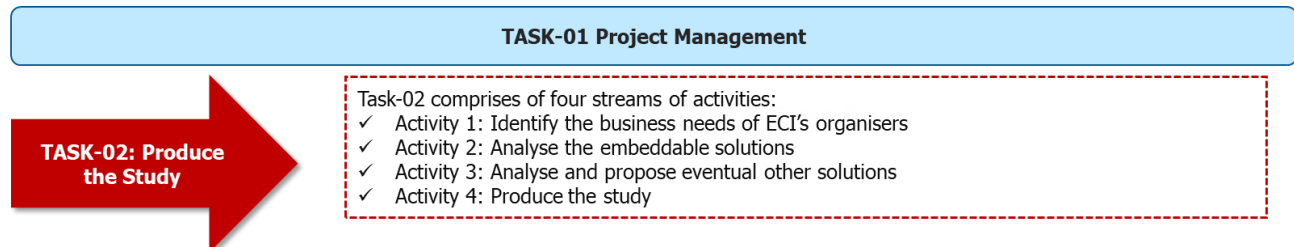


Figure 8: Project Tasks

The four streams of activities were organised over a period of four months, with specific objectives related to each activity. The objectives to produce the study are the following:

Objective 01 – Data Collection: To survey relevant existing documentation on ECI through desk research and literature review. Produce a SWOT analysis of the embeddable technical solutions identified. Draft the questionnaire with stakeholders and draft inception report.

Objective 02 – Analysis and Consolidation of Data: To consolidate the outcome of data collected via interviews with stakeholders. Analyse the embeddable solutions proposed in detail, and the risks associated with the support collection process if any of the solution is implemented. Draft Interim Report.

Objective 03 – Draft Final Report: To draft the final report with the full results of the different analyses and assessments and provide realistic recommendations for the to-be state.

Objective 04 – Final Report: To submit a final report which fully reflect the European Commission comments, together with a power point presentation and an executive summary.

The overall approach taken for the project implementation is structured around the objectives and schedule presented in the Figure 9 below:

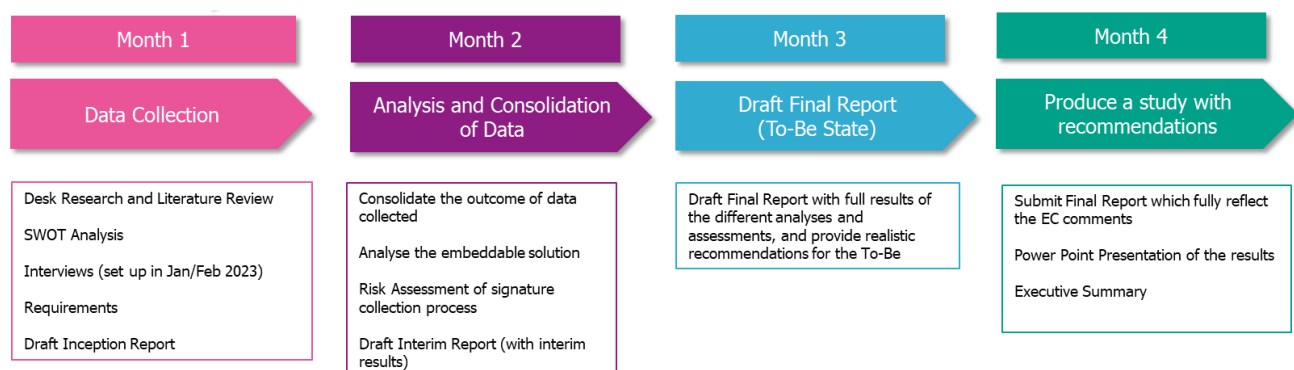


Figure 9: Project's Objectives

Final Report

The project work plan is organised over a period of four months (17 weeks). The full project schedule is shown in figure 10 below. During this period weekly technical meetings have taken place between the contractor and the European Commission. These meetings specifically addressed the above described four streams of activities, and their related objectives.

On a monthly basis the contractor reported on the project progress report, by submitting a project status report which highlighted the main decisions taken in the previous month, and the risks identified, and actions taken. There is a closing meeting during W17 of the project where the contractor presents the final project status report.

In relation to Task 02, the below Gantt chart reports on the progressive stages of the study, with deadlines proposed at W5 for the Inception Report, at W9 for the Interim Report, at W13 for the first draft of the final report, and at W17 for the final submission of the final report, together with a power point presentation and an executive summary.

For the data collection process, interviews with relevant stakeholders are organised between W4 and W7, with some flexibility according to the stakeholders' availability.

