
# Study on data requirements for the European Citizens' Initiative

*Final Report*

22nd September 2017

Submitted by Optimity Advisors under Framework contract no JUST/2015/PR/01/0003 on Supply of Impact Assessment, Evaluation and Evaluation related services in the policy areas – Lot 1

Prepared by Optimity Advisors and Tipik Legal



**EUROPEAN COMMISSION**

Secretariat General
Directorate C — Smart Regulation and Work Programme

Unit C4 – Work Programme and Stakeholder Consultation

*E-mail:* sg-unite-C4*@ec.europa.eu*

*European Commission*
*B-1049 Brussels*

# Contents

# I. Executive Summary

## I.1. Introduction

Optimity Advisors was contracted by the European Commission's Secretariat-General to carry out a Study on data requirements for the European Citizens' Initiative under Framework contract no JUST/2015/PR/01/0003 on Supply of Impact Assessment, Evaluation and Evaluation related services in the policy areas – Lot 1.

## I.2. Problem Definition

The primary premise of this study is that the current ECI data requirements are impacting the progress of ECIs and that further optimisation of these requirements, and the mechanisms surrounding them is possible.

### I.2.1. Policy objectives

The study aimed to follow the operational policy objectives as laid out below:

- To simplify the data requirements for signatories of statements of support (proportionally to the outcome);
- To ensure all eligible EU citizens are able to support an ECI;
- To ensure only eligible citizens are able to support an ECI while minimising the burden of verification;
- To ensure that the personal data of supporters is safeguarded.

### I.2.2. Scope and Methodology

The key study objectives include the provision of insight on the following points:

1. the **sensitivity of the ECI's data requirements**, and the related mechanisms and processes, in light of similar national or regional participatory instruments;
2. the **scope and possible options for simplifying these data requirements**, and the related mechanisms and processes, also in light of national level systems; and
3. the **data protection environment in which the ECI operates** presently, the foreseen environment after the General Data Protection Regulation (GDPR) enters into force, and any challenges posed in this respect.

In order to exhaustively address these three objectives, it has been necessary to collect extensive data on the implementation of the ECI across the Member States, as well as the implementation of similar national or regional participatory instruments, and highlight:

- the **best practices** and **challenges** relating to the ECI data requirements, in terms of: the data required of signatories at step 4 of the ECI process (i.e. collection of statements of support); the mechanisms used to verify statements of support; and issues related to the sensitivity to provide data;
- the **types** of similar national or regional participatory instruments in existence at national level, the **best practices** employed by these instruments and the possible **applicability** of a number of these practices to the ECI, in light of the objectives to simplify the data requirements; and
- the likely **impact of the GDPR** on the processes and mechanisms used to implement the ECI.

The information provided in this study was drawn using the following research tools:

- Desk research / evidence review exercises

- Interview programme
- Risk assessment
- Comparative analysis
- Case study analysis
- Country fiche

## I.3. Data sensitivity and the General Data Protection Regulation

The issue of "data sensitivity" is relative. The issue does not simply relate to the question of whether certain data are, in general or in certain countries, seen as inherently 'sensitive'. The question of 'sensitivity' is closely linked to issues of data security, as perceived by potential supporters of an ECI. The extent to which they are reluctant to provide certain data, such as ID numbers or ID document details, depends on the context in which they are asked for these data, and the identity of the entity to which they are disclosing the data.

Regarding the personal data that European citizens are reluctant to provide, the results of the Public consultation on the European citizens' initiative confirm the varying importance of the type of potential sets of personal data as well across Member States. The public consultation illustrates that over 58% of those who responded, across all Member States, would be unwilling to provide their driving license number, over 49% would be unwilling to provide their personal identification number, 37% would be unwilling to provide the last three digits of their personal identification number or driving license, which is followed by 33% who would be unwilling to provide their place of birth. Importantly to note, whilst 28% of respondents would be unwilling to provide their address when giving their support to an ECI, 30% expressed a willingness to provide all the types of personal data examined (personal identification number, driving license number, the last three digits of their personal identification number or driving license, place of birth, address, name at birth, email address, date of birth, name, nationality).

Variations have also been observed depending on the country of citizenship of the respondents. In particular, within 7 countries (Bulgaria, Croatia, Estonia, Latvia, Poland, Spain and Portugal), Address was the most common type of data respondents were unwilling to provide and in 2 additional countries (Italy, Cyprus), Address was the second most common after the driving license number.

However, there have been only a few formal assessments of the ECI processes by data protection authorities. The European Data Protection Supervisory (EDPS) has assessed the provisions as set out in the original Commission proposal for the ECI Regulation but not the final provisions of the Regulation. In any processing of personal data related to ECIs, the national authorities involved – the authorities in charge of certifying online collection systems, the authorities in charge of verifying statements of support and the other public bodies involved in this verification – are subject to their own national data protection laws and, in relation to the GDPR, to that instrument and any national rules implementing provisions of that instrument that allow the Member States to define the application of those rules more precisely, and to any further, special data-related restrictions imposed by the ECI Regulation. The Commission is in this regard only subject to Regulation (EC) 45/2001 and the special data-related restrictions in the ECI Regulation.

Organisers are also bound to comply with data protection legislation as regards the statements of support they collect.

The situation of organisers is more complex than for the other actors involved in terms of applicable law, and because there will still be differences between the Member States, even after the GDPR comes fully into force in May 2018, this causes difficulties.

It would therefore be better if any revised version of the ECI Regulation could expressly stipulate the applicable law for any processing of personal data by ECI organisers within the ECI process. The liabilities of the entities involved in ECIs – organisers, certification authorities, verification authorities and other national bodies involved in verification (such as municipal authorities) and the Commission are limited to their respective processing.

However, there is no need for an open-ended, wide, not-data-protection-related liabilities clause (such as is now contained in the ECI Regulation). If some wider (not data protection-related)

liabilities are to be retained, they should be strictly circumscribed and limited to clear civil wrongs (F: *faute*; D: *unerlaubte Handlung*) with appropriate culpability.

As regards the implications of the entry into force of the GDPR, if organisers are given practical guidance on how to perform the tasks required under the GDPR, and follow that guidance, they should be in a position to fulfil their obligations under the GDPR; whereas for the other national actors involved in ECIs (certification authorities, verification authorities and other national bodies involved in verification), the GDPR does not impose any burdens over and above what they, as public authorities, are already under in relation to any processing of personal data by them.

## I.4. Conclusions

Regarding the ECI data requirements, a term which encompasses the data collected through statements of support as well as the data used to verify the same statements of support, a wide range of **challenges appear to limit the simplicity and efficiency of the ECI**.

Primarily, this concerns the significant **variation that exists across the national level data collection requirements for the ECI**. In fact, Annex III of the ECI Regulation details 13 different sets of statement of support data requirements.

Linked to this overarching issue, the ECI data requirements face criticisms of **excessive data collection**. In particular, this relates to the number and, to a lesser extent, the sensitivity of the data that signatories are required to provide, which is also relative as explained above. It is worth noting that, as detailed in the study's risk assessment, the risk of reduced ECI participation due to excessive data requirements should be given high priority.

Regarding the number of data points, the majority of stakeholders agree that, in many Member States, supporters of an ECI are required to provide too much data. This perception is further supported by the comparison of the ECI with similar national or regional participatory instruments, which finds that, for the most part, similar national or regional instruments require signatories to provide fewer data than the ECI.

Regarding the sensitivity of data, stakeholders in most Member States (21) have no concerns over the sensitivity of the ECI data requirements. However, where concerns have been raised, they primarily relate to the collection of personal ID (document) numbers. For these concerns, and the issue of data sensitivity more generally, the key challenge is ensuring trust in the entities or individuals collecting, controlling and processing the data.

The challenge of excessive data collection is even more pertinent when considered against the type of outcome achieved by an ECI. It is generally considered, upon the analysis of national and regional participatory instruments, that the requirements of an instrument imposed on supporters should reflect the outcome achieved by that instrument (i.e. the greater the impact, the greater the requirements). However, national and regional instruments which realise similar outcomes to the ECI have greatly reduced data requirements in comparison to many Member States for the EU's instrument. As such, the ECIs data requirements are not considered to be proportional to its outcome.

These challenges are further complicated by the fact that signatories residing in a Member State different from their country of citizenship, can choose (in most cases) to provide the data required by their country of citizenship or the data required by their country of residence. In practice, this is not possible across all Member States and results in the exclusion of some groups of EU citizens from ECI participation.

Regarding the verification process, there is **limited coherence between the data collected via statements of support and the data used for verification** of those same statements of support; this issue is particularly evident in light of practices employed by similar national or regional participatory instruments. To illustrate, for similar instruments, 85% of Member States verify all and only those data collected, whereas, for the ECI, this is only true for 57% (16) of Member States. The compliance of these practices with the ECI Regulation, which says that the purpose of collecting the data is their subsequent verification by Member States' authorities, is questionable.

Other challenges related to the processing of statements of support include:

- the absence of specific provisions in the ECI Regulation ensuring the compliance with the data protection legislation as regards **the storage and transfer of paper statements of support** from organisers to Member States' competent authorities – this is particularly pertinent in light of the focus placed on securing online statements of support;
- the **circuitous route online statements of support are required to take when being transferred** from the online collection systems to the competent national authorities for verification (first from the system to the organisers and then from the organisers to the competent national authorities).

To address the challenges identified in the ECI process, **best practices from similar national and regional participatory instruments**, many of which have been alluded to above, have been identified. These practices can be grouped as follows:

- **Minimised data requirements:** the similar national and regional instruments examined require fewer data at the collection and verification stages than the ECI;
- **Coherent data requirements:** the similar instruments identified across the Member States maintain a better connection between the data collected through statements of support and the data verified than the ECI;
- **Data requirements proportional to outcome:** the data collection and data verification requirements of many of the national and regional participatory instruments are better proportioned in light of the outcome of the instrument, when compared with the ECI;
- **Use of technology:** One beneficial application of technology in this respect is to **facilitate engagement with participants**. For example, the online component of the Finnish citizens' initiative *Kansalaisaloite* is administered through a dedicated government-hosted web platform. This platform is a one-stop shop for all relevant information on participation in, and organisation of, a citizens' initiative.

A second beneficial application of technology, currently in use in the Slovenian popular initiative, relates to the use of secure e-signatures to submit support for an initiative. The statements of support require a secure e-signature, verified by a qualified certificate and the signatory is immediately notified if his/her statement of support has been rejected.

In contrast to the above, the following findings indicate the **ECIs positive practices and, in some cases, its advancement beyond the examples found at the national and regional level**:

- As evidenced by this study's risk assessment, the majority of the identified data protection and data security risks to the ECI process are considered to be at an **acceptable level**;
- **Acceptance of both paper and online statements of support:** this practice has a positive impact on engagement with the ECI across the EU and is not common among national and regional participatory instruments (63% of these similar instruments only permit paper collection); and
- **Approach to verification:** the ECI process for verification is well designed in comparison to many similar national and regional instruments. For example, a number of these instruments require in-person authentication of signatures and others require very limited (i.e. no verification of the veracity of data) or even ad-hoc verification of statements of support.
- **Approach to data security:** the ECI has a comprehensive approach to the security of the online collection systems used to store statements of support, as evidenced by the extensive risk mitigation demonstrated in this study's risk assessment including the technical specifications accompanying the ECI Regulation; and
- **Use of technology:** in a similar fashion to some of the national and regional instruments, technology has been used to facilitate the ECI process. In particular, the positive use of technology includes: the development of software to automate the verification of online statements of support and the conversion of paper statements of support to electronic format by scanning them, allowing for more secure transfer of statement of support data.

A number of policy options were developed and assessed, the full list of policy options is as follows:

- Options for the simplification and harmonisation of the data requirements:
  - **Option 1.1** – one set of data (**name, surname, residence/address, date of birth** and **nationality)**:
  - **Option 1.2** - require two sets of data, either the set of data listed under option 1.1 (name, surname, residence/address, date of birth and nationality), or a similar set which would not include the address and date of birth, but the passport or ID number instead.
- Options allowing to transfer the responsibility for the protection of personal data:
  - **Option 2** presents the possibility of transferring all responsibility for the collection, storage and transfer of personal data submitted through online statements of support to the European Commission.
  - **Option 3** presents two possibilities for amendments to the mechanisms for handling the personal data of signatories submitted through paper statements of support.
- Other options applicable to online collection only:
  - **Option 4** describes possibilities for: i) two-step data collection systems where signatories initially submit minimal personal data before submitting further personal data at a later date (option 4.1); and ii) two-step systems whereby signatories register with an entity (e.g. the Commission), which allows them to support ECIs at later dates with just one-click (option 4.2).
  - **Option 5** describes possible implementations of the ECI that make use of eID or available e-government portals.

On the basis of the research undertaken for this study, a number of conclusions can be drawn from the options developed in section VI.

In terms of **data simplification and data harmonisation**, the nationality principle should be followed, ensuring each national verification authority is in charge of verifying statements of support for their own nationals, wherever they reside. While it would require two Member States (UK and Ireland) to adapt their verification mechanisms, it would be the least invasive and obstructive change to the current situation.

While the data required under option 1.1 (**name, surname, residence/address, date of birth** and **nationality**) would fulfil the simplification and harmonisation criteria, it would not allow all Member States to adequately verify all their nationals and consequently exclude a significant number of EU citizens of supporting an ECI. Consequently, option 1.2 is considered the most viable of the two. Option 1.2 would require two sets of data, either the set of data listed under option 1.1 (**name, surname, residence/address, date of birth** and **nationality),** or a similar set which would not include the address and date of birth, but the passport or ID number instead. The UK and Ireland would have to ask for the first set of data (i.e. including the address) to nationals residing in the country, and the second set of data (including passport number) to their citizens residing abroad.

It would ensure that all EU citizens can participate in an ECI, that the data collected are minimised in all countries and that statements of support can be verified by all competent national authorities.

Other options could also be envisaged to address specific elements of the collection of statements of support.

1. With regards to options allowing the **transfer of the responsibility for the protection of personal data**, Option 2 setting up a sole central collection system for online statements of support, for which responsibility lies with the European Commission has many advantages. Significant benefits, in particular for the policy objective related to

safeguarding the personal data of supporters will be achieved by the implementation of Option 2.

2. With regards to the **collection of paper statements of support**, Option 3.1 where organisers are in charge of scanning the paper form in order to upload them directly to the online collection system is preferred over option 3.2 where they would enter this information manually. Both options reduce the substantial risk of data loss in transit by moving to uploading these paper statements of support as well as the burden on Member States' competent national authorities in the verification of paper statements of support, especially given the significant number of Member States who physically verify every single paper statement of support. Option 3.1 has the added advantage of reducing inputting mistakes.

3. The **use of eIDs** would be beneficial in that it would simplify the requirements and significantly reduce the burden of verification by national authorities. However, it should also be noted that eID is currently not implemented across all Member States and the penetration within Member States also varies, making this option unsustainable as the only possibility of signing at the current time.

4. Finally, were the simplification and harmonisation of the data requirements under Option 1.2 not to be achievable at the current time, a two-step system could be setup where supporters would first be asked to submit limited data at the initial point of support, and additional data would then be requested electronically at a later stage to provide a level of robustness to the verification mechanism. Alternatively, a pre-registration system could be setup. These two-step options present an opportunity to have the data requirements minimised at the point of signing a statement of support for signatories. However, the added value of these options is substantially diminished if the set of data is minimised in accordance with Option 1. It is also not clear whether supporters would be willing to provide the additional data in the second stage and whether this would not be particularly prejudicial to the success of citizens' initiatives.

Overall, data simplification and harmonisation would be the most immediate and important goals. In the current situation, these would be achieved by the introduction of Option 1.2. It is possible to imagine a situation where ECIs are supported by EU citizens through the use of eIDs as this would mitigate or cancel a number of risks identified in the risk assessment as well as simplify the process for supporters and national authorities. This will only be possible once all Member States adopt eIDs which is certainly not the case currently.

# II. Overview of the study

*This document constitutes the Draft Final Report for the 'Study on data requirements for the European Citizens' Initiative' under Framework contract no JUST/2015/PR/01/0003 on Supply of Impact Assessment, Evaluation and Evaluation related services in the policy areas – Lot 1.*

*Chapter II provides a brief description of the objectives of the study and the research methodology employed to achieve the objectives.*

## II.1. Study objectives

The primary objectives of the study are as follows:

- Assess the scope and possible approaches for simplifying the **data requirements for ECI signatories** within the existing legislative framework;
- Assess the scope for streamlining the related **data protection (and security) requirements for organisers**, while ensuring the protection of these data in accordance with the ECI Regulation; and
- Assess more broadly the proportionality of the provisions of the Regulation as **regards data requirements for signatories and the verification of statements of support**, also in relation to other instruments of direct and participatory democracy at national/regional level, and put forward possible **alternative options** in this regard should the Commission decide to propose a revision of the ECI Regulation[1].

## II.2. Methodology

In order to meet the study objectives, the following three tasks have been undertaken:

- **Analyse the ECI at national level**: i) analyse the ECI statement of support data requirements and the mechanisms implemented to verify statements of support at the Member State level; ii) assess the sensitivity of data requirements across the EU in relation to the ECI; and iii) identify best practices related to the collection and verification of statements of support and tackling data sensitivity issues;
- **Identify and assess the data protection and data security risks in the current ECI processes**, building on existing risk assessments. Assess the scope for simplification of the technical specifications for online collection systems[2];
- **Analyse similar national or regional participatory instruments**: i) analyse the data that signatories are required to provide to support national or regional

[1] On 11th April 2017, First Vice President Frans Timmermans announced a revision of the ECI Regulation, which was followed by the publication of a Roadmap on the Revision of Regulation (EU) No 211/2011 on the citizens' initiative (Ares(2017)2537702).

[2] This present study was done in conjunction with with the "Study on the improvement of the Commission Implementation Regulation (EU) No 1179/2011 of 17 November 2011 (a.k.a. Technical Specifications) laying down the technical specifications for online collection systems pursuant to the ECI Regulation" and the "Study on the use of Electronic Identification (eID) for the European Citizens' Initiative" that investigated this topic in greater detail.

participatory instruments of a similar nature to the ECI before comparing these with the ECI; ii) analyse the verification mechanisms implemented by similar national or regional participatory instruments; iii) assess the sensitivity of data requirements across the EU in relation to national or regional participatory instruments; and iv) identify best practices related to the collection and verification of statements of support and tackling data sensitivity issues;

Subsequently, based on the triangulation of outputs from these three tasks, the study **assesses the proportionality of current data requirements** and **develops possible options** for the simplification of the data requirements within, as well as outside, the ECI Regulation.

The methodology used for this assessment builds upon comparative and legal analysis techniques and relies on **mixed methods qualitative and quantitative research,** as well as expert opinion, consisting of:

- **Familiarisation interviews** with relevant European Commission officials and EU civil society organisations at the inception of the study;
- **Desk-based research:** aimed at compiling, processing and analysing existing evidence from different sources. These include elements such as legislation and rules implementing ECIs at national level, statistics on participation in ECIs and data on similar national or regional participatory instruments;
- **Interviews** with national authorities responsible for implementing the provisions of the ECI Regulation and, if applicable, other similar instruments; citizens' committees; national civil society and NGOs and their European umbrella organisation (such as EDRi; the ECI Campaign; European Citizens Action Service) and the European Commission;
- **Country fiches:** developed based on the national data collection exercise (interviews and desk research), which contain all the information collected on the legal and practical implementation of ECIs (data requirement, data protection, verification mechanisms etc.) as well as information on participation rates for ECIs and other participatory instruments, attitudes to data security and other relevant information; and
- **Case studies** covering four Member States and Switzerland. The cases selected aim to unpick in greater detail the approaches of national or regional participatory instruments to addressing issues identified in the course of the analysis of the ECI.

These data have been assessed using the following types of analyses:

- **Descriptive analysis** providing information and comparison of the situation, attitudes to data sensitivity and data requirements in all Member States;
- **Comparative (legal) analysis** comparing and analysing the laws, implementation rules, data and information across all Member States;
- **Statistical analysis** on the level of participation / support for ECIs and other participatory instruments at national and regional level and on the level of participation / support for each ECI and similar participatory instruments;
- **Risk assessment** covering possible data protection and data security risks to the ECI and its current processes;
- **Development and assessment of options** to simplify data requirements in the context of ECIs.

## II.3. Limitations to the quantification and assessment of the policy impacts

There are strong limitations associated with attempts to quantify impact on participation in the ECI. Whilst inferences can be made based upon agreed indicators that affect participation, and based upon existing literature and stakeholder consultation, statistically significant causal links

cannot be established between a reduction in data requirements and an increase in the participation in ECI's by European citizens.

Similarly, no comparative study exists on the data sensitivity of citizens across the Member States of the EU, and therefore any resulting analysis of the impact of data sensitivity on the participation in participatory instruments must be based upon inference and not statistically significant causal links.

Whilst attempts were made to contact relevant national authorities and other stakeholders in all Member States regarding disparate aspects of the study, responses from several stakeholders, and particularly national authorities, were not forthcoming. However, this was mitigated through the increase use of desk research and additional interviews with relevant stakeholders.

Finally, it is worth noting that while Chapter VI presents alternative options and assesses the proportionality of each of the options against policy objectives, the risk assessment presented in Section III.4 and where the data protection responsibilities lie between different actors, this study is not an impact assessment and should therefore not be considered as such.

## II.4. Structure of the report

This report is structured as follows:

- **Chapter I:** contains the executive summary;
- **Chapter II:** the present chapter sets out the objectives and methodology of the study;
- **Chapter III:** presents background information on the ECI before analysing the ECIs data collection and data verification requirements, as well as the verification mechanisms implemented across the Member States. Chapter III then analyses the interaction between the ECI and data protection issues, before the data protection and data security risks to the ECI are assessed;
- **Chapter IV:** provides an analysis of data sensitivity across the EU Member States;
- **Chapter V:** presents a descriptive analysis of the national or regional participatory instruments identified and examined before providing a comprehensive comparative analysis of the data requirements of the ECI and similar national or regional participatory instruments;
- **Chapter VI:** presents the possible alternative options for the simplification of the ECI's data requirements; and
- **Chapter VII:** presents the conclusions of the study.

In addition, this document contains 5 appendices:

- A list of stakeholders consulted;
- A bibliography;
- 5 country case studies presenting national or regional participatory instruments across Finland, Germany (Berlin), Slovenia, Switzerland and the UK;
- An overview of e-government and e-identity schemes and national registries;
- An overview of the ECI's data and data verification requirements.

# III. Data requirements for the European Citizens' Initiative: the current situation

*Chapter III sets out the current situation with regard to data requirements for ECIs, including the data collected, required and verified. It provides an overview of the situation in the Member States (with the specific information for each Member State provided in the country fiches as part of the Appendices). The section is structured around the following sub-sections:*

**III.1.** **The ECI – how it works:** this sub-section introduces the European Citizens' Initiative and details the process by which an ECI proceeds from the formation of a citizens' committee to the potential examination, public hearing in the European Parliament and answer by the European Commission;

**III.2.** **ECI data requirements:** this sub-section analyses the data requirements for the ECI by examining:

- **III.2.1.** ***Why*** Member States require these data (i.e. the data's purpose);
- **III.2.2.** ***What*** data is required to achieve the above purpose in terms of: i) data collected through statements of support (i.e. Annex III of the ECI Regulation); and ii) data used for verification; and
- **III.2.3.** ***How*** the data collected is used to verify the statements of support according to the purpose (i.e. the data verification process).

**III.3.** **The protection of personal data in ECIs**: this section sets out the current data protection requirements applied to the ECI and each of the actors involved (organisers, national authorities, the Commission etc.) and highlights changes which will be brought about by the application of the GDPR in May 2018.

**III.4.** **Risk assessment:** Following the agreed methodology, and incorporating the analysis already presented on several of the most pertinent risk scenarios this sub-section presents the analysis of the data protection and data security risks identified at each of the ECI steps within the scope of the study and the components of each risk. Furthermore, this sub-section discusses risk treatment options and the overall risk profile of the ECI.

## III.1. The ECI – how it works

Created to connect EU citizens to EU decision-makers, the ECI is a petitioning mechanism that allows citizens to invite the European Commission to propose a legal act. It was enshrined in the Treaty of Lisbon[3] and is aimed at **increasing direct democracy within the EU through the inclusion of citizens in agenda-setting at the EU level.**[4] Participation from one million EU citizens, spanning at least one quarter of the Member States, is necessary to invite the Commission to initiate a proposal for a legal act through an ECI. Such a legal act must be in a field where the Commission has the competence to act. This ability to invite the Commission to initiate such a proposal places the ECI, and thus the EU's citizenry, alongside the European Parliament and the Council of the EU in this function. In 2011, MEP Diana Wallis, ECI co-

[3] Article 11(4) of the Treaty on European Union and Article 24 of the Treaty on the Functioning of the European Union, which pertains to Union Citizenship

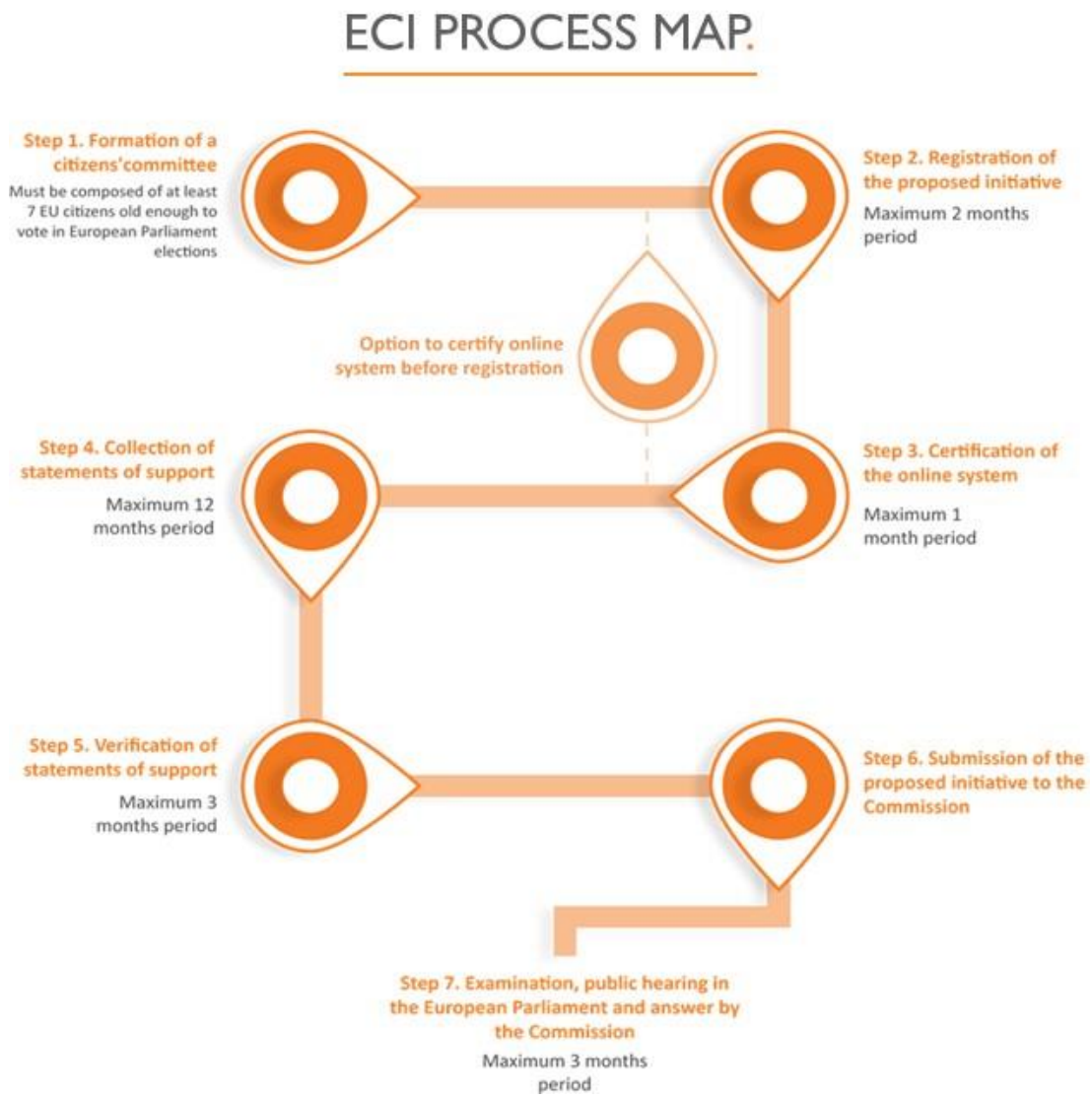
[4] Report on the application of Regulation (EU) No 211/2011 on the citizens' initiative. Available at: http://ec.europa.eu/transparency/regdoc/rep/1/2015/ EN/1-2015-145-EN-F1-1.PDF. Accessed: 13 July 2016

rapporteur in the European Parliament, stated that the ECI let citizens 'push the start button of the legislative process'.[5]

The rules and procedures governing the ECI are laid out in *Regulation 211/2011 on the citizens' initiative* (the ECI Regulation).[6] Between its inception and March 2015, an estimated 6 million ECI statements of support have been collected across 36 registered ECIs.[7]

Figure 2 provides an overview of the seven step process that governs the lifecycle of an ECI from its launch through to the public hearing in the European Parliament and the European Commission's response. Each stage is further explained below.

**Figure 1: European Citizens' Initiative process map**




*Source: Optimity Advisors based on publicly available information on the ECI.*

5 'Hearing on European Citizens' Initiative: reform is urgently needed!' Agenda Europe. Available at: http://euractiv.m.tap.cr/news/view/1377974. Accessed 15 July 2016

6 Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative

7 Report on the application of Regulation (EU) No 211/2011 on the citizens' initiative. Available at: http://ec.europa.eu/transparency/regdoc/rep/1/2015/ EN/1-2015-145-EN-F1-1.PDF. Accessed: 14 July 2016

### Step 1: Formation of a citizens' committee

In order to begin an initiative, a **citizens' committee** must be formed by citizens. The citizens' committee will manage the initiative throughout the process. The committee must meet the requirements laid out in Article 3(2) of Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative registration criteria, containing at least **seven EU citizens living in at least seven different Member States**.

### Step 2: Registration of the proposed initiative

Following the formation of a citizens' committee, the Commission will determine whether to register a proposed initiative based on the criteria laid out in Article 4(2) of the Regulation on the citizens' initiative.[8] Should the initiative meet the registration criteria, the Commission will **register the initiative** within two months of the request.

### Step 3: Certification of the online system

Organisers can collect **statements of support** both online and in paper format. In order to collect statements of support online, organisers can:

- Use an online collection system using an existing or specifically built online collection software hosted privately;
- Use the Commission's open-source software, hosted privately; or
- Use the Commission's open-source software, and the hosting by the Commission (in Luxembourg) as exceptionally offered by the Commission.

Any system used by organisers must meet the broad security and technical requirements laid out in both Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative *and* the Commission Implementing Regulation (EU) No 1179/2011 of 17 November 2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative.

Following the setting-up of a bespoke online collection system, organisers should request certification of their system from the relevant national authority of the Member State where the data will be stored, providing documentation to this competent national authority to prove the system meets the abovementioned security and technical requirements. To date, only the national authorities in Poland and Germany have certified online collection systems, in addition to Luxembourg, which certifies all the systems hosted by the Commission.

**Throughout the study, the national authorities in charge of certifying online collection systems are called 'certification authorities'.**

### Step 4: Collection of statements of support

After the registration process for those wishing to use paper statements, as well as the certification process for those wishing to use an online system, organisers can begin the process of collecting statements of support from citizens. The organisers then have 12 months from the date of registration to collect the required one million statements of support from at least seven Member States. Whilst organisers are not required to have signatories from each Member State, they are required to reach the minimum number of signatories from at least seven Member States.[9]

---

8 Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative

9 Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative

Organisers must comply with the legislation governing the protection of personal data (Directive 95/46/EC) throughout the process. In particular, before beginning to collect statements of support, organisers may be required to notify the national data protection authority(ies) in the Member States where the data of their activities will be processed.[10] Organisers must use forms which comply with the models first laid out in Annex III of the Regulation on the citizens' initiative, and amended in the Commission delegated Regulation in 2015,[11] as the basis for the statements of support forms. The forms must include all required information for the proposed initiative and take into account each Member State's specific data requirements.

The data that signatories must provide **varies significantly between the different Member States**, presenting challenges for the collection of statements of support.

Practices in most Member States allow non-national EU citizens to sign a statement of support providing either: i) the data required by their country of **citizenship**; or ii) the data required by their country of **residence**. For example, a Spanish citizen living in Belgium would be able to provide the data required by Spain (country of citizenship) or the data required by Belgium (country of residence). Signatories are only permitted to submit one statement of support for an ECI and must provide all data required by the Member State selected. However, for some combinations of citizenship and residence, this choice is not possible and, furthermore, in select cases, this results in the exclusion of some groups of EU citizens from supporting an ECI. For instance:

i. Citizens of Ireland and the UK residing abroad only have the option of providing the data required by their country of residence.

ii. Non-national EU citizens that reside in Austria, Bulgaria, Czech Republic, France or Portugal only have the option of providing the data required by their country of citizenship.

The overlap between these two bullet points results in exclusion from submitting a statement of support for an ECI. Irish and British citizens that reside in Austria, Bulgaria, Czech Republic, France, Portugal or any non-EU country are not able to provide the data requirements to their country of citizenship (i.e. as per point i) or their country of residence (i.e. as per point ii).

Furthermore, citizens of Belgium, Denmark, Germany and Luxembourg residing abroad can provide: i) the data requirements of their country of residence (except for those citizens residing in AT, BG, CZ, FR and PT, as detailed above); or ii) the data requirements of their country of citizenship but only if they have pre-notified those national authorities of residence in a different country. For example, a German citizen living in Denmark would be able to submit a statement of support based on: i) his/her residency in Denmark (i.e. providing the Danish data requirements); or ii) his/her citizenship (i.e. providing the German data requirements) but only if (s)he had notified the German authorities of his/her residence in Denmark.

Beyond these differences related to citizenship and residency, there is a second key difference by which Member State data requirements can be categorised: whether a signatory's personal identification (document) number is necessary to sign a statement of support. Currently, 18 of 28 Member States require a personal identification (document) number to be provided. The requirements related to the personal identification (document) number in those 18 Member States are summarised in Table 1, below.

As can be seen in the table, 36 types of personal identification (document) number are eligible across the 18 Member States. However, only 13 Member States permit the use of personal identification (document) numbers that are available to non-national EU citizens (illustrated in bold).

[10] Data Protection. Europa. Available at: http://ec.europa.eu/citizens-initiative/public/data-protection. Accessed: 14 July 2016

[11] Commission Delegated Regulation (EU) 2015/1070 of 31 March 2015 amending Annexes III, V and VII of Regulation (EC) No 211/2011 of the European Parliament and of the Council on the citizens' initiative

**Table 1: Personal identification (document) number requirements, per Member State, and availability of those numbers to non-national EU citizens.**

| Member State | Personal identification (document) number: Type<br>**(Bold = those types available to non-national EU citizens)** |
|---|---|
| AT | • Passport<br>• Identity card |
| BG | • Personal Number |
| CY | • Identity card<br>• Passport<br>• **Alien registration certificate** |
| CZ | • National identity card<br>• Passport |
| EL | • Identity card<br>• Passport<br>• **Residence certificate / permanent residence certificate** |
| ES | • Identity card<br>• Passport<br>• **Foreigner's identification number (NIE)** |
| FR | • Passport<br>• National identity card |
| HR | • **Personal identification number** |
| HU | • Identity card<br>• Passport<br>• **Personal identification number** |
| IT | • Passport (incl. issuing authority)<br>• **Identity card (incl. issuing authority)** |
| LT | • **Personal number** |
| LV | • **Personal identification number** |
| MT | • Identity card<br>• **Residence document** |
| PL | • **PESEL Identification number** |
| PT | • Identity card<br>• Passport<br>• Citizen's card |
| RO | • Identity card<br>• Passport<br>• **Registration certificate**<br>• **Permanent residence card for EU citizens**<br>• Personal identification number |
| SE | • **Personal identification number** |
| SI | • **Personal identification number** |

As such, and as highlighted in the European Ombudsman's own-initiative inquiry into the functioning of the ECI, many stakeholders agree that **the main issues that need to be addressed** relate to the **level and heterogeneity of ECI personal data requirements.**[12]

[12] Letter to the European Commission requesting an opinion in the European Ombudsman's own-initiative inquiry OI/9/2013/TN into the functioning of the European citizens' initiative (ECI). European Ombudsman.

### Step 5: Verification of statements of support

Should organisers manage to gather the required number of statements of support (1 million or more), the next stage is to contact the relevant national authorities in each Member State where they collected statements of support, in order for the aforementioned authorities **to verify the number of valid statements of support collected for that country** (Article 8(1) of the ECI Regulation).