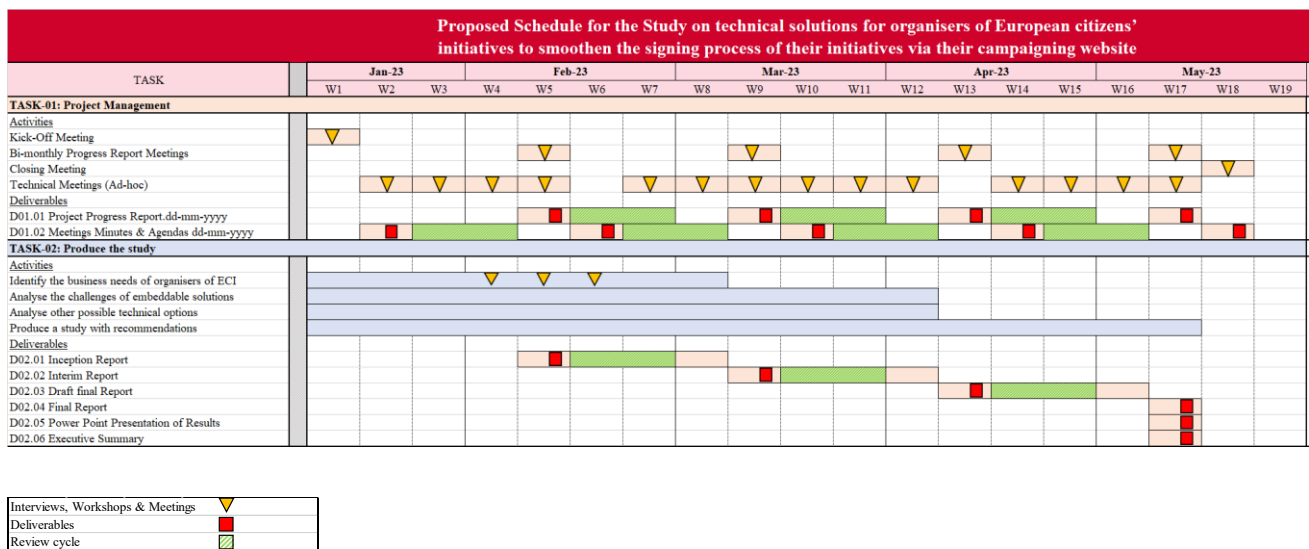


Figure 10: Project Schedule

Annex II - Risks Matrix





This project is using the PM² Risk Likelihood/Impact Matrix, as following:

The risk level is calculated by the product of likelihood and impact in the following way:

Table 19: Risk Likelihood/Impact matrix

		Impact			
		1=Very low	2=Low	3=Medium	4=High
Likelihood	5=Very high	5	10	15	20
	4=High	4	8	12	16
	3=Medium	3	6	9	12
	2=Low	2	4	6	8
	1=Very low	1	2	3	4

Legend:

	Risks can be accepted, contingency plans may be developed.
	Risks cannot be accepted, a risk response strategy should be developed (avoid, reduce, transfer/ share)
	Unacceptable – immediate risk reduction or avoidance response
	Risk appetite

Annex III - ECI's Stakeholders' Questionnaire

Q.1. Could you please explain why it is important for organisers to have an embeddable solution on their initiative websites? Did you consider other solutions?

Q.2. Do you think the European Commission (EC) should offer an embeddable solution for the frontend part of the signature collection process?

<input type="checkbox"/> Yes	<input type="checkbox"/> No
------------------------------	-----------------------------

2a. If "yes" at question 2, please explain why and elaborate on what should be the main features (functional and technical) that such an embeddable solution should offer?

2b. If "no" at question 2, please explain why:

Q.3. Three embeddable technical solutions are presented in Table 1 above, according to your needs what would be the solutions that you would recommend for implementation? Could you please explain your choice?

Q.4. Would you propose any other technical solutions than the ones presented above to be considered for this study?

Q.5. Do you see any risks in the implementation of the above solutions regarding security, data protection and/or any other risks?

<input type="checkbox"/> Yes	<input type="checkbox"/> No
------------------------------	-----------------------------

5a. If "yes" at question 5, please elaborate on the risks identified. What measures would be needed to mitigate those risks? Who would be best placed to implement those measures?

5b. If "no" at question 5, please explain why:

Q.6. Could you provide an assessment of the impacts that an embeddable solution can have on the management of your initiative, in terms of costs or any other impact you can think of? Please explain the types of impacts, and if these impacts are negative, could you please explain how you would mitigate them?

Annex IV - ECI's Stakeholders' Answers

Answers: Centre des Technologies de l'information de l'État Luxembourg

Stakeholder - Introduction	
Name of Organisation:	Centre des Technologies de l'information de l'État – Luxembourg (CTIE)
Type of Organisation:	Member State Authority
Name of Respondent:	Mr Lionel Antunes
Date of the Interview:	10 February 2023
Background and Relevance:	Mr Antunes is the head of internal audit at the Luxembourg's Government IT Centre (CTIE) and Luxembourg's representative in the ECI Expert Group. He provided answers to the questionnaire as an external stakeholder that has been supervising the certification of online collection systems and validation of statements of support since 2012, and who has therefore been in contact with organisers of European Citizens' Initiatives (ECI). During the whole duration of the first ECI Regulation, the CTIE has certified 42 online Collection Systems, reviewed the security plans and risk assessments submitted by 42 groups of ECI's organisers, and verified the statements of support for 14 ECIs.

General Assessment

Q.1. Could you please explain why it is important for organisers to have an embeddable solution on their initiative websites? Did you consider other solutions?

Answer 1:

First, I am not the best person to answer this question, which is more directed towards ECI organizers. However, in my view the first question to ask would be: is it important for organisers to have an embeddable solution?

The debate between an individual and a centralised collection system had been ongoing since 2012.

Following the entry into force of the first ECI Regulation (2012) and the initial difficulties faced by organisers to set up an individual online collection system, organisers asked the European Commission to provide a hosting solution. The European Commission agreed to this request and chose Luxembourg to host their Online Collection System. At CTIE, we have certified 42 Online Collection Systems hosted by the Commission that received more than 10 million statements of supports. We did not receive complaints from organisers about the online collection system hosted by the Commission, so our assumption is that the Online Collection System of the European Commission is fulfilling their needs.