For a statement of support to be verified, it must meet certain conditions, stipulated at various points in the ECI Regulation. These conditions include:

- Article 5(5): that the **statement of support was collected after the date of registration of the proposed ECI** and within a period not exceeding 12 months from that date;
- Article 3(1): that the **natural person is an EU citizen and old enough to vote in European Parliament elections** (without it being a requirement that the person is actually registered to vote in those elections);
- Article 5(3): that the **natural person has given his/her support to the ECI in question only once**.

The ECI Regulation further specifies that the authentication of handwritten signatures (a data requirement of paper statements of support) shall not be required (Article 8(2)). If the statements of support are collected through an online collection system, the organisers must export the electronic statements of support from the place where the server of the online collection system is hosted. These online statements of support, alongside the paper statements of support, are then sent to the competent national authority. Section 2.7.7 of the Commission's Implementing Regulation (EU No 1179/2011) further requires that online collection systems provide for the encryption of data during both storage and transit to the competent authorities.

The relevant national authorities then have three months to verify and certify the number of valid statements of support, regardless of the ratio of paper to electronic statements. In order to certify the number of valid statements of support collected, the national authorities verify the statements of support collected, which may be based on random sampling or may involve the individual checking of each statement of support.

**Throughout the study, the national authorities in charge of verifying the statements of support and certifying the number of valid statements of support collected are called 'verification authorities'.**

### Step 6: Submission of the initiative to the Commission

Once organisers have received the certificates certifying the number of valid statements of support from the relevant national authorities, meeting the requirements of one million signatories and the respective minima in at least seven Member States, they can submit their initiative to the Commission.

### Step 7: Examination, public hearing in the European Parliament and an answer by the Commission

After submission to the Commission, the initiative enters into the process of examination, public hearing in the European Parliament and the provision of an answer by the Commission. The Commission has three months to complete this process and provide an answer to the organisers. The Commission can decide to take action by initiating a legislative procedure, to take other forms of action or not to take any action and it should explain why.

---

Available at: http://www.ombudsman.europa.eu/cases/correspondence.faces/en/54609/html.bookmark. Accessed: 14 July 2016

## III.2. ECI data requirements

The personal data of EU citizens is vital to ensure the validity of ECI statements of support. However, as highlighted above, many stakeholders agree that one of **the ECI's main issues** relates to the **level and heterogeneity of ECI personal data requirements.**[13] This sub-section examines three key questions concerning the ECI data requirements:

- **Why** do the Member States need the data collected through statements of support (i.e. what is the purpose of the data);
- **What** data is required to achieve the above purpose (i.e. the data collected through statements of support and the data used for verification);
- **How** is the data collected used in practice to verify the statements of support (i.e. the data verification process);

These three questions will be assessed according to (i) the ECI Regulation, the Implementing Regulation and Annex III, and (ii) the situation in practice across the Member States.

### III.2.1. The purpose of verification (and thus of the data collection) – WHY?

As highlighted above, the first question to ask regarding the ECI data requirements relates to why ECIs need to collect data from signatories (the mechanism for which is the statement of support). The short answer is that the data is necessary to verify that a statement of support is valid but, as this and subsequent sections will demonstrate, there is significant discussion regarding the practical application of the regulatory provisions on this matter. This section will set out the purpose of verification, as stipulated in the ECI Regulation, before discussing the interpretation of these regulatory conditions.

The text of the Regulation is not very explicit about what exactly is to be "verified". One view to take would be that the competent national authorities need to verify if all the data to be provided by a signatory in the relevant Member State have been entered for the statement of support that is being verified. However, the text of the Regulation suggests that the verification process is meant to be more than such a "tick-box" exercise. Article 8(2) implies that what is to be verified is whether the statements of support submitted to the competent national authorities are "valid" for the purposes of the ECI Regulation, i.e. can be counted as part of the required total.

#### Conditions for the validity of the statements of support

As detailed in section III.1, a statement of support must meet four conditions to be verified. These conditions are stipulated at various points in the ECI Regulation and are as follows:

- that the **statement of support was collected after the date of registration of the proposed ECI** and within a period not exceeding 12 months from that date (***condition 1***);
- that the **natural person is an EU citizen** (***condition 2***) **and is old enough to vote in European Parliament elections** (***condition 3***);
- that the **natural person has given his/her support to the ECI in question only once** (***condition 4***).

Furthermore, some Member States have to some extent implemented the verification of a fifth condition, namely that the signatory of the statement of support has not been impersonated.

[13] Letter to the European Commission requesting an opinion in the European Ombudsman's own-initiative inquiry OI/9/2013/TN into the functioning of the European citizens' initiative (ECI). European Ombudsman. Available at: http://www.ombudsman.europa.eu/cases/correspondence.faces/en/54609/html.bookmark. Accessed: 14 July 2016

The following paragraphs discuss, for each condition, how the terminology of the ECI Regulation could be interpreted and implemented in practice.

### Condition 1: Verification of whether the statement of support was collected in the appropriate period.

The condition of a specified period for the submission of valid statements of support implies that statement of support on paper must be dated, and that automated date- and time logs must be kept of online statements of support. To allow for meaningful verification of compliance, such logs should be reasonably tamper-proof (cf. Article 6(4)(b)).

The Commission-provided Online Collection Software does indeed contain automated date / time logs. As regards paper statements of support, signatories are required to indicate the date of signing. Member States verify if this date is within the collection period for the initiative concerned (with the risk that the signatory has indicated a false or erroneous date).

### Condition 2: Verification that the statements of support originate from a natural person

Presumably, this issue does not really arise in relation to statements of support collected on paper, offline, directly from individuals. (Note that this is a different issue from fraudulent entries of names etc. of real people but who did not actually support the ECI, impersonation: addressed as condition 5, below.)

In relation to statements of support submitted online, a "*captcha*" system can be used to ensure that the supporter was a natural person; one such system is built into the Commission-provided Online Collection Software. The Technical Specifications for Online Collection Systems in the Annex to the Implementing Regulation says, under the heading "Technical Specifications aiming at implementing article 6(4)(a) of Regulation (EU) No 211/2011", that:

> *In order to prevent automated submission of a* statement of support *using the system, the signatory goes through an adequate verification process in line with current practice before submission of a* statement of support*. One possible verification process is the use of strong 'captcha'.*

Clearly, while this obviously recommends the use of "strong 'captcha', it does not make its use mandatory. However, a verification process is mandatory. "*Captcha*" has generally been criticised as an obstacle to visually impaired people and to people not using the Latin alphabet, and as slowing down and thus hindering sign-up processes.[14] "*Captchas*" have also been shown to offer no full proof against fraud or hacking.[15]

### Condition 3: Verification of whether the person who signed a statement of support is an EU citizen and *of the age to be entitled* to vote in elections to the European Parliament

As the Commission Guidelines expressly clarify:[16]

> *According to Article 3(4) of the Regulation, signatories, who must be citizens of the Union,* ***must be of the age to be entitled to vote*** *in elections to the European Parliament. This means that having the right or being registered to vote in elections to the European Parliament cannot be a requirement to support a citizens' initiative. Member States must only verify whether the signatory is old*

[14] Ironically in the present context, one Australian disabled person started a petition against *captchas* on this basis, see:
http://www.techspot.com/news/53495-disabled-australian-starts-petition-to-kill-captcha.html.
[15] See: Trust Management: Proceedings of IFIPTM 2007: Joint iTrust and PST Conferences on Privacy, Trust Management and Security, July 30-August 2, 2007, New Brunswick, Canada.
[16] European Commission (2013) The European Citizens' Initiative: Guidelines and Recommendations for Practical Implementation.

*enough to be able to vote in these elections (18 years of age in all Member States, with the exception of Austria, where the voting age is 16).*

In most cases, the eligibility to participate in an ECI – i.e. the citizenship and the age of a person who supports an ECI – can be checked with reference to the mandatorily provided data themselves. As will be illustrated in section III.2.2, all Member States require signatories to enter their nationality, and 19 out of the 28 Member States also require signatories to provide their date of birth. Of course, people can provide false or erroneous information in these respects. (The seven Member States that do not require supporters to provide their date of birth do all ask for personal ID numbers or personal ID document details, and the person's age will be knowable from those.)

A signatory's age can be verified with reference to state-held records and registers such as population registers, personal ID registers (registers of all residents' personal identification numbers – PINs – in countries where these have been issued) or records of identification documents such as passports.

Indeed, one may question why so many Member States that require signatories to provide the details of their PINs or ID documents (11 out of 18) also require that they provide their date of birth and nationality – or much of the other required details (apart from first and last name and date of statement of support and signature). They will already be able to find the relevant other data by means of the personal ID numbers or personal ID document details.

One could argue that the demand for the not-strictly-necessary data is therefore not in accordance with Article 5(3). While it could be counter-argued that having various data can help in detecting "false errors" (e.g. when the signatory has changed residence since signing the initiative or where minor information such as the street number has been omitted), the Regulation does not foresee to collect additional data solely for this purpose. Furthermore, the more data are required, the more chance there is that such false errors occur.

### Condition 4: Verification that the natural person has given her/his support to the ECI in question only once

In principle (leaving impersonation aside), condition 4 can be almost fully checked with reference to the provided data themselves: first, it should be checked whether there are duplicate names (full first names plus family name); for people with the same full names, their dates of birth, places of residence or places of birth can be checked. While there will undoubtedly be people named "John Smith" that are born on the same day (of different parents), it it highly unlikely for them to also live at the same address. In such unlikely instances, the two statements of support are (wrongly) marked as a duplicate entry and only counted as one; however this will have a negligible effect on the overall tally.

Member States that require signatories to provide the details of their PINs or ID documents can of course easily check if any person issued with such a number or document has signed more than once: all they have to do is check for duplicates of those numbers, making sure that they have not supported several times by using different numbers (e.g. the passport number and the ID card number).

### Condition 5: Verification that the person whose details were registered was the actual person submitting the statement of support, i.e. that there was no fraud or "impersonation"

As noted above, the need to check for impersonation is not expressly spelled out in the Regulation and only undertaken to some extent by some Member States, in most cases not as an additional check but as an alternative check where some of the conditions above cannot otherwise be checked. It should be noted that this is the most demanding check. For this verification, it does not suffice to check that the personal data are, in the official records, linked to the persons whose names are listed as signatories. Rather, it must be checked whether the nominally-listed persons had actually themselves entered those data on the (offline or online) list – i.e. that it had not been someone or something else who fraudulently added their names. This verification can really only be done at three moments: either (i) at the time of registering a statement of support, by putting in place some form of confirmation of identity; or (ii) ex post

facto, by the people carrying out the verification contacting the nominally-listed persons. In practice, this is the option used by those Member States undertaking this verification. A third option (iii) could be for people to "pre-register" for ECIs at certain websites, with this verification being done once, at the time of registration with the website. This option is further explored as part of the policy options.

### III.2.2. Data requirements necessary to verify the statements of support – WHAT?

Building on the purpose of verification and the possible routes to verification discussed above, this sub-section focuses on the data themselves. Firstly, the data that signatories are required to provide through statements of support will be examined, as per Annex III of the ECI Regulation. Secondly, the data that are used to achieve the verification purposes describe above will be examined and compared with the data collected through statements of support.

#### Data required of ECI signatories according to the ECI Regulation (Annex III)

Annex III to the ECI Regulation contains two basic lists of required data on signatories: one for Member States that do not require the provision of a personal identification number or personal identification document number (statement of support form – Part A); and one for Member States that do require the provision of a personal identification number or personal identification document number (statement of support form – Part B). The only difference between the two lists is the addition of a field for this personal identification (document) number in the latter list. The listed data are as follows:

- Full first names;
- Family names;
- Residence (street, number, postal code, city, country);
- Date and place of birth;
- Nationality;
- Date and signature;

*For those countries that require personal identification (document) number only:*

- Personal identification number/personal identification document type and number.

However, both lists also spell out, in footnotes, a considerable number of clearly negotiated deviations from the above listed data, with certain countries requiring more, and certain countries requiring less than, or only parts of, the listed data. The table below shows the full divergences as provided for in the Annex and the footnotes.

Presumably, the Member States, in drafting the Annex as they did, felt they needed the data listed for them in order to verify the statements of support against each of the conditions stated above but as explained below, it appears that not all these data are in practice used for the verification.

**Table 2: ECI data requirements**

| | Full first names | Family names | Father's name | Name at birth | Residence | | | Date of birth | Place of birth | Nation-ality | PI(D)N* | Date & signature |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Street etc. | City | Country | | | | | |
| **Member States that do not require personal ID numbers/personal ID document details:** | | | | | | | | | | | | |
| BE | X | X | | | X | X | X | X | X | X | | X |
| DE | X | X | | | X | X | X | X | X | X | | X |
| DK | X | X | | | X | X | X | X | X | X | | X |
| EE | X | X | | | X | X | X | X | X | X | | X |
| FI | X | X | | | | | X | X | | X | | X |
| IE | X | X | | | X | X | X | X | | X | | X |
| LU | X | X | | | X | X | X | X | X | X | | X |
| NL | X | X | | X | X | X | X | X | X | X | | X |
| SK | X | X | | X | X | X | X | X | X | X | | X |

| | Full first names | Family names | Father's name | Name at birth | Residence | | | Date of birth | Place of birth | Nation-ality | PI(D)N* | Date & signature |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Street etc. | City | Country | | | | | |
| UK | X | X | | | X | X | X | X | | X | | X |
| **Member States that do require personal ID numbers/personal ID document details:** | | | | | | | | | | | | |
| AT | X | X | | | X | X | X | X | X | X | X | X |
| BG | X | X | X | | | | | | | X | X | X |
| CY | X | X | | | | | | | | X | X | X |
| CZ | X | X | | | | | | | | X | X | X |
| EL | X | X | X | X | | | | X | | X | X | X |
| ES | X | X | | | | | | X | | X | X | X |
| FR | X | X | | | X | X | X | X | X | X | X | X |
| HR | X | X | | | X | X | X | | | X | X | X |
| HU | X | X | | | | | | | | X | X | X |
| IT | X | X | | | X | X | X | X | X | X | X** | X |
| LT | X | X | | | | | | | | X | X | X |
| LV | X | X | | | | | | | | X | X | X |
| MT | X | X | | | | | | X | | X | X | X |
| PL | X | X | | | X | X | X | | | X | X | X |
| PT | X | X | | | | | | X | | X | X | X |
| RO | X | X | | | X | X | X | X | | X | X | X |
| SE | X | X | | | | | | | | X | X | X |
| SI | X | X | | | | | | X | X | X | X | X |

[*] PI(D)N = Personal identification Number / Personal identification document type and number
[**] For Italy, the authority that issues the listed ID document should also be recorded.

As illustrated in the tables above and below, the data required for signing statements of support varies significantly across Member States, including the need for personal ID (document) numbers, name, nationality, date and place of birth, address, and the signatory's father's name. The data that are most commonly required are name (both full first and family names), nationality, date of birth and personal ID (document) number.

Additionally, some Member States require specific data requirements that are not required by the vast majority of Member States. These include the requirement for the name of the authority issuing your personal ID number by the Italian authorities, as well as the submission of the signatories father's name in Bulgaria and Greece and the signatories name at birth in Greece, the Netherlands and Slovakia.

Table 2 above, further separates the Member States by whether or not they require a personal identification (document) number / details. As is evident, for those Member States requiring such identification data, name, nationality and the relevant personal identification (document) number are required by all Member States. For those Member States that do not require such identification details, address and date of birth appear to be important supplementary data to name and nationality; these four data types are required by all 10 Member States. Furthermore, these data demonstrate that, on average, the requirement to provide a personal identification (document) number reduces the number of data a signatory is required to provide from 4.9 to 4.3 data. However, again with regard to the number of data required, there is markedly more variance in the group of Member States that require a personal identification (document) number than in the group that do not. More specifically, the number of data types required by the first group (i.e. where ID is required) ranges from 3 to 7 with a standard deviation from the mean of 1.3 data types, whereas the range of the second group is only 2 and the standard deviation from the mean sits at only 0.7 data types. This is to say that **greater harmonisation is found amongst the data requirements of the group of Member States that do not require a personal identification (document) number**.

### Table 3: What data is required for statements of support across the EU?

| Data required | Country | Total |
|---|---|---|
| **Name (Full First and Family Names)** | All MS | **28** |
| **Nationality** | All MS | **28** |
| **Date and signature** | All MS | **28** |
| **Date of Birth** | BE, DE, DK, EE, FI, IE, LU, NL, SK, UK, AT, EL, ES, | **19** |

| Data required | Country | Total |
|---|---|---|
| | FR, IT, MT, PT, RO, SI | |
| **Personal ID (Document) Number** | AT, BG, CY, CZ, EL, ES, FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI | **18** |
| **Address** | BE, DE, DK, EE, FI[17], IE, LU, NL, SK, UK, AT, FR, HR, IT, PL, RO | **16** |
| **Place of Birth** | BE, DE, DK, EE, LU, NL, SK, AT, FR, IT, SI | **11** |
| **Name at Birth** | NL, SK, EL | **3** |
| **Father's name** | BG, EL | **2** |
| **Other, please specify** | IT – Authority issuing the identification document | **1** |

### Data requirements in practice (what data is used for verification)

Regarding the types of data used for verification, they understandably follow similar frequency of use trends to those data collected through statements of support. For example, as for the collected data, presented above, the data used most commonly for verification are **name** (used by 25 Member States); **nationality** (used by 23 Member States); and **date of birth** (used by 22 Member States). Similarly, the least common data used for verification included father's name (used by 2 Member States) and name at birth (used by three Member States). The full list is presented in Table 4, below.

**Table 4: What data is used for verification of statements of support across the EU?**

| Data required | Country | Total |
|---|---|---|
| **Name (Full First and Family Names)** | AT, BG, CY, CZ, EL, ES, HR, HU, IT, LT, MT, PL, PT, RO, SE, SI, BE, DE, DK, EE, FI, IE, LU, SK, UK | **25** |
| **Nationality** | AT, BG, CZ, EL, ES, HR, HU, IT, LT, MT, PT, RO, SE, SI, BE, DE, DK, EE, FI, IE, LU, NL, UK | **23** |
| **Date of Birth** | AT, BG, EL, FR, HU, IT, MT, PL, PT, RO, SI, BE, DE, DK, EE, FI, IE, LU, NL, SK, UK | **21** |
| **Personal ID (Document) Number** | AT, BG, CY, CZ, ES, FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI | **17** |
| **Address** | AT, BG, FR, HR, PL, RO, BE, DE, DK, EE, FI[18], IE, LU, NL, SK, UK | **16** |
| **Place of Birth** | AT, BG, FR, IT, SI, DE, EE, LU, SK | **9** |
| **Name at Birth** | EL, FR, SK | **3** |
| **Father's name** | BG, EL | **2** |
| **Other, please specify** | IT – Authority issuing the identification document | **1** |

*Note: The data presented here stems from the responses provided by Member States' authorities when contacted. Some of the information provided appear not always to be in line with the information provided on the register(s) used for the verification or on the verification process. For instance, the population register used to verify the statements of support in France does not include addresses, while they have been reported to be verified.*

Although the data that are used for verification are similar to those that are collected, it is clear that variance exists between the data used for verification and the data collected through statements of support. Based on data collected from national-level stakeholders and presented in the Appendix VIII.6. Country fiches, the **competent national authorities in 13 Member States use different data for the verification of ECI statements of support than they require signatories to submit at the collection phase**.

[17] In case of Finland – only the country of residence is to be provided and not the full address.
[18] In case of Finland – only the country of residence is to be provided and not the full address.

10 of these Member States (BE, CY, DK, EL, ES, FR, IT, LV, NL, SK) require fewer data for verification than signatories are required to provide; 2 require more data for verification than signatories are required to provide (BG, HU); and 1 Member State requires the same number of data but requires date of birth for verification rather than nationality, which is collected (PL). The 10 Member States that require fewer data for verification than they collect, on average, require that signatories provide more data than in the other Member States: 5.3 types of data per Member State compared with an EU-wide average of only 4.5 types of data and an average across the remaining 18 Member States of just 4.2 types of data.

Justification has been provided by the competent national authorities in several Member States: in Belgium, Denmark, Greece, Latvia and Spain, for example, the excess data are reportedly included as they allow the statements of support to be verified even in cases where certain data are missing, incorrect or illegible. In these instances, the excess data collected enables the competent authority to verify the statements of support. Of this group, a smaller subset of national authorities consider that these data requirements are appropriate and particularly relevant to the use of automated image recognition software.

On the other hand, representatives of civil society and ECI organisers are of the opinion that reducing the data to be collected is desirable for citizens. These stakeholders thus favour a procedure where minimal verification is carried out or where only a sample of signatories are required to provide all the data which is currently required. Others, however, were of the opinion that requiring personal information of a certain sensitivity was important in order to ensure that signatories saw the difference between supporting an ECI and signing a petition.

In principle, if a Member State requires signatories to an ECI to provide their national ID-, passport- or residence card-number and name (first and family name), there should be no need for any further information: that should suffice to carry out the minimal checks. However, as one Belgian official involved in verification put it: "The more data we have, the easier it is for us to do the checks"; a sentiment that the findings suggest is shared across at least the 10 Member States highlighted here.

It is worth noting that the **data used for verification does not vary significantly between Member States that require signatories' personal ID (document) details and those that do not**. Whilst all the Member States that require personal ID numbers/personal ID document details, verify these ID numbers[19], there is a substantially reduced use of signatories' address for verification by several Member States. In this respect, Italy presents a unique case as it requires the personal identity card number, the name of the identity card issuing authority and the address of signatories. Each of Italy's 8,092 municipalities "comune" has a civil registry and therefore, in order for the Ministry of Interior to identify the municipality to which the Italian signatory of the statement of support is registered, the Ministry of Interior examines the address. These statements of support are sent to the relevant municipal authorities for verification against the civil registry of the municipality of residence. The address itself is not used for verification of a statement of support but just as an identifier of the relevant local authority.

It would seem that officials use any not-strictly-necessary data that has been collected by organisers on signatories to see if they can still match the individual against one of the above-mentioned lists, even if that was not possible from the necessary data (perhaps because an ID number had been incorrectly entered or was illegible). In other words, if not all the stipulated data are entered into paper statements of support, if data are entered incorrectly or if data are not in accordance with the register in question, the officials still try to perform a secondary check with the additional data (whether the person can be found in a general, national or regional register). If that secondary check is successful, and the person in the register is of voting age, the statement of support is counted as valid.

Such a situation was expressly confirmed in **Portugal**. Specifically, this concerned the submission of erroneous ID card numbers or the submission of ID card numbers that were no longer valid but were in the process of being renewed. Portuguese officials stated that "in both [these] situations, where the situation is verified and there is the possibility to identify the

[19] In the case of Greece, only if needed (where the electoral roll is not sufficient to carry out the verification).

citizen and see that the renovation process was ongoing, the statements of support were accepted". Similarly, in **Estonia**, Annex III dictates that signatories must provide their place of birth in a statement of support. However, in practice, an inaccuracy in that regard is not considered sufficient to exclude the signature, because the state registers themselves lack clarity on these data. This clearly raises the issue of why this information is asked to signatories if it cannot be used for verification purposes.

In **Greece**, the required data include the signatory's ID number, but since that number is not included on the electoral roll, yet the signatures are checked only against that roll, the ID number data is not used in the first place. However, it can be used if there is an issue with the verification on the basis of the electoral roll. In addition, officials believe that the inclusion of the ID number in the mandatory data is useful, even though it is perceived as sensitive, because "it provides adequate significance in the eyes of the signatory and accentuate the seriousness of his / her participation."

In **Cyprus**, the officials interviewed did not include nationality in the data they said were required, although that item is listed in Annex III of the ECI Regulation for Cyprus – but since organisers do have to obtain ID-, passport- or resident permit data, the nationality of each signatory can still be gleaned from these.

### III.2.3. The ECI data verification process – HOW?

Preceding sections detail the ECI Regulation's provisions on the conditions to be verified by competent national authorities – section III.2.1 – and the data to be collected by ECI organisers (and provided by ECI signatories) in order to verify statements of support – section III.2.2. This section first re-iterates the previously highlighted fact that the ECI Regulation and accompanying Commission Guidelines place the onus for the processes and mechanisms for verification on the Member States (i.e. how competent national authorities use the data collected by ECI organisers to verify statements of support). Subsequently, this section examines the processes and mechanisms implemented across the Member States for the verification of statements of support; in other words, **how the Member States use the data discussed in section III.2.2 to achieve the verification purposes established and discussed in section III.2.1**.

#### Data verification according to the ECI Regulation

The data required by competent national authorities to verify statements of support is informed by the conditions that must be verified – this interdependency has been reflected in Annex III. However, the onus for designing and implementing the verification processes and mechanisms is on the Member States – a fact which is clearly projected through the regulatory framework (Box 1, below).

**Box 1: Verification processes and mechanisms according to the ECI Regulation.**

#### Limited provisions on the processes and mechanisms for verification

Article 8(2) of the ECI Regulation states that:

*The competent authorities shall […] verify the statements of support submitted on the basis of **appropriate checks**, in accordance with national law and practice, **as appropriate**. […]*

*For the purpose of the verification of statements of support, the authentication of signatures shall not be required.*

Recital 18 adds the following on the use of the term 'appropriate checks':

*Taking account of the need to limit the administrative burden for Member States, they should […] carry out such verifications on the basis of appropriate checks, which may be based on **random sampling**, and should issue a document certifying the number of valid statements of support received.*

Although the Commission Guidelines[20] do not clarify the term 'appropriate checks', they do provide Member States with guidance on the implementation of certain mechanisms, stating that:

> *"The Regulation only requires the Member States to **check the coherence of the data** provided by signatories." And*
>
> *"given that the verification exercise has legal implications, which could be contested before the courts, **it is important that certain safeguards are in place**, in particular when random sampling is the method used."*[21]

Following this statement, the Guidelines list three types of verification safeguards, as follows:[22]

- **Sample size:** Member State authorities should ensure that they choose a statistically valid random sample, i.e. a sample that is sufficiently large and, where appropriate, takes account of different levels of risk within the population. In order to do so, they should opt for a margin error and a confidence level that ensure that the results will be as accurate as possible. They should also assess whether there is a need to stratify the population prior to sampling, particularly if there is a suspicion that certain batches of statements of support are less reliable.
- **False errors:** Certain minor mistakes or changes should not invalidate the statements of support. This should be the case if, for example, there is no suspicion of fraud (e.g. the signatory has made a genuine error or omitted minor information which does not cast doubt on the authenticity of the statement of support or prevent the authorities from identifying him/her), or the signatory has changed residence since signing the initiative. It is possible to account for such mistakes or changes by considering that a certain percentage of invalidated statements of support are in fact valid. If verification is automated, it may be necessary to double-check the rejected statements of support manually in order to detect such false errors.
- **Benefit of the doubt:** When extrapolating the results of the sample to the whole population, the Member State authorities should give the benefit of the doubt to the organisers by choosing the lower threshold in the confidence level (i.e. the interval obtained by adding and subtracting the margin of error from the result).

From this text, it is clear that the Commission's Guidelines do not offer verification prescriptions to the Member States but instead encourage a certain sentiment to be implemented by the competent national authorities. The emphasis is not on detecting "unreliable batches" or otherwise fraudulent statements of support, but on checking whether the details of ECI signatories meet the conditions listed previously, and conducting these checks with a certain leniency.

Moreover, as is expressly stressed in the Regulation (Recital 18), national authorities can choose to carry out these checks only in relation to a random sample of the collected statements, provided that the sample is sufficiently large (and possibly stratified) (see the bullet point re "Sample size", above).

This could be argued to be too limited. Specifically, as stated above, Article 8(2) of the Regulation must be read as saying that the relevant authorities must use **"appropriate checks" to confirm the validity of the statements of support** (while also clarifying that if there are checks stipulated or used in national law or practice unrelated to ECIs, such as national electoral or plebiscite laws or practices, that are deemed by those national authorities to be also "appropriate" for ECIs, those can be used; and that any national law specifically regulating ECIs in the country concerned can set out the domestic checks to be used in more

[20] European Commission (2013) The European Citizens' Initiative: Guidelines and Recommendations for Practical Implementation.
[21] *Idem*.
[22] European Commission (2013) The European Citizens' Initiative: Guidelines and Recommendations for Practical Implementation.

detail – although they will still have to be "appropriate" to the aim of confirming the validity of the statements of support).

### Data verification in practice

Based on the above discussion, the remainder of this section will first discuss the different techniques and tools used by Member States to verify ECI statements of support. More specifically, this relates to: i) whether Member States use **sampling techniques or whether they verify all statements of support**; and ii) the types of **registers or databases** used by Member States to verify statements of support. Subsequently, the section will discuss how the data collected through statements of support are **linked** to the data held on the relevant registers or databases.

### Sampling v. full verification

The verification systems used by the national authorities in each Member State vary between three systems: i) verification of a **random sample** of statements of support; ii) verification of **all statements of support**; and iii) a **combination method**, where both random sampling and full checks are used across the paper and online statements of support. Table 5 provides an overview of the systems in use by the Member States.

As can be seen, the most common method, as implemented by 14 Member States, is the use of random sampling techniques. Under such a system, the competent national authorities select a sample of statements of support at random to verify and, based on the rejection rate within the selected sample, determine the overall rejection rate for the submitted statements of support. In 9 Member States, all statements of support, in both paper and online forms, are verified. The third system – as seen in Cyprus, Finland, Lithuania and Portugal – uses different verification methods (i.e. full verification vs. sampling) for paper and online statements of support.

**Table 5: What national verification systems are in place implementing Art 8(2) for verifying the validity of statements of support in the Member States?**[23]

| Type of checks | | Member States | Total |
|---|---|---|---|
| **i)** | **Random sampling** | BE, DE, DK, EE, EL, ES, FR, IE, IT, NL, LU, PL, SE, UK | **14** |
| **ii)** | **All statements of support** | AT, CZ, HR, HU, LV, MT, RO, SI, SK | **9** |
| **iii)** | **Combination method** | CY, FI, LT, PT | **4** |

In most Member States only a sample of signatures is verified and a variety of sampling techniques are used – in **Cyprus**, for example, 10% of statements of support are selected and, to ensure the randomness of the selection, the 9$^{th}$ of every 10 statements of support is selected and verified (i.e. 9, 19, 29, …, etc.). In other Member States, a statistical formula is used to calculate the size of the sample in such a way as to ensure a specific confidence rate (in **Netherlands** and **Ireland**, 90%; in **Estonia**, 95%; in **Greece** 99%) and a specific error rate (in **Netherlands**, 3%; in **Ireland**, 2.5%; in **Estonia**, 5%; in **Greece**, 1%). In **Poland**, a slightly different approach again has been selected, with a two stage verification process implemented. Polish authorities, in the first instance, randomly select a small sample of 200 statements of support. Once these are verified, a larger sample of 1,000 statements of support are selected for verification. If the rejection results of both verification stages match up, the results are confirmed.

[23] It has not been possible to include Bulgaria in the analysis of verification techniques, as no data has been provided on this point by the Bulgarian authorities.

National authorities in **France** use the random sampling method of verification on between 5-10% of the statements of support, depending on the number of statements of support, with the implication that datasets large enough for statistical accuracy will require random sampling verification on just 5% of the statements of support.

With regard to Member States that use a combination method, **Portugal** verify all online statements of support automatically against the similarly-structured national identity database; however, for paper statements of support, a representative random sample of 37.5% is verified, by manually entering the data into an XML file and carrying out the verification in the same way.

### Use of registers or databases

Member States use a variety of mechanisms to match up data collected with data on record. The primary mechanism – used by 23 Member States – relates to verification of ECI statements of support through centralised registers and databases. For example, these databases include census registries of citizens and in a few cases electoral rolls. Contrastingly, two of the larger Member States (**German** and **Italy**) rely on municipal or regional authorities to conduct verification. **Ireland** and **Spain** approach verification in a third way, combining centralised (for online statements of support) and de-centralised verification (for paper statements of support); furthermore, for certain statements of support, **Ireland** employs direct verification with signatories. An overview of the use of these mechanisms by Member States is presented in Table 6.

**Table 6: How is the verification of statements of support carried out in each Member State in practice?**

| Verification process | Member States | Total |
|---|---|---|
| **Verified through central databases / registry's / census / electoral rolls** | AT, BE, BG, CY, CZ, DK, EE, EL, FI, FR, HR, HU, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK | **23** |
| **Verified through records held by municipal / regional authorities' database** | DE, IT | **2** |
| **Combination method** | ES, IE | **2** |
| **Direct verification** | UK | **1** |

For the 25 Member States that **use centralised verification** to some extent (i.e. including Ireland and Spain), it is clear that heterogeneous databases are in use. This is understandable given that the databases pre-date the ECI and are the product of Member State-specific needs. Furthermore, this presented an obvious limitation for the relevant national authorities and the ECI as a whole, in the agreement of data requirements for ECI statements of support, as they must complement existing, Member State-specific infrastructure. This characteristic must be considered with regard to any proposed amendments of the ECI data requirements, as it plays a vital in role in how Member States can verify ECI statements of support.

Table 7 below, presents a list of the primary databases used by the Member States in order to undertake the verification of ECI statements of support, thus demonstrating the variation in the sources of verification data.

**Table 7: Databases used to verify statements of support.**

| Member State | Database used for verification |
|---|---|
| **AT: Austria** | ID Document Register |
| **BE: Belgium** | National Register |
| **BG: Bulgaria** | Unified System for Civil Registration and Administrative Services, Ministry of Regional Development and Public Works |
| **CY: Cyprus** | Civil Registry |
| **CZ: Czech Republic** | Register of Inhabitants (ROB), Fundamental register of residents, Register of Identity Cards or Register of Passports |
| **DE: Germany** | Local population registers |
| **DK: Denmark** | Civil Registry System |
| **EE: Estonia** | Population Register |
| **EL: Greece** | Electoral Roll, population register |
| **ES: Spain** | Population register |
| **FI: Finland** | Population Register |
| **FR: France** | Base of Register of Natural Personal (Base des répertoires des personnes physiques), managed by the Institut national de la statistique et des études économiques (INSEE), Ministry of the Interior |
| **HR: Croatia** | Register of Voters (Ministry of Interior can be involved) |
| **HU: Hungary** | Electoral Register, Population Register, Passport Register |
| **IE: Ireland** | Electoral Register, Department of Housing, Planning, Community and Local Government |
| **IT: Italy** | Municipal civil registries |
| **LT: Lithuania** | Register of Population |
| **LU: Luxembourg** | Central Citizens database |
| **LV: Latvia** | Population Register (Iedzīvotāju Reģistrs), Central Election Commission and Citizenship and Migration Department |
| **MT: Malta** | National identity database |
| **NL: Netherlands** | Population Register, Municipal Authority of The Hague, as delegated by the Ministry of the Interior |
| **PL: Poland** | State Register System |
| **PT: Portugal** | Central Registry for Citizens, Instituto Dos Registos e do Notariado (IRN), Serviço de Estrangeiros e Fronteiras (Service on borders and foreigners) |
| **RO: Romania** | National Register of Persons Records and Database of the General Inspectorate for Immigration (GII), Directorate for Persons Record and Database Management (DEPABD) and GII, Ministry for Internal Affairs |
| **SE: Sweden** | Population Register |
| **SI: Slovenia** | Voting Rights Register, Permanent Residence Register or Register of Foreigners |
| **SK: Slovakia** | The Register of Residents of the Slovak Republic (which includes Slovak citizens residing abroad) |

For those Member States that require **municipal or regional authorities** to verify all or some of the statements of support, it is clear that there must be some way of identifying the relevant de-centralised authority for each statement of support. In **Germany, Italy** and **Ireland**, signatories are required to provide their address for this purpose; in **Spain**, however, signatories are not required to provide their address but this information is identifiable when combined with the personal identification number / passport number / foreigner identification number that signatories are required to provide as they are both included in the Population Register. Although information on why a de-centralised approach has been implemented in these instances has not been explicitly collected as part of this study, primary reasons, inferred from the information provided, may include the division of the workload for the verification of paper statements of support, which are considered more difficult to verify by a number of national authorities, and having the capability to verify data against local registers.

A third verification technique is used to complement the first two as part of the combination method used in **Ireland** and the **UK** – through direct contact with signatories. In **Ireland**, this third technique is used in instances where the signatories of an ECI statement of support are not found on the electoral register, a letter is sent by postal mail to the signatory. **Ireland**, in line with the European Commission's Guidelines, aims to give the benefit of the doubt to signatories with regard to the validity of statements of support. As such, in these instances, signatories are only required to respond if they have not submitted a statement of support for the ECI in question. Thus, if no response is received, the statement of support is considered valid. In the **UK**, the national authority selects a random sample of signatories. These signatories are then sent a letter via postal mail. If the signatory did not sign the ECI, they must respond within 2 weeks otherwise the statement of support is validated.

### Achieving the purpose of verification

Regardless of the tools and techniques used, the key element of verification is how Member States ensure the data submitted through a statement of support is valid. As stated earlier, this means a Member State has to assess whether the data collected meets four conditions:

- that the **statement of support was collected after the date of registration of the proposed ECI** and within a period not exceeding 12 months from that date (***condition 1***);
- that the **natural person is an EU citizen** (***condition 2***);
- that the **natural person is old enough to vote in European Parliament elections** (***condition 3***);
- that the **natural person has given his/her support to the ECI in question only once** (***condition 4***).