Moreover, we have observed that the Commission has been continuously enhancing their OCS software along the years, based on requests from organizers, for instance by improving the user experience, integrating social networks, adding email collection and campaign features, etc. Finally, the results of a satisfaction survey recently presented by DIGIT at an ECI Expert Group meeting also seem to indicate that a large majority of users are happy with the Central OCS.

Since 2012, I have also seen alternative collection systems to the European Commission Online Collection system being used, including for successful ECI campaigns. However, with Individual Collection systems the security of the collected personal data is a major concern for me. In my view, and based on our in-depth evaluation of the Commission's OCS software and hosting service, the use of the Central Online Collection system is limiting those risks.

To the best of my knowledge, the use of embeddable solutions or the individual collection system is not a general need of all organizers, and I don't believe that it is critical for the success of the European Citizens' Initiative instrument. As demonstrated by all successful campaigns based on the Central Online Collection System, this solution can satisfy the functional needs of the organizers. It also provides the highest guarantees in terms of data protection and security, because it is bound to the IT security policy of the European Commission that can manage and control all the ECI IT Ecosystem. It also frees the organizers of the liabilities associated with storing and managing a large amount of personal data.

In relation to the three embeddable solutions identified, I consider that they are quite complete and that they cover all the possible technical approaches that I am aware of. The issue at stake is again individual vs centralised system, which we have both tried, and we now have an intermediate hybrid solution being discussed. The ECI Regulation in 2019 progressively removed the first approach (individual), and as far as I know there were no major complaints from ECI organizers. Based on the information I have, I believe that most organisers and users are happy with the Central online collection system.

Q.2. Do you think the European Commission (EC) should offer an embeddable solution for the frontend part of the signature collection process?

<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
------------------------------	--

2a. If "yes" at question 2, please explain why and elaborate on what should be the main features (functional and technical) that such an embeddable solution should offer?

2b. If "no" at question 2, please explain why:

Answer 2:

In my opinion, the European Commission should not offer an embeddable solution.

First, as explained before I think this approach would introduce new security risks, which outweigh the potential benefits for organizers and signatories.

I believe that the hybrid solutions may potentially be even more risky than the previous individual collection system if they are not bound to strict requirements through an implementing regulation. Until now, both individual and central online collection systems had to be certified according to (EU)1179/2011 or (EU) 2019/1799, but under the current legal framework, an hybrid approach could leave some technical components out of all control and without review. Therefore, in my view, any technical proposal for a hybrid approach should come with a set of security requirements, which would have to be independently evaluated before opening an online collection system to the public.

Further, this discussion is reopening a debate we have had for 7 years about centralized vs decentralized approaches. After similar studies by the Commission on this topic in 2015

and 2017, as well as a public consultation to prepare the revision of Regulation (EU) 211/2011, this debate was closed with Regulation (EU) 2019/788, which decided to go towards a centralized system. Now, we are again challenging the decision of centralizing the collection of statements of support with a hybrid solution, and it is not clear for me why the conclusions of the previous discussions on this topic would be invalid today.

Q.3. Three embeddable technical solutions are presented in Table 1 above, according to your needs what would be the solutions that you would recommend for implementation? Could you please explain your choice?

Answer 3:

From a technical perspective, I think the table actually presents two fundamental approaches (iframe and API), TS02 being just an improvement on TS01 regarding accessibility and usability.

Technically speaking, an API is the most modern approach of the two, but in this specific case I believe it is probably the worst solution, because it is the one that offer the least control before the data reach the EC data storage. For me, TS03 is not a real "signatures collection" solution, because the backend of the Central Online Collection System would really offer a "transmission" API, whose purpose would just be to receive information sent by the campaign sites.

Contrary to an iframe approach, in an API approach the personal data would not be any more directly submitted by the citizens to the Central OCS, but it would be first collected by the campaign sites and then transmitted to the Central OCS. For me this makes a big difference both from the technical and legal perspectives.

The Iframe approach also present security risks, like spying, code injection, etc.

Q.4. Would you propose any other technical solutions than the ones presented above to be considered for this study?

Answer 4:

The three proposed solutions capture the two overall possible approaches, which are embedding a component provided by the Commission in the collection sites, or using an API towards the Commission's Central OCS. There are multiple technologies and standards to implement these approaches, but fundamentally I do not see another approach than what I see there in the table provided.

Q.5. Do you see any risks in the implementation of the above solutions regarding security, data protection and/or any other risks?

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

5a. If "yes" at question 5, please elaborate on the risks identified. What measures would be needed to mitigate those risks? Who would be best placed to implement those measures?

5b. If "no" at question 5, please explain why:

Answer 5:

Yes, I see a lot of risks.

First, there are non-technical risks related to changing the approach taken so far. The ECI Regulation states that until December 2022, organisers could also use individual solutions to collect signatures, then from 1 January 2023, organisers can only use the Central Online Collection System. So EU citizens were informed of the fact that ECIs could now only be supported on the Central Online Collection System, hosted on the “europa.eu” domain, and that any other website would be illegitimate.

If we now go back and say that any website hosted anywhere could potentially be a legitimate ECI collection site, this would confuse citizens, and it would facilitate the creation of phishing sites. To see a TLS connection to the “europa.eu” domain in a browser is an important marker of a legitimate ECI collection site, which is easily recognizable by EU citizens. When they see this, supporters can be reasonably sure that the connection is safe, and that data can be provided with confidence.