It would appear that the **majority of Member States, with interesting exceptions, essentially conduct verification as a "tick-box" exercise of these conditions**; i.e. whether duplicate statements of support exist (*condition 4*) and whether the statement of support was signed within the allotted timeframe (*condition 1*); then whether each signatory is listed on the general population register or some similar general list of lawful residents (as listed above) and, if so, whether that natural person is an EU citizen (*condition 2*) and of voting age (*condition 3*). If these checks are positive, the signature is declared to be valid and counted.

For instance, in **Lithuania**, the competent authority verifies if the personal data provided through the statements of support are identical to the data of the Register of Population before confirming the following facts: if each citizen is at the age at which citizens are entitled to vote in elections to the European Parliament (*condition 3*); if the person, who signed, was not dead at the time of signing; if the personal data are indicated correctly; if the natural person, who signed the statement of support, is a citizen of the Member State of the European Union (*condition 2*); and if there are repetitive identical entries (*condition 4*).

Similarly, in **Denmark**, verification comprises checking the submitted data is accurate, as compared with the Civil Registry System, before ensuring the criteria of European citizenship and age (*conditions 2 and 3*) are fulfilled. Furthermore, a check is made to ensure that duplicate statements of support do not appear (*condition 4*). Although Denmark does not collect ID numbers from signatories to an ECI, these are used in the following way to identify duplicate

statements of support: the ID numbers associated with the signatories are identified through the checks against the Civil Registry and extracted into a separate Excel file. Automated checks for duplicate statements of support are then conducted within this Excel file.

A few Member States take additional and/or alternative steps should the authorities not be able to ensure signatories meet conditions 2 and 3, and by doing so address condition 5. As mentioned previously, **Ireland** engages in direct contact with a selection of signatories to an ECI. In **Ireland**, signatories that cannot be located on the Irish electoral register, and therefore the authorities cannot ensure conditions 2 and 3 are met, are contacted by postal mail. Similar to the UK's practices, the contacted signatories are given two weeks to reply in the case that they did not state their support for the ECI in question.

Furthermore, the **Lithuanian** Central Electoral Commission contracts a graphology expert to conduct visual verification of the handwriting provided on paper statements of support. The objective of this practice is to determine whether there are multiple entries done "by one hand", if there are any signs that the data could have been extracted illegally from the existing databases and entered into the forms of statements of support as well as whether there are entries where separate fragments are written in different writing styles, by different writing means, which could lead to a conclusion that the entries of a specific line of the form of statements of support were included at a later date.

The practices in these three Member States appear to perform to some extent the fifth verification condition, as outlined in section III.2.1: i.e. verification that the person whose details were registered was the actual person submitting the statement of support(i.e. that there was no "impersonation" or fraud). This **fifth condition is not a requirement under the ECI Regulation**.

### Rejection of statements of support at the verification stage

As a result of the verification practices described through this section, Member States determine the number of valid statements of support provided to them by an ECI organiser. However, statements of support will not always be accurate or eligible and competent national authorities will be required to reject statements of support. The final paragraphs of this section detail the extent to which statements of support are rejected, the reasons why they are rejected and the perceptions of national authorities on the likelihood of fraud related to ECI statements of support.

The **rates of rejection of statements of support at the verification stage vary significantly** across Member States, as well as across paper and online collection, and also across ECIs themselves.

Focusing first on variation across Member States, some report relatively high rejection rates, whereas others report relatively low rejection rates. For instance, **Irish** authorities reported extremely low validity rates of 66% for the ECI 'One of Us' and 68% for the successful ECI Stop Vivisection; and a higher, but still low, validity rate of 85% for Right2Water. Furthermore, **Cypriot** authorities rejected 14% of all statements of support related to the Stop Vivisection ECI, and **UK** authorities rejected 10% of all statements of support related to the Right2Water ECI.

Contrastingly, **Belgium** and **Slovakia** report low rejection rates. Table 8, below, presents data on the number of statements of support submitted and verified for three ECIs in Belgium (Right2Water, One of Us and 30km/h) and two ECIs in Slovakia (Right2Water and One of Us). As can be seen, the rejection rates for Right2Water (R2W) and One of Us (OofU) in both Member States are extremely low (i.e. <1%). The rejection rate for 30km/h in Belgium is slightly higher, at 2.5%, but it is still low.

**Table 8: Statements of support verification Slovakia and Belgium.**

| ECI | Number of signatures in Belgium | | | | Total handed in | Total after verification | % rejected |
|---|---|---|---|---|---|---|---|
| | Paper | % | Online | % | | | |
| **R2W** | 28,985 | 70% | 11,927 | 29% | 40,912 | 40,549 | 0.80% |
| **OofU** | 1,136 | 19% | 4,851 | 81% | 5,987 | 5,478 | 0.85% |
| **30km** | 354 | 9% | 3,466 | 91% | 3,820 | 3,725 | 2.50% |

| ECI | Number of signatures in Slovakia | | | | Total handed in | Total after verification | % rejected |
|---|---|---|---|---|---|---|---|
| | Paper | % | Online | % | | | |
| **R2W** | 10,983 | 51% | 10,320 | 49% | 21,303 | 20,988 | 0.15% |
| **OofU** | 28,585 | 88% | 3,961 | 12% | 32,546 | 31,951 | 0.18% |

Concerning the variation between the rejection rates for paper and online statements of support, relevant examples from the Netherlands and Luxembourg can be presented. In the **Netherlands**, for instance, the ratio of statements of support rejected was between 15-19% for paper submissions compared with 3-5% for statements of support submitted online. Similarly, the **Luxembourgish** authorities rejected just 2% of online statements of support compared with a 10% rejection rate for paper statements of support.

With regard to the final illustration of variation relating to verification rejection rates, it is evident in a number of Member States that rejection rates differ between ECIs. For example, the validity of statements of support ranged from 98% to 84% for all the statements of support verified by the **Greek** authorities. Similarly, the validity ratios reported by the **Irish** authorities of statements of support for the Right2Water initiative was 85% compared with validity ratios of 66% and 68% for the One of Us and Stop Vivisection initiatives respectively, as highlighted above. Furthermore, the **UK** rejected 10% of the statements of support for the 'Right2Water' initiative compared to 5% of the statements of support for the 'One of Us' initiative, and **Danish** authorities reported rejection rates of 2.75% to 7.5% across the four ECIs verified.

The main **reasons for rejection of statements of support** at the verification stage by national authorities are consistent across the Member States. These reasons focus around incorrect or missing data from the statements of support, multiple statements of support from the same signatory and signatories not meeting age requirements. Additionally, particular requirements for signatories that vary by Member State, form another significant cause for the rejection of statements of support by national authorities, such as an invalid date of signing in **Portugal**

**Cypriot** authorities confirm the above, stating that the main reasons for rejection were: multiple statements of support from the same signatory; too many missing data items leading to the impossibility to identify the signatory; wrong data leading to the impossibility to identify the signatory; unreadable data; and the requirement of being of voting age not being met. Similar reasons were also mentioned by **Slovakian** and **UK** national authorities.

Of those statements of support rejected by the **Danish** authorities, on average, approximately 30% have been invalidated due to data missing, incorrect data or data being unreadable. Approximately 38% were rejected due to a missing signature on paper statements of support and the rest due to various reasons including signatories being less than the minimum age or non-EU citizens (which also seems to be a particular issue in some Baltic states). Around 10% of the rejected statements of support have been invalidated due to multiple statements of support from the same signatory.

Table 9 below, provides an overview of the main reasons for the rejection of statements of support.

**Table 9: Main reasons for rejection of statements of support at the verification stage.**

| Member State | Main reasons for the rejection of statements of support |
|---|---|
| **France** | - Receiving multiple statements of support from the same signatory<br>- Missing or incorrect data leading to an inability to identify the signatory<br>- Signatory was not entitled to sign<br>- Signatory did not meet the age requirements |
| **Croatia** | - Receiving multiple statements of support from the same signatory<br>- Missing or incorrect data leading to an inability to identify the signatory |
| **Italy** | - Receiving multiple statements of support from the same signatory<br>- Missing or incorrect data leading to an inability to identify the signatory<br>- Signatory did not reach the voting age |
| **Portugal** | - Receiving multiple statements of support from the same signatory<br>- Missing or incorrect data leading to an inability to identify the signatory<br>- Signatory did not meet the age requirements<br>- Invalid date on the statements of support<br>- Signatory did not meet the nationality requirement<br>- Signatories were deceased |
| **United Kingdom** | - Receiving multiple statements of support from the same signatory<br>- Missing or incorrect data leading to an inability to identify the signatory<br>- Signatories withdrawing their support after being contacted for verification |
| **Cyprus** | - Missing or incorrect data leading to an inability to identify the signatory, in particular ID numbers<br>- Receiving multiple statements of support from the same signatory<br>- Signatory did not meet the age requirements<br>- Illegible data leading to an inability to identify the signatory |
| **Czech Republic** | - Missing or incorrect data leading to an inability to identify the signatory, in particular ID numbers<br>- Receiving multiple statements of support from the same signatory<br>- Signatory did not meet the age requirements<br>- Illegible data leading to an inability to identify the signatory |
| **Slovakia** | - Missing or incorrect data leading to an inability to identify the signatory, in particular ID numbers<br>- Receiving multiple statements of support from the same signatory<br>- Signatory did not meet the age requirements |
| **Austria** | - Missing or incorrect data leading to an inability to identify the signatory, in particular ID numbers<br>- Receiving multiple statements of support from the same signatory<br>- Signatory did not meet the age requirements |
| **Denmark** | - Missing or incorrect data leading to an inability to identify the signatory, in |

| Member State | Main reasons for the rejection of statements of support |
|---|---|
| | particular ID numbers<br>- Receiving multiple statements of support from the same signatory<br>- Signatory did not meet the age or EU citizen requirements |

**Submission of fraudulent statements of support**

For the most part, the national authorities rate the likelihood of fraud at the collection stage, in particular on a large scale, as low. Member States to explicitly confirm these findings include the national authorities in **Croatia**, **Portugal**, **Denmark, Hungary** and **Slovakia**. For example, **Portuguese** authorities believe their current verification process, i.e. using identity cards, is sufficient to detect fraud. Furthermore, no instances of significant fraud have been identified by the Member States.

On the other hand, however, **Swedish** authorities believe the possibility of fraud to be significant, remarking that the information in the Population Register (as used for verification) is generally accessible through the principle of public access. The same authorities further stated that developing a verification process that did tackle such fraudulent activities would not be possible. **Belgian** authorities agree to some extent, stating that they believe there is a reasonable possibility of fraud.

Mechanisms for detecting fraud are reported to be minimal. Many Member States do not have such a mechanism, beyond the current verification process. One Member State that has implemented such a mechanism is **Lithuania**. In contrast to the reported occurrence of fraud in the use of the **Lithuanian** national participatory instrument, the Lithuanian Central Electoral Commission has not encountered any instances of fraud during the verification of statements of support for the ECI. However, it has still enacted a mechanism to tackle fraud within the ECI – Article 89 of the Code of administrative offences No XII-1869, which regulates the breach of the procedures and conditions of ECI.

## III.3. The protection of personal data in ECIs

A key element of this study is to assess issues relating to the protection of personal data, in particular of of ECI supporters. This section summarises and presents conclusions on the following key elements:

- Relevant data protection norms and instruments
- The views of data protection authorities;
- Discussions on the applicable law with regard to ECI data handling;
- The data protection status of the various entities involved in the ECI;
- How to ensure 'accountability' for data protection compliance; and
- The ECI Regulation's liability provisions (also beyond data protection aspects).

### III.3.1. Relevant data protection norms and instruments

The ECI Regulation asserts, in simple declaratory terms, that:

> *This Regulation respects fundamental rights and observes the principles enshrined in the Charter of Fundamental Rights of the European Union, in particular Article 8 thereof, which states that everyone has the right to the protection of personal data concerning him or her. (Recital 26)*

More specifically, Article 12(1) of the Regulation makes clear that:

> *In processing personal data pursuant to this Regulation, the organisers of a citizens' initiative and the competent authorities of the Member State shall comply with Directive 95/46/EC and the national provisions adopted pursuant thereto.*

Recital 23 furthermore clarifies that:

> *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data is fully applicable to the processing of personal data carried out by the Commission in application of this Regulation.*

Directive 95/46/EC[24] and Regulation (EC) 45/2001[25] are the main EU data protection instruments in relation to the processing of personal data by private entities and Member State authorities, and EU institutions respectively. They will be referred to hereafter also as "the 1995 Data Protection Directive" (or "the 1995 Directive") and "the EU Institutions Data Protection Regulation" (or Regulation 45/2001).

From May 2018, the 1995 Directive will be replaced by a new General Data Protection Regulation ("GDPR") which, as a regulation, will apply directly in the legal order of the EU Member States (rather than through national implementing legislation).[26] References in other EU legal instruments, including the ECI Regulation and Implementing Regulation, to the 1995 Data Protection Directive, should, from then on, be read as references to the GDPR.

### III.3.2. Applicable data protection rules

**The current rules**

The 1995 Data Protection Directive is implemented in the Member States through national law ("implementing legislation"). Unfortunately, the national data protection laws implementing that directive vary in many important aspects and detail – which was indeed one of the main reasons to replace it with a regulation which, applies directly, and in theory uniformly, in the Member States, without the need for implementing legislation.

However, the GDPR still contains more than 30 provisions that allow the Member States to determine how they are to be applied – meaning that even after the GDPR comes fully into effect in May 2018, there will still be differences in which it is applied in the Member States.[27]

Yet, although the GDPR should lead to significantly closer harmonisation, and has various mechanisms – the so-called consultation, cooperation and consistency mechanisms – built into it to ensure this, in contrast to the 1995 Directive, it does not contain any "applicable law" rules to determine when which of the still-different national rules apply to transnational (but intra-EU) processing operations, or steps within chains of operations.

Presumably, however, the data protection authorities and the European Data Protection Board (established by the GDPR) will continue to adopt the same approach in relation to situations in which there are differences between the laws applied in the different Member States (i.e., in

[24] Full title: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.1995, p. 31.
[25] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L8, 12.1.2001, p. 1.
[26] 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), OJ L119, 4.5.2016, p. 1.
[27] See: https://edri.org/analysis-flexibilities-gdpr/; Full analysis: https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf

respect of the 30+ provisions of the GDPR that allow Member States to further regulate an issue) as they took under the 1995 Directive.

**The current rules applied to ECIs**

It is not difficult to determine the applicable law in relation to **national authorities** involved in ECIs (the certification authorities, the central verification authorities and other national public bodies, such as municipalities, that may assist in verification): insofar as they are not bound by more specific (stricter) rules in the ECI Regulation, they will all be subject (only) to their national data protection law and, from May next year, to the GDPR and any special rules on the application of the GDPR in the country concerned. Similarly, to the extent that they are not bound by the more specific rules in the ECI Regulation, any **Commission services** involved in ECIs will be subject (only) to Regulation (EC) 45/2001.

The question of applicable law is more complex in relation to **organisers**, because the ECI Regulation itself stipulates that they have to consist of "at least seven persons who are residents of at least seven different Member States" (Art. 3(2)). Moreover, statements of support may be collected from websites registered in, and by volunteers collecting them in paper form in any Member State.

The question of applicable law in relation to organisers of ECIs, was raised in the discussions between the Commission and ECI organisers, held in Brussels on 28 September 2012. The summary report of that meeting states the following in that respect:

> On [the issue of the data protection rules], organisers shared their opinions and experiences, in particular concerning the notification of national data protection authorities. The Commission presented its interpretation, which was also submitted on 26 September 2012 to the "Article 29 Data Protection Working Party" (the group assembling the representatives of the national data protection authorities and of the European Data Protection Supervisor dealing with the implementation of the Directive 95/46/EC), and according to which organisers were bound to one applicable law and should therefore notify the data protection authorities of only one Member State, in principle the one of the residence of the citizens' committee's representative – see the annex for more details. The Commission indicated that it had also communicated this interpretation vis-à-vis the Luxembourgish authorities.

The interpretation referred to (which of course addressed the issue in terms of the 1995 Directive, and not yet of the GDPR) is set out in an Annex of the summary report, as follows:

> National data protection law(s)
>
> Which national law applies to the processing of personal data in the context of an ECI?
>
> The collection and treatment of statements of support for a citizens' initiative, if intended as a set of operations, may be considered as one processing, according to Article 2 (b) of the Directive 95/46/EC:
>
> > Article 2
> >
> > Definitions
> >
> > For the purposes of this Directive:
> >
> > […]
> >
> > (b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
>
> Article 4 of the Directive ensures that for one processing one national law only applies and provides for the criteria defining which one does (in the context of the ECI, only the criterion in point a is relevant):
>
> > Article 4
> >
> > National law applicable

> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; […]

> In this regard, the citizens' committee as a whole is to be considered the data controller, according to Article 12 of the ECI Regulation. Therefore, the national law applicable is the one of the Member State where the organisers carry out their main activities. This would be, typically, the representative's country of residence or the country where the main operation centre of the ECI Committee is located.
>
> The considerations above apply without prejudice to the possible specific internal arrangements between the organisers.

It is not clear from the summary report whether the Article 29 Working Party (WP29) or the EDPS confirmed the Commission's interpretation. But in any case, the above only refers to the situation where organisers carry out their main activities in one country whereas other situations are possible, depending on how the citizens' committee is organised.

First of all, as the WP29 has made clear in its opinion on the concepts of controller and processor, issued in 2010,[28] in complex operations involving a range of actors, some of those actors can often be identified as controller or joint controller for certain parts of phases of the overall operation, and other actors involved in the overall operation as controllers for other parts or phases of the overall operation. This is further discussed below, in section III.3.4, but is also relevant in relation to the question of applicable law, since that hinges in part on who is the controller of a processing operation.

Secondly, the WP29 opinion on applicable law, also issued in 2010,[29] makes clear that in relation to cross-national (but intra-EU) activities, the core issues for determining that law are what personal data processing operations can be said to be carried out "within the context of the activities" of each "establishment" of the controller or controllers involved.

If there are different "establishments" involved in a chain of activities in different countries, then it could be that only the one law of the Member State where the central "establishment" is located will be the applicable law – if "effective control" is exercised over all the other, peripheral activities by the other "establishments" from that central "establishment". Or different laws of different Member States can apply to different processes (in different stages) within the overall process – if the peripheral actors in practice exercise "effective control" over their own activities (even though those are all linked, and may serve one overall purpose). The "establishments" need not be major, permanent institutions; they could be just offices, even of single persons. But they must have some permanency and stability, in relation to the overall activities.