Second, there are technical risks.

For TS03 I already mentioned that for me it is not really a “collection API”, and that the signatures are in fact collected in an uncontrolled environment, which introduces plenty of risks. But TS01 and TS02 also have well-known technical risks associated to the iframe technology. Hackers could for instance use a legitimate Commission’s iframe within a phishing website, which would then spy on the personal data entered in the iframe.

Fundamentally, the problem is that we lose control and observability on what really happens to the citizen’s personal data as soon as we allow collection of signatures outside of a controlled environment such as the Commission’s centralised OCS. Based on our past audits, I consider that the Central Online Collection System hosted at the Commission is secure. On the other hand, I have no idea about the security of independently developed and hosted online collection systems, since the source code was not public and since we have never audited one.

By hosting the collection website, the Central Online Collection System offer extra features to check IP addresses, rate of submission of signatures, browser metadata, etc. These features provide more contextual information that ensure better traceability and better support against fraud. This information would not be available any more with approach TS03, since the Central OCS is not interacting directly with the citizen any more.

Further question from the audience: *“Do you offer API gateways?”*

Answer to the audience question: We have several services that are open to national actors of the public sector through SOAP/REST webservices, but usually they are not exposed on the Internet. Apart from a few exceptions, for services offered to citizens on the Internet, we usually offer a web interface, in general with mandatory strong user authentication. We are currently putting in place a proper API gateway to industrialize the opening of some services by machine usable APIs.

Q.6. Could you provide an assessment of the impacts that an embeddable solution can have on the management of your initiative, in terms of costs or any other impact you can think of? Please explain the types of impacts, and if these impacts are negative, could you please explain how you would mitigate them?

Answer 6:

As with question 1, I cannot really speak about the impact from an organizer's perspective. Also as an auditor and a security person, the risks of misuse of citizen's personal data are my main focus, more so than costs.

Nevertheless, from an operational perspective I think that in terms of the hybrid solutions proposed:

- TS01 has more limited impact as you share the code of the whole COCS, but usability is probably the lowest for signatories.
- TS02 is more demanding – a change of the COCS architecture is needed, but with better usability and user experience.
- TS03 would rely on an API gateway from the EC, so reusing a solution which may not have a big impact on the ECI personnel. However, the operational work for the API Gateway team (distributing API keys, revocation management, access control, etc.) should not be underestimated, and it might be hard to absorb if a lot of websites are used to collect signatures.

Further question from the audience:

"If an embeddable solution is implemented, should we audit the website as the regulation indicated previously? Or audit the code?"

Answer to the Audience question:

Actually Implementing regulation (EU) 2019/1799 covers more than just the collection website, but it also includes requirements on governance, risk management, change management, human resources, etc.

If any of the 3 embeddable approach is chosen, I definitely think that we need to define a set of security requirements to be put in place, and some kind of independent entity to verify that the system of the organisers is secure and compliant with data protection.

In principle, this work could be done by the same national authorities that were in charge of the certification of online collection systems. However if an embeddable solution is implemented on many websites, it could significantly increase the amount of work for certifying these websites: it takes one minute to embed a support collection form, but it requires much more work to evaluate and certify a collection system. If the collection is decentralized on many websites, the amount of work for national authorities to control the security would become unmanageable.

There is another issue that we have observed in practice with audits of individual online collection systems, and which would also be relevant for embeddable solutions. We have seen in the past that some online collection system have been modified after their certification. Since the Regulation does not foresee a supervision of certified systems by national authorities, these changes may have not been noticed by national authorities, and therefore not evaluated from a security perspective. This is another kind of risk that does not exist when using the Central OCS, which has strict rules for change management.

Answers: Fur Free Europe

Stakeholder - Introduction	
Name of Initiative:	Fur Free Europe
Type of Collection System:	Individual Online Collection System (IOCS)
Name of Respondent:	Ms Elise Fleury
Date of the Interview:	13 February 2023
Background and Relevance:	Ms Fleury is a senior campaigner for the Eurogroup for Animals, and one of the organisers of the <i>Fur Free Europe</i> initiative. She provided answers to the questionnaire in her role of ECI's organiser with relevant and direct knowledge of the signatures' collection process. In particular, Fur Free Europe's organisers used the Individual Online Collection system to collect EU citizens' signatures. Ms Fleury was also involved with the <i>Save Cruelty Free Cosmetics</i> initiative as a co-organiser. This latter initiative collected signatures via the Central Online Collection system. Both initiatives were successful in collecting over 1 million statements of support.

General Assessment

Q.1. Could you please explain why it is important for organisers to have an embeddable solution on their initiative websites? Did you consider other solutions?

Answer 1:

For Free cosmetics, I also was co-organiser, but not leading. I could see during that ECI some issues with the collection process. They were using the COCS. While it is easy to collect and submit the signatures with the COCS, supporters were giving feedback saying that the European Commission is seen as a remote institution for citizens. They said that signing on the EC website is seen as an extra obstacle.

Key point. We are a campaign organisation, therefore it is important for us to engage our supporters, so we need to have a portal that has at the forefront our campaign with pictures, etc., but, to be honest, the EC portal is not super-engaging for the organisers. Supporters are reluctant to give ID to the EC website, because they do not want the EC to have their data. Supporters trust the organisations, so they feel more confident to provide signatures to NGOs who they know and have affiliation with.

The fact that you cannot really play with the layout and the signatures collection is on the EC portal, these are two obstacles for supporters to come, stay and sign. In fact, one thing is to attract the people to your campaign website, and another is to keep them on your website and make them act, so signing the ECI you campaign for. For this latter point, it is more complicated to achieve it, if the signature collection is on the EC portal, than if you have a campaign portal with an embedded solution to collect signatures. Secondly, a lot of NGOs get involved in campaigns, and they invest a lot, and it is important to have a return on investment. When you integrate the widget on your campaign website you can ask people to sign up for newsletter, leave their email to be kept informed about the related future activities. These are potential new supporters.

Extra actions in the collection process risk is to lose these supporters, as they have an extra step to provide their signature on the EC website.

Further, with a widget we can extract important information. We can really analyse the activity and where the signature comes from. We can then replicate successful promotion, with similar target action on social media. Running campaigns on social media costs, advertisement, boost etc. We chose the Open ECI system, because we could use their system on the website of other organisations that support us, the big organisations.

The signature collection experience is also about email harvesting, enlarge your outreach to citizens, keep them informed about the related activities of your campaign.. We are used to making petitions, and engagement with the public is crucial, because campaign for an ECI is an expensive choice, but we trust in that, therefore, fundraising, harvesting email, and engaging with the public are all important steps.

In terms of our initiative's success, if we have been successful is not because of the widget choice [OpenECI software], but mostly on the preparation and organisation before going for an ECI.

The widget probably did not make a difference in the number of signatures collected. It depends more on the campaign, than the tool. It is more about having a strong campaign. However, for the ECI on Cosmetics, before redirecting their supporters to the COCS, the organisers asked for their email addresses, but then they realised that they lost some of the supporters for the signatures. Therefore, if an embeddable solution is offered, organisers can ask in first instance for the supporters' signatures and after they ask for their email.

For our initiative, Fur Free Europe, we educated supporters on the data collection process. We made an official video of ECI steps. We developed community management, and we said to the people that it was safe to sign.

It is important for organisers to have the ability to grow your supporters' engagements. Not too many clicks, not redirection, not moving out from the campaign site, but having the widget in your own platform: yes.

Q.2. Do you think the European Commission (EC) should offer an embeddable solution for the frontend part of the signature collection process?

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

2a. If "yes" at question 2, please explain why and elaborate on what should be the main features (functional and technical) that such an embeddable solution should offer?

2b. If "no" at question 2, please explain why:

Answer 2:

Yes, if the EC offers an embeddable solution with the possibility to collect supporters' emails. Yes, if you maintain the supporters in the same environment. People giving emails to the EC may not work. Supporters trust the NGOs they are supporting.

Q.3. Three embeddable technical solutions are presented in Table 1 above, according to your needs what would be the solutions that you would recommend for implementation? Could you please explain your choice?

Answer 3: Not answered. No technical knowledge.

Q.4. Would you propose any other technical solutions than the ones presented above to be considered for this study?

Answer 4: No reply, too technical.

Q.5. Do you see any risks in the implementation of the above solutions regarding security, data protection and/or any other risks?

<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
------------------------------	--

5a. If “yes” at question 5, please elaborate on the risks identified. What measures would be needed to mitigate those risks? Who would be best placed to implement those measures?

5b. If “no” at question 5, please explain why:

Answer 5:

No, because we trusted the software company (Open ECI) they worked with other ECIs previously - so we were not worried about risk. Open ECI is accepted by the European Commission. We trusted the tool, and we knew the rules. We used the OpenECI solution on 30 campaigning websites. We hired OpenECI and we trusted them. Implementation based on trust.

Further question asked from the audience:

“Did OpenECI informed you on the potential risk of using their solution?”

Answer to the Audience question:

Anyone using the widget had to respect the rules. They had the certification of the German Authority so we trusted them.

Q.6. Could you provide an assessment of the impacts that an embeddable solution can have on the management of your initiative, in terms of costs or any other impact you can think of? Please explain the types of impacts, and if these impacts are negative, could you please explain how you would mitigate them?

Answer 6:

The OpenECI solution to collect signatures was not the expensive part. Visual and Social media campaigns are more expensive. The tool should be the easiest possible for supporters.

Answers: the ECI Campaign

Stakeholder - Introduction	
Name of Organisation:	The ECI Campaign
Type of Organisation:	Grassroots coalition of democracy advocates. Provider of the OpenECI software for ECI's organisers.
Name of Respondent:	Mr Carsten Berg (Director), Mr Daniel Pentzlin-Kordecki (Strategy Advisor), Mr Xavier Dutoit (IT Engineer).
Date of the Interview:	14 February 2023
Background and Relevance:	The ECI Campaign is a grassroots coalition of democracy advocates and over 120 European NGOs dedicated to the creation and successful implementation of a European citizens' initiative right. Since 2002, the ECI Campaign campaigned for the legal introduction of the European Citizens' Initiative (ECI). Up until 31 December 2022, the ECI Campaign provided the individual ECIs - that requested their help - with an individual online collection software: the OpenECI software. On 1 January 2023, and in line with Regulation (EU) 2019/788, this individual online collection system was phased out. The ECI Campaign also provides advice to organisers on campaigning, fundraising and legal matters. The coalition provided answers to the questionnaire in their role of ECI's stakeholder with relevant and direct knowledge of the signatures' collection process.

General Assessment

Q.1. Could you please explain why it is important for organisers to have an embeddable solution on their initiative websites? Did you consider other solutions?