In other words, the Commission conclusion that "the national law applicable [to organisers] is the one of the Member State where the organisers carry out their main activities", and that this would "typically" be the representative's country of residence or the country where the main operation centre of the ECI Committee is located, needs some further elaboration. Indeed, the use of the word "typical" in this conclusion already indicates that the conclusion is not a hard and fast one, applicable to all cases.

As an additional example: if the representative has an office (or in reality is linked to an organisation that backs the ECI, and indeed presumably is at the centre of the ECI), and if most of the activities for the ECI are directed from this office, it would be reasonable to conclude that all the personal data processing operations under the control or direction of that office take place "within the context of the activities" of that office; and that the data protection law applicable to those operations is therefore in principle the law of the Member State where that

[28] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" (WP169) of 16 February 2010.
[29] Article 29 Working Party, Opinion 8/2010 on applicable law (WP179) of 16 December 2010,

office is situated. This would include the retrieving of statements of support from the organisers' own Online Collection System and the transmission of those statements of support to the relevant national verification authorities.

However, there might be cases where the other organisers (and the organisations to which they may belong, and that may support the ECI in their country) will operate with some independence (although of course still within the framework of the ECI Regulation and Implementing Regulation). If they have "effective control" over the collecting of statements of support for the ECI in their country, it would be reasonable to conclude that they are the controllers of the personal data processing that those activities involve off-line (paper collection).

**The situation under the GDPR**

The situation under the current rules in the 1995 Data Protection Directive, described above, is unclear and unsatisfactory, and creates legal uncertainty and practical difficulties for organisers.

Unfortunately, these will not be completely resolved by the coming into force of the General Data Protection Regulation in May 2018, because that regulation, although it aims to ensure greater harmonisation, will still leave many issues to be determined by Member State law.

### III.3.3. Views of data protection authorities

There have been only a few formal assessments of the ECI processes by data protection authorities. The European Data Protection Supervisory (EDPS) has assessed the provisions as set out in the original Commission proposal for the ECI Regulation but not the final provisions of the Regulation.[30]

The Italian data protection authority, the *Garante per la protezione dei dati personali*, issued an opinion on the draft law on the implementation of the ECI Regulation in Italy.[31] The *Garante* stressed, as a preliminary observation, that participation in ECIs is a "delicate matter" since it involves the exercise of citizens' political rights, and "can" (*può*) involve the processing of "sensitive data" in the formal-legal data protection sense, i.e., in Italy:[32]

> *Personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life.*

Accordingly, the *Garante* concluded, the personal data collected in the context of an ECI should be processed, by any entity doing the processing, subject to the stricter rules on the processing of such data, compared to the somewhat more relaxed rules applicable to processing of non-sensitive data (*Garante* Opinion, p. 3). This also means that the verification of the correctness

[30] Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council on the citizens' initiative, O.J. C 323, 21.04.2010, p. 1ff. The reference for the Commission proposal of 31 March 2010 is COM(2010)119final.

[31] Parere del Garante sullo schema di regolamento che descrive le modalità di attuazione del Regolamento dell'Unione europea sull'"iniziativa dei cittadini", Rome, 19 July 2012. Hereafter "*Garante* Opinion".

[32] *Garante* Opinion (footnote 2, above), p. 3. The definition is taken from Article 4(1)(d) of the Italian data protection law, the *Codice in materia di protezione dei dati personali* or Privacy Code (in the English translation provided on the *Garante*'s website). This somewhat expands on the definition of such data ("special categories of data") in Article 8(1) of the 1995 EC Data Protection Directive:

> personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … data concerning health or sex life.

Article 9(1) of the EU General Data Protection Directive (GDPR), which will come into full force in May 2018, also expands on the 1995 definition, as follows:

personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and … genetic data, biometric data [when processed] for the purpose of uniquely identifying a natural person, data concerning health [and] data concerning a natural person's sex life or sexual orientation.

of the statements of support must be taken seriously. The *Garante* found that it was incompatible with this principle, that the Italian authorities wanted to use a "legal fiction", according to which, statements of support were to be "deemed" correct and valid if the local authorities to which they had been sent for verification did not report back that they were invalid. In the *Garante*'s view, this did not ensure that the (possibly sensitive) data were correct – in violation of Article 11 of the Privacy Code. The *Garante's* criticisms were heeded and the procedure now requires a formal positive confirmation of validity of statements of support from the local authorities, as part of the verification process.

By contrast, in other countries, such as **Ireland** and the **UK**, the personal data collected in the context of an ECI are generally not treated as sensitive.

Under the GDPR, Member States DPAs could continue to differ on whether they should treat all processing of statement of support data as processing of "sensitive data", and thus on whether controllers (organisers) are required to appoint Data Protection Officers, carry out Data Protection Impact Assessments, etc. (as discussed in section III.3.5, below). Although most of these issues could perhaps be resolved through the new consultation-, cooperation- and consistency mechanisms in the GDPR, and/or by the new European Data Protection Board (EDPB), that would be cumbersome and time-consuming.

The European Data Protection Supervisor did not provide any assessment as to the possible sensitivity of the data collected in its opinion.

In its opinion on the draft Regulation,[33] the EDPS welcomed the express clarification of the applicability of the main EU data protection instruments to ECI organisers, Member States' authorities and the Commission as concerns their ECI-related activities (EDPS Opinion, para. 23).

He was also "pleased" to see that Article 12(2) of the Regulation "makes explicit that the organiser and the competent authority must be considered as data controllers for the purposes of their respective processing of personal data" (para. 24). This is in line with the stipulation in the EU data protection instruments that, if processing is carried out on the basis of Member State or Union law, that law may indicate who shall be regarded as the controller of the processing (or, if there are distinct aspects to the processing, which entities shall be regarded as controllers for the distinct operations) (cf. Art. 2(d) DP Directive; Art. 4(7) GDPR; Art. 2(d) of Regulation (EC) 45/2001). However, as further discussed in section III.3.3, below, Article 12(2) does not in itself clarify the precise scope of that indication in relation to ECIs, i.e., of what specific processing operations that are part of the overall ECI process the entities mentioned (organisers and national certification- and verification authorities) are to be regarded as (respective) controllers.

### III.3.4. The status of the various entities

The following entities have specific roles as regards the processing of personal data under the ECI Regulation and are therefore data controllers with respect to those processings:

- **Organisers** have responsibilities and liabilities under EU data protection law in collecting of statements of support on paper forms and online via the online collection system and in passing them on to the relevant verification authorities.
- The **national certification authorities** have responsibilities under EU data protection law in respect of personal data they obtain in relation to certification of organisers' own Online Collection Systems only.

[33] The EDPS had in fact already been informally consulted prior to the adoption of the proposal and "welcomed this informal consultation and [was] pleased to see that most of his remarks have been taken into account in the final proposal." (Opinion, para. 3). Of course, as already noted, the EDPS assessed the provisions as set out in the original Commission proposal for the ECI Regulation but not the final provisions of the Regulation. His comments are therefore limited to that extent.

- The **national verification authorities** have a larger role to play, working closely with the relevant **national bodies** who check statements of support against the registers they maintain (as the case may be), but their responsibilities and liabilities would still be well-delineated and limited to the processing of the personal data contained in statements of support in the actual verifications concerned (including the relevant transfers). For this assessment, when the national verification authority works with other national bodies, it is considered that they are best regarded as "**joint controllers**" for these operations. One could argue that the public bodies in this act as processor for the Verification Authorities, but since they themselves are responsible for the registers they check against, we elected to see them as co-controllers (with the Verification Authority in question).
- The Commission is responsible for the personal data of the organisers contained in the Register of citizens' initiatives.

### III.3.5. Ensuring 'accountability' for data protection compliance

For each of the requirements to ensure compliance with data protection rules, the following section sets out the rules under the current regime as well as under the GDPR, before specifying how these apply to the ECI.

#### General duties

***The rules***

Under the current EU data protection instruments, controllers already have a general duty to ensure that their personal data processing operations are in accordance with the basic rules and principles in the applicable instrument: cf. Art. 6(2) of the 1995 Data Protection Directive; Art. 4(2) of Regulation (EC) 45/2001. For EU institutions, this already extends to a duty on the part of each EU institution controller to record the main aspects of its operations in a register and (with the help of the institution's Data Protection Officer, discussed at iii, below) assess whether those operations are in fact in accordance with the Regulation (cf. Art. 25 of Regulation (EC) 45/2001).

For controllers currently subject to the 1995 Data Protection Directive (i.e., in the context of ECIs, organisers and national authorities involved in certification of Online Collection Systems and in verification of statements of support), the General Data Protection Regulation will significantly tighten up the broadly-phrased duties, both in general, under a new principle of "accountability" (as discussed in this sub-section) and in relation to a new duty to appoint Data Protection Officers and/or carry out Data Protection Impact Assessments where applicable.

The new principle is set out in the GDPR as follows:

> The controller shall be responsible for, and [shall] be able to demonstrate compliance with, [the principles relating to processing of personal data] ('accountability')" (Art. 5(2)).

The core new requirement is the duty on the part of controllers to **demonstrate** that they comply with the new rules. In various contexts, this will or may require them to keep detailed records of all their personal data processing operations; adopt appropriate technical and organisational measures (and record those); draft and implement data protection policies and statements; conclude agreements with other controllers (in case of joint control) and processors; adopt data transfer clauses if any data are transferred out of the EU/EEA; etc.

***Application of the rules to ECIs***

The *various entities involved in an ECI – organisers, certification authorities, the Commission, national verification authorities and other national authorities involved in verification of statements of support – will need to be able to "demonstrate compliance" with the relevant EU data instrument – for organisers and national authorities: the GDPR; for the EU bodies involved:*

*Regulation (EC) 45/2001 – in respect of the operations for which they are responsible as (sole or joint) controller or processor.*

**Data Protection Officers**

***The rules***

The currently still applicable 1995 Data Protection Directive does not require public- or private-sector controllers subject to it to appoint Data Protection Officers or Officials (DPOs), but allows Member States to exempt controllers from the requirement of notification of their operation (or to allow simplified notification) if they have appointed such an official (Art. 18(2), second indent) – and many, especially large and/or multinational companies have appointed a DPO (or a Chief Information Officer, CIO, also responsible for other data-related issues such as freedom of information requests).

In Member States that have adopted this approach, such as Germany (where the institution of Data Protection Officer originates and where it is mandatory for all public entities and for any company of a designated size or involved in significant processing of personal data),[34] the Directive stipulates that that person must be responsible, in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to the Directive; and
- for keeping a register of processing operations carried out by the controller, containing various details of those operations

If a controller who is subject to the Directive and who has appointed a Data Protection Official (as it is called in the Directive) wants to undertake processing that is "likely to present specific risks to the rights and freedoms of data subjects", it is this DPO who should notify the national data protection authority of this, so that the latter can carry out a "prior check" of the proposed operation (Art. 20).

From May 2018, the General Data Protection Regulation requires the appointment of a Data Protection Officer by all public authorities or bodies involved in the processing of personal data subject to that instrument (except for courts acting in their judicial capacity) (Art. 37(1)(a) GDPR), but for private-sector controllers only in certain cases, i.e.:

- when the **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, **require regular and systematic monitoring of data subjects** on **a large scale**; or
- when the **core activities** of the controller or the processor consist of **processing on a large scale of special categories of data pursuant to Article 9 [i.e., of so-called 'sensitive data']** or of **personal data relating to criminal convictions and offences** referred to in Article 10.

  *(Article 37(1)(b) and (c) GDPR)*

EU institutions – or to be precise, entities and units within the EU institutions – are all already required to appoint DPOs. The EU institution's Data Protection Officer must maintain this record; check that the reported information indicates that the data and the processing conform to the relevant rules (i.e., for EU institutions, Regulation (EC) 45/2001); and crucially, also make sure that the rules are complied with in practice. Moreover, as made clear in Article 24(1)(e), the DPO must "notify[..] the European Data Protection Supervisor of [any] processing operations [supervised by that DPO] likely to present specific risks within the meaning of Article 27" (i.e., "risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their

[34] For a brief description in English of the role and functions of the DPO under German law, see, e.g., this summary by law firm Wilde-Beuger-Solmecke:
https://www.wbs-law.de/eng/practice-areas/internet-law/it-law/data-protection-officer/
For a more detailed summary in German, see the Däubler/Klebe/Wedde/Weichert Short Commentary on the German Federal Data Protection Law (Kompaktkommentar zum BDSG), 3rd. ed., comments on §4f BDSG, comprising 85 margin notes, pp. 187 – 213.

purposes"); and the EDPS must then perform a "prior check" of the operation, as again discussed in the next sub-section.

***Application of the rules to ECIs***

The Commission service involved in ECIs has been required to have a DPO supervising their personal data processing operations, as required by Regulation (EC) 45/2001. The Commission (specifically: its Secretariat-General) has registered the Register of citizens' initiatives as a personal data file with the Commission's data protection officer, recording that it lists the details of ECI organisers[35]. Given that the Commission is not the controller of the processing as regards online collection systems hosted on its servers (i.e. the organisers of an ECI remain controllers of their Commission-hosted system, with the Commission only acting as processor on their behalf).), no notification was needed. This is explained in the DPO notification as regards the Register of citizens' initiatives.

Under the GDPR, the national public authorities involved in ECIs – i.e. the certification authorities, the verification authorities, and the other public authorities involved in verification – will all also have to appoint a DPO by next May (if they have not already done so).

The main question is whether organisers will have to appoint a DPO under the GDPR. Under the GDPR, a DPO is required when processing special categories of data ("sensitive data") on a large scale. In the light of the views of the Italian and German data protection authorities that the personal data processed in relation to an ECI "can" constitute "sensitive data" within the meaning of the GDPR, it would appear that depending on the subject of an ECI the "core activities" of the organisers "consist of processing [of such sensitive data] on a large scale". This would be the case for ECIs which are manifestly "political" or related to other "sensitive" issues such as religion, but also possibly other issues, depending on the broader context of the initiative. From this, it would follow that the organisers of those initiatives should appoint a DPO to advise them on the data protection implications of their activities and to supervise them. Note that the GDPR does not exempt controllers that only process data manually from the duty to appoint a DPO.

**Prior Checks, Data Protection Impact Assessments and Prior Consultation**

***The rules***

The 1995 Data Protection Directive envisages the carrying out of "**prior checks**" of "**processing operations likely to present specific risks to the rights and freedoms of data subjects**" by the national data protection authority but leaves it to the Member States to determine what kinds of operations present such risks (Art. 20). If a controller has appointed a Data Protection Official (as it is called in the Directive), it will be that official who notifies the DPA; otherwise, the controller as such must do so (e.g., through its general counsel) (*idem*).

The "prior check" system is regulated differently in the different laws of the Member States implementing the Directive, and in the different Member States can have different effects:[36]

> *[Notification of a processing operations for prior checking purposes (as per Article 20 of the Directive)] is regulated by specific provisions laid down in domestic laws, and usually results into issuing of a prior opinion, an authorisation or permit by the competent data protection authority or an opinion by a data protection official who in case of doubt must consult the supervisory authority.*

The General Data Protection Regulation expands significantly on this, and provides for a more harmonised system of in-depth checks. It first of all, under the general principle of "accountability" discussed above, at VI.ii, requires controllers to carry out a **risk assessment** for all of their processing operations (cf. Art. 24(1) GDPR). If this shows that "**the processing**

[35] See: http://ec.europa.eu/dpo-register/details.htm?id=44647
[36] Article 29 Working Party, Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union, WP106, 18 January 2005, p. 6.

**is likely to result in a high risk to the rights and freedoms of natural persons**", the controller must, prior to the processing, carry out a **data protection impact assessment** (DPIA) of the impact of the envisaged processing operations on the protection of personal data (and on those rights and freedoms).

The GDPR does not charge the DPO (where one has been appointed) with the carrying out of such DPIAs or the writing of such DPIA documents. Rather, the DPO is tasked with "provid[ing] advice where requested as regards the data protection impact assessment and monitor its performance" (Art. 39(1)(c) GDPR). However, in practice the DPO is likely to fulfil a core role in such assessments and, as noted, that official must in any case "monitor the performance" of the assessment – i.e., must ensure that in practice measures are taken to mitigate any risks identified in the assessment. Indeed, apart from identifying the risks, working out those practical measures is of course the main aim of the assessment; and the DPO (where one has been appointed) will have a central role in both.

If the DPIA establishes that "the processing [will] result in a high risk *in the absence of [such risk-mitigating] measures*", the controller must consult the relevant supervisory (= data protection) authority (or -authorities if the processing is transnational) (Art. 36 GDPR). In other words, if the controller (and its DPO) manage to identify and implement adequate measures to mitigate even "high risks", they need not consult the DPA (or DPAs). The responsibility rest on the controllers in terms of deciding what mitigating measures are effective and sufficient: the DPIA document should spell out those conclusions.

If there are doubts – or even, if the DPO feels it would simply be helpful – the controller and its DPO should opt for consulting the DPA(s) over "risky" operations, even if they feel that they may have identified appropriate mitigating factors – just to have that view confirmed. The GDPR expressly confirms that DPOs should consult the relevant DPA(s) "where appropriate" with regard to any personal data processing-related matter, not just in relation to DPIAs (Art. 39(1)(e)).

Since the entering into force of Regulation (EC) 45/2001, the EU institutions have already been required to instruct their DPOs to ask the European Data Protection Supervisor to carry out a "**prior check**" of any proposed **personal data processing operations that are "likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes"** (Art. 27(1) of the Regulation). If a DPO is in doubt as to whether or not a proposed operation involves such risks, he/she should consult the EDPS on the matter (Art. 27(3)).

Upon receiving such a request (notification), the EDPS issues, within two months (extendable by another two months), its **opinion** on the proposed operation; and in this, it can make **proposals** to avoid any breach of the rules in Regulation (EC) 45/2001 (Art. 27(4)).

### *Application of the rules to ECIs*

The question of whether, for each of the various entities involved in ECIs, the specific processing operations for which they are responsible (as indicated in the previous section) present "specific" or "high" risks to the rights and interests of the relevant data subjects – and whether they must therefore take special steps – must be answered separately for each of them.

However, leaving aside the current regime under the 1995 Data Protection Directive, which will soon be redundant, in each case the answers to this question turn mainly on whether the relevant entity, in its ECI-related activities, carries out "processing on a large scale of special categories of data" (i.e., of sensitive data) (GDPR) or whether the "nature, scope or purposes" of the processing poses such risks (Regulation (EC) 45/2001). Given the close interplay between the different EU data protection instruments, it may be assumed that "processing on a large scale of special categories of data" (i.e., of sensitive data) by EU institutions will also be deemed to inherently present "specific" (and indeed "high") risks because of the "nature" of the data, even if Regulation (EC) 45/2001 does not specifically mention it as an inherently risky process.