Answer 1:

What we learnt is that a campaign website must contextualise the meaning of the campaign with (e.g.) images, videos, text... the campaign website should generate in the supporters, emotional attraction (look and feel). The generation of such sentiment will help the supporters to relate to the ECI initiative, and then they decide whether they want to sign. Images, illustrations, etc, are crucial, we achieve a better engagement rate if they cause emotional attachment, which together with a wide coverage of the ECI initiative on various websites, in multiple language will help the initiative to succeed. Supporters sign because they trust the organisation they are affiliated to.

So, when we say whether an embeddable solution is important, we say absolutely yes. The flow should be to have not only one initiative's page, but many websites. Offer the possibility to everyone that wants to contribute to an ECI initiative to have the possibility to embed the widget on their own websites.

Getting people organised across lingual and cultural borders, provide a Restful API, provide a low code for organisers that have no IT knowledge, therefore, offer to many NGOs to embed the widget in their webpages, and to have the opportunity to share it on social media (e.g.) through friends and partners.

You want people to engage in different way. Have a restful API to integrate and get permission from them to contact them later on is the way to promote the ECI.

For Fur Free Europe, 95 partners and NGOs have shared the widget on their websites. Supporters trust the organisation that is displaying the widget on their website. The supporters' journey is crucial, collecting signature and email to be able to keep in touch.

The COCS, however, is preventing to push further the campaign. NGOs that organise ECIs want to have access to the supporters' emails. The ECI are successful with OpenECI because they grow their own list of contacts.

They care about emails, also after the signature collection process for the follow up. The ECI is not over when the signature collection is completed.

Further, many organisations promote ECI initiatives and have millions of emails stored, like Greenpeace. These organisations are committed to GDPR, and they know how to handle emails. They do not think that the EC system is safer or that provides more trust in the supporter. Their supporters would not trust the EC. European Institutions are far away from citizens.

Emails collected during an ECI campaign are important... think at a journey. Imagine, an Estonian civil rights organisation that has 20.000 supporters. There is an ongoing ECI. They put an ECI widget on their website, supporters reach the widget via an email sent to them. They do A-B Testing. Two emails to different datasets of supporters. The data I have in my database can be re-used to prefill the signature form for the supporter. Then the supporter click on the email, the form will be prefilled with a specific identifier. After, I can see that 80% of email A signed for the ECI, but only 50% of email B signed. I can check which email brought me a higher rate of signatures.

Then some of these supporters promote the ECI initiative via friends, and then they sign. Here we need to have a way, not only to share the URL to a central COCS, but to a webpage where it is embedded the form. Grow overtime the group of people and supporters.

Therefore, through the API provide the possibility to collect email.

Q.2. Do you think the European Commission (EC) should offer an embeddable solution for the frontend part of the signature collection process?

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

2a. If "yes" at question 2, please explain why and elaborate on what should be the main features (functional and technical) that such an embeddable solution should offer?

2b. If "no" at question 2, please explain why:

Answer 2:

Rest API much more flexible. We have IT capacity. But having low code option for organisers with less IT capacity. Having both is better.

Q.3. Three embeddable technical solutions are presented in Table 1 above, according to your needs what would be the solutions that you would recommend for implementation? Could you please explain your choice?

Answer 3 (provided in writing):

This is thought from both the individual citizen and the organisers perspective:

1. An iframe of the COCS as is, is most likely not a viable option and presents neither benefits to individual citizen, nor to organisers. The simple reason: embedding a complete webpage with blocks or models, such as navigation and side panels, is not feasible for most websites, that require minimum standards for user experience and responsiveness to various screen sizes and devices. Integrated workflows are not possible.
2. An iframe of an applet or content block that contains not more than the sign on form, code, if well designed, offer a somewhat satisfactory solution to embedding into responsive webpages. For individual citizen, this is a slight improvement as they don't have to leave the webpage of the organiser and do not have to orientate themselves on a separate webpage. However, without additional functionality for the organisers to adapt the look and feel (CCS etc), such an iframe solution, will always have problems for the user experience. For the organiser, this presents no added benefit whatsoever, as the iframe is still effectively, a firewall between the web application of the organiser and the COCS; as a result, it is not possible to offer any workflow integrations.
3. A rest API, thus, remains the only viable option apart from a third-party application, such as OpenECI. Ideally, it is combined with option two (embeddable COCS applet) to allow organisers with little budget or technical skills to get the COCS frontend functionality on their webpage with low or no coding required.

A restful API poses opportunities and challenges. A key risk that has to be mentioned at this point, however, is central to the COCS itself: the COCS is a centralised endpoint for personal data, making it an attractive target for malicious attacks. A decentralised system for collecting and storing data might be preferable. For example, the 27 member states could offer standardised Apis for data reception and storage. This way the EC wouldn't have to deal with personal citizen data and it's associated risks at all. From an organisers perspective, the COCS API might be done so it could manage direct end to end encrypted data flows from the citizen client directly to their respective member state's endpoint. A member states that wants to, could then be empowered to use a provided application or program, their own application for real time authentication of a signature.

Q.4. Would you propose any other technical solutions than the ones presented above to be considered for this study?

Answer 4:

It is great for organisers to also have their own software, it is good also for the EC as this would promote innovation and citizens' engagements.

Suggest to member state to have their own data storage endpoints via an API and collection point. Decentralising data collection, rather than on the EC. The EC will not have the big data. The Member States gets the data directly and validate it. This also enable Member States to automatically validate the signatures collected. It could be in real time.