This means that any of the entities involved in ECIs who can be said to carry out such large-scale processing of sensitive data in their ECI-related activities should, in view of the coming

into full force of the GDPR in May 2018, take the additional steps mentioned. These steps are detailed in the conclusion to this chapter.

### III.3.6. Liability under the ECI

***The current rules in relation to data protection***

Article 23(1) of the 1995 Directive stipulates that:

> *Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.*

This left it entirely to the Member States to determine the nature and form of the relevant process in which this compensation could be awarded, and indeed whether non-material damages were included in the stipulation (although it has since been clarified that they are).[37] It also did not clarify the allocation of liability in cases of damage of processing involving several different entities.

***Rules under ECI Regulation***

In his Opinion, the EDPS welcomed the fact that the proposal for an ECI Regulation not only reaffirmed the principle but also provided some further clarification on the appropriate process:

> In Article 13 [of the proposed ECI Regulation] it is stated that the Member States must ensure that the organisers resident or established on their territory shall be **liable under their civil or criminal law** for infringements of the proposed Regulation and in particular for, inter alia, non-conformity with the requirements for online collection systems or the fraudulent use of data. In Recital 19 reference is made to Chapter III of Directive 95/46/EC which deals with judicial remedies, liability and sanctions and states that this chapter is fully applicable as regards the data processing carried out in application of the proposed Regulation. Article 13 of the proposal must be seen as an addition to this referring explicitly, contrary to Chapter III of Directive 95/46/EC, to the civil and criminal law of the Member States. The EDPS obviously welcomes this provision. (Para. 28, emphasis added)

However, this explicit reference to "civil and criminal law" was removed from the final text of the ECI Regulation, as adopted, which deals separately with "liability" and "penalties" without using those terms. Article 13 simply reads:

> *Organisers shall be liable for any damage they cause in the organisation of a citizens' initiative in accordance with applicable national law.*

Particularly problematic in this final text is the lack of qualification in Article 13. It makes organisers liable, not just for damages that result from "infringements of [the] Regulation" and in particular for, *inter alia*, "non-conformity with the requirements for online collection systems" or "the fraudulent use of data" (as envisaged in the Draft ECI Regulation), but for any damages "cause[d] in the organisation of a citizens' initiative", "in accordance with applicable national law". There is no requirement of malicious intent, culpability or negligence, or even that the

[37] In almost all Member States, the right to compensation always extended to both material and immaterial damages caused by breaches of the law implementing the 1995 Data Protection Directive. However, under the UK's 1998 Data Protection Act, compensation for immaterial damages ("distress") could only be awarded if there had also been material damages. However, in 2015 the Court of Appeal ruled, in the case of *Vidal-Hall v Google*, that the UK limitation was in breach of the 1995 DP Directive, and should be set aside, so that compensation under the DPA can now be awarded for distress alone. See: https://www.burges-salmon.com/news-and-insight/legal-updates/damages-for-distressed-data-subjects-google-withdraws-its-appeal/

damage must have been caused by non-compliance by the organisers with the requirements of the ECI Regulation. Not surprisingly, this has worried some organisers.

This question is linked to the issue of the status of the entities involved in an ECI, as discussed above, at III.3.4, since (as the EDPS also noted) one main effect of designating someone as a controller under data protection law is that that designated entity "has primary responsibility for compliance with data protection rules", and carries primary liability for damage resulting from breaches of data protection law (even if, if the damage was caused by an agent of that controller, including a processor, the controller may be able to recoup any moneys awarded).

***Future rules: the GDPR***

The GDPR once again expands on and strengthens the provisions of the 1995 Directive, in Article 82. Para. (1) first of all makes it explicitly clear that:

> *Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*

Paras. (2) – (5) furthermore deal with cases involving more than one controller or processor, or both a controller and a processor, and imposes so-called joint and several liability in such cases (Art. 82(4)), while adding that:

> *A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. (Art. 82(3))*

Moreover, Article 82(6) clarifies that the issues are to be determined in courts of law (rather than in non-judicial proceedings), although it is left to the Member States to determine which court or courts shall be competent to deal with relevant cases.

### III.3.7. Conclusion

In any processing of personal data related to ECIs, the national authorities involved – the certification authorities, the verification authorities and the other public bodies involved in verification – are subject to their own national data protection laws and, in relation to the GDPR, to that instrument and any national rules implementing provisions of that instrument that allow the Member States to define the application of those rules more precisely, and to any further, special data-related restrictions imposed by the ECI Regulation. The Commission is in this regard subject to Regulation (EC) 45/2001 and the special data-related provisions in the ECI Regulation.

The situation of organisers is more complex in terms of applicable law, and because there will still be differences between the Member States, even after the GDPR comes fully into force in May 2018, this causes difficulties. Although most of these could perhaps be resolved through the new consultation, cooperation and consistency mechanisms in the GDPR, and/or by the new European Data Protection Board (EDPB), that would be cumbersome and time-consuming.

**It would therefore be better if any revised version of the ECI Regulation could expressly stipulate the applicable law for any processing of personal data by ECI organisers within the ECI process.**

The various entities involved in an ECI – organisers, certification authorities, the Commission, national verification authorities and other national authorities involved in verification of statements of support – will need to be able to "demonstrate compliance" with the relevant EU data instrument – for organisers and national authorities: the GDPR; for the EU bodies involved: Regulation (EC) 45/2001 – in respect of the operations for which they are responsible as (sole or joint) controller or processor.

For organisers, specifically, this includes in particular that they had to be diligent in terms of collecting statements of support, in preventing abuse or fraud by their own staff or volunteers, and in handling, storing and transferring the paper statements carefully and securely and

maintaining their integrity (e.g. in ensuring that statements of support collected for a particular ECI are not used for another ECI or some other popular initiative).

The other entities involved – certification authorities, the Commission, national verification authorities and other national authorities involved in verification of statements of support – are all public bodies, who may be expected to already operate in accordance with clear and strict data protection- and security rules and guidance. They should generally already be able to "demonstrate compliance" with the general rules – in the case of the Commission, through the register of processing operations they are already required to keep, and the supervision from the Commission's own Data Protection Officer's guidance and reports.

**Under the GDPR**, the national public authorities involved in ECIs – i.e. the certification authorities, the verification authorities, and the other public authorities involved in verification – will all also have to appoint a DPO by May 2018 (if they have not already done so).

It appears that depending on the subject of an ECI, the "core activities" of the organisers can be said to "consist of processing [sensitive data] on a large scale". In such cases, organisers should appoint a DPO to advise them on the data protection implications of their activities and to supervise them. In those cases, organisers must carry out a risk assessment of the operations for which they are responsible (and designated as controllers). The organiser's DPO's task then essentially consists of making sure that this guidance is followed, and recording this (and any still occurring data breaches, etc.). **To make sure that this is not costly and demanding for those organisers, guidance should be offered to them.**

The national verification authorities who, together with the relevant national bodies (such as municipalities), verify statements of support, may also be said to "process sensitive data on a large scale" (even if the work of the latter authorities is limited to checking samples, they still receive all the statements). In that case, they should, under the GDPR, carry out risk assessments of all the steps involved in this (i.e., of the databases and data carriers used; the means of transferring the data to and from the local authorities; data access by staff; security measures at all the relevant premises; etc.), and identify and adopt measures aimed at mitigating any data risks. This should of course involve the DPOs of all the bodies in question (which must all appoint such officers under the GDPR by May 2018 latest).

The liabilities of the entities involved in ECIs – organisers, certification authorities, verification authorities and other national bodies involved in verification (such as municipal authorities) and the Commission are limited to their respective processing.

A revised ECI Regulation could in this regard simply but expressly cross-refer to the GDPR by stipulating that, in respect of damages resulting from breaches of data protection rules, the rules on liability in that new instrument will also apply to such liability questions under the ECI Regulation. That would also in and by itself bring the situation closer to the proposal welcomed by the EDPS, in particular by requiring judicial settlement of such claims.

In addition, there is a need to clarify the open-ended stipulation in the current ECI Regulation:

> *Organisers shall be liable for any damage they cause in the organisation of a citizens' initiative in accordance with applicable national law.*

If it were felt that imposing liability for damages on ECI organisers in respect of breaches of data protection rules is insufficient, it should first of all be made clear what other kinds of wrongful acts the legislator has in mind. If there is a need for such wider, not-data-protection-related liabilities, those liabilities should be strictly circumscribed and limited to clear civil wrongs (F: *faute*; D: *unerlaubte Handlung*) with appropriate culpability.

Organisers should be in a position to fulfil their obligations under the GDPR and would not expose themselves to excessive fines under the GDPR; whereas for the other national actors involved in ECIs (certification authorities, verification authorities and other national bodies involved in verification), the GDPR does not impose any burdens over and above what they, as public authorities, are already under in relation to any processing of personal data by them. They could/should be given practical information by the Commission or WP29 on how to perform the tasks required under the GDPR,

**Finally, to free organisers of all responsibilities as regards the online collection, a revised version of the ECI Regulation could foresee that the Commission is in charge of the online collection via a central system as well as of the transfer of the statements of support to the verification authorities.**

## III.4. Risk assessment

Building on the preceding text, this sub-section assesses the data protection and data security risks to the ECI focusing on two key steps of the ECI process: i) the collection of statements of support for an ECI (step 4); and ii) the verification of those statements of support by national authorities (step 5). The methodology used is an adaptation of the ISO/IEC 27005:2011 approach to information security risk assessment.[38] The risk assessment comprises the following sections:

- **Context establishment:** details the scope and objectives of the risk assessment.
- **Risk identification, analysis and evaluation:** based on the scope and objectives, this section details the identified risks and the components that contribute to each risk before analysing and visualising the likelihood of each risk being realised and the potential impact if each risk was realised. Furthermore, this section will evaluate the risks identified as a whole in order to identify key areas on which risk treatment should focus.
- **Risk treatment:** this section presents relevant risk treatment options for the identified risks.

### III.4.1. Context establishment

A vital component of a risk assessment concerns establishing the context in which risks can manifest. This is important to ensure that all stakeholders engaging with the risk assessment understand the context in which decisions are made and outputs are developed. As mentioned above, the key contextual elements established through this section are the **scope and objectives of the risk assessment**.

#### Scope of the risk assessment

As for all elements of the study, the **focus of the risk assessment is the ECI data requirements.** This risk assessment therefore covers data protection and security risks in steps 4-6 of the ECI process (as detailed in section III.1). More specifically, the risk assessment will consider the potential risks from the beginning of the collection of statements of support (i.e. step 4) through the delivery of statements of support to, and subsequent verification of those statements of support by, the national authorities to the submission and receipt of Member State-issued verification certificates by the Commission (step 6).

Although risks related to the other steps of the ECI process are considered out of scope for this risk assessment, these steps will need to be discussed given they can play important roles in risk mitigation. For example, one potential risk is that of fraudulent signatures resulting in the illegitimate success of an ECI; however, steps 2 and 7 of the ECI process offer inherent mitigation measures for this risk. Firstly, these steps aim to ensure an ECI is aligned to the EU's legislative capabilities, values and interests. Secondly, step 7 ensures that the success of an ECI

[38] ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. *NB the cited document, developed by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), presents guidance for information security risk management. As the context of this risk assessment goes beyond information security, it has been necessary to adapt the methodology.*

(through the collection and verification of one million statements of support) does not guarantee legislative action. This is to say that, although the assessment of specific risks will focus on the abovementioned steps of the ECI process, the **risk assessment will be considered within the context of the entire ECI process**. As such, this assessment builds on the description and analysis of the full ECI process presented through section III, incorporating, most prominently, the existing mitigation measures implemented through the process.

Furthermore, as inferred above, this assessment implements an *adapted* ISO/IEC 27005:2011 approach to information security risk assessment. Thus it considers not only data security risks but also the most pertinent risks regarding the ECI data requirements, including data protection and security-related 'business risks' which are interrelated with these risk areas. It does not cover non-data related 'business risks'.

The risk assessment considers the potential risks from **several points of view**, namely:

i) Member States with the most extensive and least extensive statement of support data requirements;
ii) ECIs using, and not using, the Commission-hosted online collection software;
iii) Statements of support submitted in paper and online.

These points of view are only mentioned where relevant. For instance, regarding point iii), the assessment of each risk assumes that a distinction between paper and online methods for the submission of statements of support is not necessary, unless explicitly stated.

The risk assessment also considers the other elements related to ancillary requirements under the Regulation, namely:

- protection of personal data under the ECI Regulation (Article 12);
- applicability of Directive 95/46/EC for organisers and competent national authorities;
- liability of organisers of ECIs for any damage caused in the organisation of a citizens' initiative (Article 13);
- applicability of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data as applicable to the processing of personal data carried out by the Commission in application of this Regulation; and
- provisions of the General Data Protection Regulation (EU) 2016/679 (GDPR).

Consistent with the ISO/IEC 27005:2011 approach to information security risk assessment[39], but adapted to the needs of this implementation, this assessment presents the following three components for each risk: i) the *agent causing the risk*; ii) the *vulnerability being exploited*; and iii) the *impact* caused by the action of the agent against the vulnerability. On the basis of expert judgement and qualitative evidence, ratings on a five-point scale are provided for the **likelihood of each risk being realised**, which considers a risk's specific causative agent and specific vulnerability, and the **impact if each risk is realised**.

Lastly, the establishment of the risk assessment's scope requires presentation of the approach to identifying: i) the stakeholders potentially at risk; and ii) the assets potentially at risk. Regarding the former, and given the potentially wide-reaching impacts of the ECI process, it is considered that no restrictions should be placed on the risk assessment regarding the stakeholder groups impacted. As such, the stakeholders potentially at risk will be assessed on a risk-by-risk basis. Regarding the latter, the key assets are the personal data being collected, stored and transferred throughout the ECI process, as well as the means used for these processes (e.g. the storage mechanisms for paper statements of support, the online collection system, the data transfer mechanisms etc.). The relevant assets will also be clarified on a risk-by-risk basis.

Usually, such a discussion on the scope of a risk assessment would also consider the risk appetite of the relevant risk handling party (i.e. a business or authority). The risk appetite defines the level of risk or types of risk that are considered acceptable and therefore do not

[39] ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management.

require risk treatment. In this instance, however, such a judgement on risk appetite will be deferred given the discussions to be held on alternative options in section VI.

#### Objectives of the risk assessment

The primary aim of the risk assessment is to identify, analyse and evaluate the most pertinent high-level pan-EU **data protection** and **data security** risks, as related to the scope outlined above. Secondly, the risk assessment aims to present **treatment options** for the risks identified. Thirdly, the risk assessment aims to inform both section VI, namely the **assessment of alternative options for the ECI data requirements**.

### III.4.2. Risk identification, analysis and evaluation

Guided by the scope and objectives outlined above, the study team has examined the ECI process for high-level data protection and data security risks. This section presents the twenty one risks identified. Brief descriptions of each risk are presented in Box 2.

**Box 2: Risks to the ECI identified as per the scope and objectives of the risk assessment exercise.**

**Risks identified by the risk assessment**

**Risk 1:** Spanning three key steps of the ECI process (i.e. step 1: formation of a citizens' initiative; step 2: registration of the proposed initiative; and step 4: collection of statements of support), the first risk identified concerns the establishment of a fraudulent ECI for the express purpose of collecting and misusing the personal data of EU citizens.

**Risks 2 and 3:** Intrinsically linked, risks 2 and 3 relate to excessive data collection through the collection of statements of support (step 4).

**Risk 2:** Concerns the potential impact that the ECI requires signatories to provide too many data;

**Risk 3:** Concerns the potential impact of the ECI requiring signatories to provide data that are perceived as too sensitive.

**Risk 4** concerns the possibility for fraudulent activities being undertaken to illegitimately increase support for an ECI (i.e. impersonation through the submission of large numbers of fake statements of support purporting to be from real people). This is especially pertinent for the submission of online statements of support.

**Risk 5:** In a similar, but inverse, fashion to the previous risk, risk 5 concerns the possibility for fraudulent activities being undertaken to undermine support for an ECI (e.g. Denial of Service-type attacks or the submission of obviously fraudulent statements of support). As above, this is especially pertinent for the submission of online statements of support.

**Risk 6:** Due to the variable data requirements for the submission of ECI statements of support across the Member States, as stipulated through Annex III to the ECI Regulation, and different perception of sensitivity of these data in different Member States, engagement with the ECI may be higher in certain Member States (i.e. those with less sensitive / fewer data requirements) and thus restricted in others (i.e. those with more data requirements or where required data are perceived as more sensitive).

**Risk 7-15:** Relevant to the collection of statements of support (step 4), risks 7-15 concern the security of personal data, as collected through paper (risks 7-9) and online (risks 10-15) statements of support, while being **stored**.

**Risk 7:** Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when *stored* ;

**Risk 8:** Modification of citizens' data from ECI statements of support collected *on paper,*

when *stored* ;;

**Risk 9:** Destruction of citizens' data from ECI statements of support collected *on paper,* when *stored* ;;

**Risk 10:** Interception / theft / loss of *stored* personal data, submitted through *online* statements of support. Under this risk, the storage of signatories' personal data is considered in relation to the **online collection systems based on hosting provided by third parties** and online collection software provided either by the Commission or third-parties;

**Risk 11:** Modification of *stored* personal data, submitted through *online* statements of support. Under this risk, the storage of signatories' personal data is considered in relation to the **online collection systems based on hosting provided by third parties** and online collection software provided either by the Commission or third-parties;

**Risk 12:** Destruction of *stored* personal data, submitted through *online* statements of support. Under this risk, the storage of signatories' personal data is considered in relation to the **online collection systems based on hosting provided by third parties** and online collection software provided either by the Commission or third-parties;

**Risk 13:** Interception / theft / loss of *stored* personal data, submitted through *online* statements of support. Under this risk, the storage of signatories' personal data is considered in relation to **online collection systems based on the hosting and online collection software provided by the Commission**;

**Risk 14:** Modification of *stored* personal data, submitted through *online* statements of support. Under this risk, the storage of signatories' personal data is considered in relation to **online collection systems based on the hosting and online collection software provided by the Commission**;

**Risk 15:** Destruction of *stored* personal data, submitted through *online* statements of support. Under this risk, the storage of signatories' personal data is considered in relation to **online collection systems based on the hosting and online collection software provided by the Commission**.

**Risks 16-21:** Relevant to the verification of statements of support (step 5), risks 16-21 concern the security of personal data, as collected through paper (risks 16-18) and online (19-21) statements of support, while **in transit** to national authorities for verification.