Q.5. Do you see any risks in the implementation of the above solutions regarding security, data protection and/or any other risks?

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

5a. If “yes” at question 5, please elaborate on the risks identified. What measures would be needed to mitigate those risks? Who would be best placed to implement those measures?

5b. If “no” at question 5, please explain why:

Answer 5:

We see a data risk for the EC to store all these data for long time. However, in our view, the signature collection process and the risks associated to it, should be considered not from a risk avoidance perspective, but from a risk management perspective. For risk management it is always good to store data decentralised.

Supporters do not sign under a false pre-text. There is always a risk that those technically advanced can inject a code, but overall, the iframe solution is very secure. In 12 years of experience with many petitions, we did not experience any data breach.

Again, we stress more a risk management approach than a risk avoidance approach. But the likeliness that a data breach happens is really low. A very high technical level is necessary to hack the system, and we do not see a rational for doing it for an ECI. The focus is on how to mitigate these risks. All are possible but not fully avoidable, and we can assess the likeliness and the impact, and have a proper risk matrix. With risk management, the EC can create a State of the Art on risk mitigation from a technical point of view.

In terms of risk management, we certify the server that collect the data and explain how the widget work. It is not manageable to certify each website with an embeddable solution. We are speaking of more than 100 websites that embed the widget for each successful initiative.

In terms of reporting to the national authorities the websites that embed the OpenECI widget, we do not know how many partners use the widget. We do not list all websites that embed the widget, as we do not know which websites they will use it.

The OpenECI code and the widget is from Europe. We do not check if the widget is embedded in Amazon US or Amazon Europe (e.g.). It is not relevant for security and the process. The ability to hack a website is not related to where the website is hosted.

It is a good practice to have *Terms of Services* to exclude websites that hosted topics like extremism, violence, etc. if the embeddable solution is implemented. But we store the URL referral of the person signing so we know the place where they signed, we can check if there is something phishy. We rely on citizens to check and advice.

Further, from the backend we can also stop that widget in case on non-compliance with the Terms of Service. Hence, anyone can embed the widget, but it is not the same widget, it is not simple code. It is a line of Javascript that creates an iframe and that comes with

an identifier. This allows us to selectively switch on and off the widget from specific websites. The EC could do something similar with an API and an embeddable widget.

Risk management process documentation and the terms of services, legally, oblige the organisers to follow a certain procedure. If there is a problem with a widget embedded somewhere, there must be guidelines on how to act, like 2-3 days to stop the widget.

If we were to develop this, in the iframe apart from the form, we would say that the data goes to the EC. If with an API, we would add an extra field, explaining where the data goes (e.g. email). Finally, we would like to be able to log in the backend, use the URL, identify the widget non-compliant and block it.

Q.6. Could you provide an assessment of the impacts that an embeddable solution can have on the management of your initiative, in terms of costs or any other impact you can think of? Please explain the types of impacts, and if these impacts are negative, could you please explain how you would mitigate them?

Answer 6:

We see only benefits, not costs.

The costs more for the development and keep the system up-to-date - with real big advantage.

An embeddable solution for civil society organisations: you have a webpage and you can embed a YouTube video then you can also embed these widgets also.

For the organisers no difference in costs in allowing third parties to embedding or iframing the ECI. Costs can also be mitigated.

Answers: Stop Finning – Stop the Trade

Stakeholder - Introduction	
Name of Initiative:	Stop Finning - Stop the Trade
Type of Collection System:	Central Online Collection System (COCS)
Name of Respondent:	Dr Nils Kluger
Date of the Interview:	17 February 2023
Background and Relevance:	Dr Kluger is the spokesperson and coordinator of the European Citizens' Initiative, <i>Stop Finning - Stop the Trade</i> . He provided answers to the questionnaire in his role of ECI's organiser with relevant and direct knowledge of the signatures' collection process. This initiative was successful in collecting over 1 million signatures from EU citizens. The organisers of this ECI used the Central Online Collection system to collect the statements of support.

General Assessment

Q.1. Could you please explain why it is important for organisers to have an embeddable solution on their initiative websites? Did you consider other solutions?

Answer 1:

It is absolutely important. What we are doing during the campaign of an ECI is to attract supporters. They get attracted from somewhere and then they click and get to the campaign website. The website gives information to the supporters. Google analytics tells us that a supporter after 3-4 minutes reading click on vote, but with the COCS people get confused because they move to an external online collection system, which is very different from the ECI campaign website. Supporters were not happy with redirection, and that cause irritation.

We could have organised social media campaigns, where we could have put a link directly to the voting page of the COCS, but in that case we could not have the supporters first on our ECI campaign website. Therefore, we could not have provided our supporters with more context on our ECI initiative, and we could not have shown more information to them. This latter point is very important.

We used the COCS, but we would have preferred to have an embeddable solution.

Q.2. Do you think the European Commission (EC) should offer an embeddable solution for the frontend part of the signature collection process?

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

2a. If “yes” at question 2, please explain why and elaborate on what should be the main features (functional and technical) that such an embeddable solution should offer?

2b. If “no” at question 2, please explain why:

Answer 2:

Yes, it is clearly yes. Supporters should easily provide their vote. They are irritated to be redirected. Obviously, they do not know the central online collection system, further they do not trust the EC platform. Supporters question why they have to leave data to the EU, when

they are signing for a ECI campaign in which they believe in. We got this feedback, not hundreds of complaints, but we got them. Sign on the campaign website would solve this issue.

Supporters do not know the Europa website. You have to explain that the COCS is a trustworthy and official website. But, as organisers, we have already the problem of explaining and promoting the campaign, only 2% of European citizens know the ECI. In addition, we have another issue to explain, that the signatures are stored in an external website run by the EC.

A critical problem is that the EU citizens do not know the Europa website, as being an EU official website.

However, we understand that if an embeddable solution is implemented, personal data would still be stored in the EC backend part of the COCS. In my view, this is a drawback of installing an embeddable solution: embed and explaining that data are stored by the EC. This is a drawback, but have the collection of signature on the organisers website and explain that data goes to the EC and are protected by GDPR and are safe, should be enough to guarantee them. Keep the embeddable solution as easy as possible.

Q.3. Three embeddable technical solutions are presented in Table 1 above, according to your needs what would be the solutions that you would recommend for implementation? Could you please explain your choice?

Answer 3:

TS01 and TS02 appear the easier solutions to install for organisers. Keep it simples for organisers. I would go with solutions 1 and 2. That would be enough. Many organisers lack IT knowledge.

Q.4. Would you propose any other technical solutions than the ones presented above to be considered for this study?

Answer 4:

Integrating an ECI into well-known petition platforms to support the collection process. These platforms have a good reach. It is very problematic to fit into their own system. They want to have the data of the people on their platforms, which is problematic. ECI can be promoted using these platforms, as they promote direct democracy. These platforms could promote the ECI as well.

Q.5. Do you see any risks in the implementation of the above solutions regarding security, data protection and/or any other risks?

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

5a. If “yes” at question 5, please elaborate on the risks identified. What measures would be needed to mitigate those risks? Who would be best placed to implement those measures?

5b. If “no” at question 5, please explain why:

Answer 5:

It is important to make organisers aware of risks. If they embed the code in their campaigning website they must be aware that their website is at risk. These risks are not just related to hacking, but they need to handle lots of wave of supporters. So, their website can go down if there is an increasing traffic. It is important to help organisers not to be trapped in this excessive traffic. The system can crash with 100.000 visits in a day. This is what happened to our campaigning site that crashed when we received a high number of visitors. If we would have had an embeddable widget at that time, this would have prevented the citizens to provide their signatures. This is the reason why if an embeddable solution is put in place, the European Commission will need to provide advice to the campaigners to make sure that they have a scalable contract with their providers to sustain waves of signatures.

Q.6. Could you provide an assessment of the impacts that an embeddable solution can have on the management of your initiative, in terms of costs or any other impact you can think of? Please explain the types of impacts, and if these impacts are negative, could you please explain how you would mitigate them?

Answer 6:

The scope is to bring everybody to vote. With an embeddable solution all process for the supporters becomes streamlined, but with the COCS you have to do one more click to vote. It is crucial to better plan the campaign within an ECI, and better coordinate and manage your supporters with an embeddable solution.

An embeddable solution would provide more signatures than the COCS. Organisers can handle risks. We need to promote the ECI more. And the key question to bear in mind is: Who attracted the supporters to vote? Was the EC? Or is it the organisers? The ECI partners? The campaigners? The supporters are attracted by the campaigners/organisers, not the EC. They want more information on the ECI website and they want to directly sign on the ECI campaign website.

Annex V - Email sent from the German Federal Office for Information Security to the Secretariat General on 31 January 2023

From: #####@bsi.bund.de
Sent: Tuesday, January 31, 2023 12:20 PM
To: #####@ec.europa.eu
Subject: AW: European citizens' initiative - online collection systems - Your feedback on embeddable options on campaigning websites - Ares(2023)673944

Dear #####,

regarding the individual online collection systems certified by BSI, we have no information about the use of widgets to sign initiatives by ECI organizers. Neither did the evidence provided to us during the certification procedure(s) contain any information regarding the use of widgets nor did organizers notify BSI during the following collection period about planning to or having added interactive widgets to their online collection systems.

The BSI certification only covers the online collection system accessible via the URL stated on the certificate. Anything beyond that is out of scope and not covered by the certification. Same applies if information about certain features that might have been withheld during the certification procedure.

If organizers plan to perform changes to their OCS or to add features (like widgets) after certification, it is within their responsibility to indicate these to BSI and provide suitable evidence ensuring that the requirements of the ECI Regulation and the technical requirements are still met. BSI will then review and evaluate the information provided.

In our understanding collecting signatures and personal data via additional sources, URLs or widgets can only be permitted if conformity to the requirements of the ECI Regulation and the technical requirements is ensured for these features as well. This might require organizers to provide the same evidence as for the initial certification, but this has to be evaluated by the case. (for the list of evidence that had to be provided to BSI during certification see our documented procedure -> https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Europaeische-Buergerinitiative/Verfahren/verfahren_node.html).

Notwithstanding the above please take note that according to article 11(7) of Regulation (EU) 2019/788 certification of individual online collection systems by national competent authorities was only possible for initiatives that have been registered by the Commission by December 2022, with the effect that the competence and involvement of BSI in the area of ECI and the certification of individual OCS has ended as of 2023.

Best Regards,

#####

the Certification-Body of BSI

Section SZXX - Certification according to Technical Guidelines
Federal Office for Information Security

#####, GERMANY
Telephone: +49 #####
E-Mail: #####
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

All informationen regarding the handling of your personal data can be found at
https://www.bsi.bund.de/DE/Service/Datenschutz/datenschutz_node.html