**Risk 16:** Interception / theft / loss of personal data *in transit*, submitted through *paper* statements of support;

**Risk 17:** Modification of personal data *in transit*, submitted through *paper* statements of support;

**Risk 18:** Destruction of personal data *in transit*, submitted through *paper* statements of support;

**Risk 19:** Interception / theft / loss of personal data *in transit*, submitted through *online* statements of support;

**Risk 20:** Modification of personal data *in transit*, submitted through *online* statements of support;

**Risk 21:** Destruction of personal data *in transit*, submitted through *online* statements of support.

As is demonstrated in the above box, the majority of identified risks are relevant to step 4 of the ECI process, the collection of statements of support. This is due to the fact that the **primary asset of the ECI is the personal data of signatories**, which are collected and stored as part of step 4.

The remainder of this section will detail how the risks have been identified before additional information is provided on each risk. As such, for a risk to be considered as a risk, it needs to comprise three key parts:

i. **Causative agent:** Such an agent may be accidental (termed a hazard) or may have malicious intent (termed a threat). For example, a threat might be the purposeful submission of fraudulent statements of support for an ECI.

ii. **Vulnerability:** For each relevant action within the scope of the risk assessment, the existence of vulnerabilities will be assessed and presented. For example, vulnerabilities may be physical (e.g. unconstrained access to buildings where paper statements of support are held), procedural (e.g. no checking that statements of support have actually been received by a national authority), in personnel (e.g. absence of adequate checks on personnel) or logical (e.g. software bugs in an online collection system that could permit unauthorised access).

At this point it should be noted that an assessment of the **likelihood of a risk** being realised will be conducted based on a combination of each specific causative agent (point i) and specific vulnerabilities (point ii).

iii. **Impact:** The final characteristic of a risk is that it must cause an impact. In standard information security terminology, the identified impacts are referred to in terms of damage to confidentiality, integrity and availability. Although this approach will be used to the extent possible, a certain flexibility is proposed in describing the **types of risks** given that the risk assessment is not restricted to information security. Assessment of this part will also include the **assessment of the stakeholders impacted**.

Furthermore, if any of these three parts are absent, there is no risk.

Assessing the possibilities related to these three key elements across the ECI led to the identification of the eighteen risks listed above. In Table 10, below, these twenty one risks are elaborated further, with information presented on the characteristics of each risk (i.e. the risk type); the three key risk components (i.e. the causative agent, the vulnerability and the impact); and the stakeholders impacted.

**Table 10: Risk identification and analysis: Risk components, types and stakeholders impacted.**

| Risk type | Causative agent | Vulnerability | Potential impact | Stakeholders impacted |
|---|---|---|---|---|
| **R1: Formulation of a fake ECI in order to collect and misuse personal data** | | | | |
| Risk to the confidentiality of the personal data of EU citizens | Malicious actor seeking to steal the personal data of EU citizens | Any group of at least seven citizens can form an ECI, given they meet the criteria set out in the ECI Regulation | Potential theft of personal data of up to 1 million EU citizens | Signatories to the fraudulent ECI |
| **R2: Reduced ECI participation as citizens are required to provide too many data** | | | | |
| Excessive data collection, data protection risk | Relates to the perception that the ECI Regulation requires that EU citizens provide too many data[40] | | Potential to reduce ECI participation | ECI as a whole |
| **R3: Reduced ECI participation as citizens are required to provide data perceived as too sensitive** | | | | |
| Excessive data collection, data protection risk | Relates to the perception that the ECI Regulation requires that EU citizens provide too sensitive data | | Potential to reduce ECI participation | ECI as a whole |
| **R4: Fraudulent activities to increase support for an ECI** | | | | |
| Risk to the integrity of the personal data of EU citizens | Malicious actor seeking to increase the registered number of statements of support for an ECI | Lack of verification against impersonation: i) in the ECI Regulation; and ii) in practice in most Member States. This is more pertinent for statements of support collected online, although it is also relevant to a lesser extent for paper statements of support | Potential to change the outcome of an ECI, thus initiating step 7 of the ECI process and potentially a legislative change | The individuals impersonated; the European Parliament and the European Commission (i.e. step 7); depending on the progress at step 7, potentially the entire EU |
| **R5: Fraudulent activities to undermine an ECI** | | | | |
| Risk to the availability and / or integrity of the personal data of EU | Malicious actor seeking to decrease the registered number of statements of | Potential vulnerabilities of the Online Collection System used to instigate such attacks, and any fraud detection measures implemented.[41] This is more | Potential to change the outcome of an ECI, thus preventing the success of an ECI and potentially | ECI organisers and potentially the entire EU |

[40] Given the adaptation of information security methodology to non-information security risks, it is not possible to define causative agents and vulnerabilities for all identified risks. In these instances, the table describes the reasons that the risk exists.

[41] In this instance, any fraud detection measures can be exploited to undermine an ECI by submitting obviously fraudulent statements of support and thus either: i) appearing to inflate the statement of support count with the ultimate result of the fraudulently submitted statements

| Risk type | Causative agent | Vulnerability | Potential impact | Stakeholders impacted |
|---|---|---|---|---|
| citizens | support for an ECI | pertinent for statements of support collected online, although the risk exists to a lesser extent for paper statements of support. A further related vulnerability is the potential for a third-party hosted Online Collection System to be amended after certification and reduce its security | valid EU legislative changes | |
| **R6: Polarisation of Member State (and citizen) engagement with the ECI** | | | | |
| Excessive data collection, data protection risk | Relates to the perception that variable data requirements across Member States could impact engagement with the ECI in Member States with heavy data requirements | | Potential isolation of Member States (and thus citizens) from involvement in the ECI | ECI as whole; citizens in Member States affected |
| **R7-15: Risks to the security of stored citizens' data – paper (R7-9) and online (R10-15)** | | | | |
| **R7: Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when stored** | | | | |
| Risk to the confidentiality of the personal data of EU citizens | Unauthorised access to the personal data of EU citizens (i.e. either malicious or accidental) | Any vulnerabilities in the process used for storing paper statements of support | Data protection breach and potential misuse of personal data of up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |
| **R8: Modification of citizens' data from ECI statements of support collected *on paper,* when stored** | | | | |
| Risk to the integrity of the personal data of EU citizens | Unauthorised access to and modification of the personal data of EU citizens (i.e. either malicious or accidental) | Any vulnerabilities in the process used for storing paper statements of support | Data protection breach related to the modification of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |
| **R9: Destruction of citizens' data from ECI statements of support collected *on paper,* when stored** | | | | |

of support being rejected upon verification; or ii) the obviously fraudulent statements of support are detected and lead to the invalidation of the ECI.

| Risk type | Causative agent | Vulnerability | Potential impact | Stakeholders impacted |
|---|---|---|---|---|
| Risk to the availability of the personal data of EU citizens | Unauthorised access to and destruction of the personal data of EU citizens (i.e. either malicious or accidental) | Any vulnerabilities in the process used for storing paper statements of support | Data protection breach related to the destruction of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |
| **R10: Interception / theft / loss of citizens' data from ECI statements of support collected *online*, when stored (third-party hosting)** | | | | |
| Risk to the confidentiality of the personal data of EU citizens | Unauthorised access to the personal data of EU citizens (i.e. either malicious or accidental) | Any technical, procedural or personnel vulnerabilities in the online collection system used to store online statements of support. A further related vulnerability is the potential for a third-party hosted Online Collection System to be amended after certification and reduce its security | Data protection breach and potential misuse of personal data of up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |
| **R11: Modification of citizens' data from ECI statements of support collected *online*, when stored (third-party hosting)** | | | | |
| Risk to the integrity of the personal data of EU citizens | Unauthorised access to and modification of the personal data of EU citizens (i.e. either malicious or accidental) | Any technical, procedural or personnel vulnerabilities in the online collection system used to store online statements of support. A further related vulnerability is the potential for a third-party hosted Online Collection System to be amended after certification and reduce its security | Data protection breach related to the modification of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |
| **R12: Destruction of citizens' data from ECI statements of support collected *online*, when stored (third-party hosting)** | | | | |
| Risk to the availability of the personal data of EU citizens | Unauthorised access to and destruction of the personal data of EU citizens (i.e. either malicious or accidental) | Any technical, procedural or personnel vulnerabilities in the online collection system used to store online statements of support. A further related vulnerability is the potential for a third-party hosted Online Collection System to be amended after certification and reduce its security | Data protection breach related to the destruction of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |
| **R13: Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software)** | | | | |
| Risk to the confidentiality of the personal data of EU | Unauthorised access to the personal data of EU citizens | Any technical, procedural or personnel vulnerabilities in the online collection | Data protection breach and potential misuse of | Signatories of the ECI in question; the ECI itself; and the |

| Risk type | Causative agent | Vulnerability | Potential impact | Stakeholders impacted |
|---|---|---|---|---|
| citizens | (i.e. either malicious or accidental) | software used to store online statements of support. | personal data of up to 1 million EU citizens, and potential invalidation of an ECI | entity liable for the data (i.e. ECI organiser or European Commission) |
| **R14: Modification of citizens' data, from ECI statements of support collected *online,* when stored (Commission hosting and software)** | | | | |
| Risk to the integrity of the personal data of EU citizens | Unauthorised access to and modification of the personal data of EU citizens (i.e. either malicious or accidental) | Any technical, procedural or personnel vulnerabilities in the online collection system used to store online statements of support. | Data protection breach related to the modification of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the entity liable for the data (i.e. ECI organiser or European Commission) |
| **R15: Destruction of citizens' data, from ECI statements of support collected *online,* when stored (Commission hosting and software)** | | | | |
| Risk to the availability of the personal data of EU citizens | Unauthorised access to and destruction of the personal data of EU citizens (i.e. either malicious or accidental) | Any technical, procedural or personnel vulnerabilities in the online collection system used to store online statements of support. | Data protection breach related to the destruction of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the entity liable for the data (i.e. ECI organiser or European Commission) |
| **R16-21: Risks to the security of citizens' data in transit – paper (R16-18) and online (R19-21)** | | | | |
| **R16: Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when in transit** | | | | |
| Risk to the confidentiality of the personal data of EU citizens | Unauthorised access to the personal data of EU citizens (i.e. either malicious or accidental) | Any vulnerability associated with the need for ECI organisers to securely transfer paper statements of support to national authorities, | Data protection breach and potential misuse of personal data of up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |
| **R17: Modification of citizens' data from ECI statements of support collected *on paper,* when in transit** | | | | |
| Risk to the integrity of the personal data of EU citizens | Unauthorised access to and modification of the personal data of EU citizens (i.e. either malicious or accidental) | Any vulnerability associated with the need for ECI organisers to securely transfer paper statements of support to national authorities | Data protection breach related to the modification of personal data belonging to up to 1 million EU citizens, and potential | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |

| Risk type | Causative agent | Vulnerability | Potential impact | Stakeholders impacted |
|---|---|---|---|---|
| | | | invalidation of an ECI | |
| **R18: Destruction of citizens' data from ECI statements of support collected *on paper,* when in transit** | | | | |
| Risk to the availability of the personal data of EU citizens | Unauthorised access to and destruction of the personal data of EU citizens (i.e. either malicious or accidental) | Any vulnerability associated with the need for ECI organisers to securely transfer paper statements of support to national authorities | Data protection breach related to the destruction of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the data |
| **R19: Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when in transit** | | | | |
| Risk to the confidentiality of the personal data of EU citizens | Unauthorised access to the personal data of EU citizens (i.e. either malicious or accidental) | Any vulnerability associated with the need for ECI organisers to securely transfer online statements of support to national authorities.<br>More specifically, the need to transfer the statement of support data twice, first from the system to the organisers and then from the organisers to the competent national authorities, is a vulnerability.<br>Furthermore, when a third-party hosted online collection system is used, it can potentially be amended after certification, which could result in reduced security when transferring data | Data protection breach and potential misuse of personal data of up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the secure transfer of the data |
| **R20: Modification of citizens' data from ECI statements of support collected *online,* when in transit** | | | | |
| Risk to the integrity of the personal data of EU citizens | Unauthorised access to and modification of the personal data of EU citizens (i.e. either malicious or accidental) | Need for ECI organisers to securely transfer online statements of support to national authorities.<br>More specifically, the need to transfer the statement of support data twice, first from the system to the organisers and then from the organisers to the competent national authorities, is a | Data protection breach related to the modification of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the secure transfer of the data |

| Risk type | Causative agent | Vulnerability | Potential impact | Stakeholders impacted |
|---|---|---|---|---|
| | | vulnerability.<br><br>Furthermore, when a third-party hosted online collection system is used, it can potentially be amended after certification, which could result in reduced security when transferring data | | |
| **R21: Destruction of citizens' data from ECI statements of support collected *online,* when in transit** | | | | |
| Risk to the availability of the personal data of EU citizens | Unauthorised access to and destruction of the personal data of EU citizens (i.e. either malicious or accidental) | Need for ECI organisers to securely transfer online statements of support to national authorities.<br><br>More specifically, the need to transfer the statement of support data twice, first from the system to the organisers and then from the organisers to the competent national authorities, is a vulnerability.<br><br>Furthermore, when a third-party hosted online collection system is used, it can potentially be amended after certification, which could result in reduced security when transferring data | Data protection breach related to the destruction of personal data belonging to up to 1 million EU citizens, and potential invalidation of an ECI | Signatories of the ECI in question; the ECI itself; and the ECI organisers liable for the secure transfer of the data |

Upon identification of the risks, and their components, each risk has been analysed. Ratings (on a five-point scale) have been assigned for: i) the likelihood of each risk being realised; and ii) the impact if a risk is realised. These ratings are based on expert judgement and the data collected for this study, and each rating is accompanied by a rationale. The ratings and the rationales for the likelihood of each risk being realised are detailed in Table 13 below, and each judgement takes into account the specific causative agent and vulnerability described above, as well as the existing mitigation measures, which are presented, first, in Table 11 below.

The likelihood ratings are followed, in Table 14, by the ratings and rationales for the **impact if each risk is realised**. Subsequently, these ratings are visualised and analysed.

The five-point scales used are detailed below, in Table 11.

**Table 11: Risk ratings: Five-point scale qualitative definitions.**

| Score | Likelihood | Impact |
|---|---|---|
| **5** | A risk that **has been, or is anticipated to be, realised** with regularity given the specific causative agent, related assessments of potential motives and opportunity, the specific vulnerability and any existing mitigation | A risk that, if realised, will **significantly restrict** the ECIs ability to achieve its objectives, or significantly impact the process itself, key assets and/or relevant stakeholders |
| **4** | A risk that is **likely** to be realised given the specific causative agent, related assessments of potential motives and opportunity, the specific vulnerability and any existing mitigation | A risk that, if realised, will have a **high impact** on achieving the objectives of the ECI process, the process itself, its assets and the relevant stakeholders |
| **3** | A risk that has a **moderate likelihood** of being realised given the specific causative agent, related assessments of potential motives and opportunity, the specific vulnerability and any existing mitigation | A risk that, if realised, will cause a **moderate impact** on achieving the objectives of the ECI process, the process itself, its assets and the relevant stakeholders |
| **2** | A risk that is **unlikely** to be realised given the specific causative agent, related assessments of potential motives and opportunity, the specific vulnerability and any existing mitigation | A risk that, if realised, will have a **minor impact** on achieving the objectives of the ECI process, the process itself, its assets and the relevant stakeholders |
| **1** | A risk that is **highly unlikely** to be realised given the specific causative agent, related assessments of potential motives and opportunity, the specific vulnerability and any existing mitigation | A risk that, if realised, will have **negligible impact** on the objectives of the ECI process, the process itself, its assets and the relevant stakeholders |

**Table 12: Existing mitigation per risk.**

| Risk | Existing mitigation |
|---|---|
| **R1:** Formulation of a fake ECI in order to collect and misuse personal data | Extensive process for formation and registration of an ECI, including verification of the identity of members of an ECI citizens' committee by the European Commission |
| **R2:** Reduced ECI participation as citizens are required to provide too many data | No existing mitigation |
| **R3:** Reduced ECI participation as citizens are required to provide data perceived as too sensitive | No existing mitigation |
| **R4:** Fraudulent activities to increase support for an ECI | **R4-5:** Certain technical protections are in place, including the verification processes of the Member States, and with regard to the online collection process the stipulations of the technical specifications for online collection systems and the thereto related certification process[42].<br>Details of the protections provided by the European Commission's Online Collection Software are presented in the 2016 Risk Analysis.<br>No mitigation in place with regard to paper |
| **R5:** Fraudulent activities to undermine an ECI | |

[42] Commission Implementing Regulation (EU) No 1179/2011 of 17 November 2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative.

| Risk | Existing mitigation |
|---|---|
| | statements of support |
| **R6:** Polarisation of Member State (and citizen) engagement with the ECI | Minimal mitigation in that an ECI's citizens' committee must include residents of at least seven different Member States (Recital 8 and Art. 3(2), ECI Regulation) and the signatories must span at least seven Member States (Art. 7, ECI Regulation) |
| **R7:** Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when *stored* ; | **R7-9:** No specific mitigation measures foreseen in the ECI Regulation.<br>The organisers being in charge of the process and liable for relevant damages, they are presumed to design and implement the measures they consider relevant in application of the data protection legislation. |
| **R8:** Modification of citizens' data from ECI statements of support collected *on paper,* when *stored* ; | |
| **R9:** Destruction of citizens' data from ECI statements of support collected *on paper,* when *stored* ; | |
| **R10:** Interception / theft / loss of citizens' data, from ECI statements of support collected *online*, when stored (third party hosting) | **R10-12:** Technical data security measures, including the stipulations of the technical specifications for online collection systems and the thereto related certification process[43].<br>To be noted that the compliance with the technical specifications for online collection systems is only verified ex-ante at the certification stage. Online collection systems are normally not controlled against further modification.<br>The organisers being in charge of the process and liable for relevant damages, they are presumed to ensure compliance of their system with the rules throughout the process.. |
| **R11:** Modification of citizens' data, from ECI statements of support collected *online*, when stored (third party hosting) | |
| **R12:** Destruction of citizens' data, from ECI statements of support collected *online*, when stored (third party hosting) | |
| **R13:** Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | **R13-15:** Technical data security measures, including the stipulations of the technical specifications for online collection systems and the thereto related certification process.<br>Each modification in the Commission software is accompanied by the relevant vulnerability tests and risks assessments |
| **R14:** Modification of citizens' data, from ECI statements of support collected *online*, when stored (Commission hosting and software) | |
| **R15:** Destruction of citizens' data from ECI statements of support collected *online*, when stored (Commission hosting and software) | |
| R16: Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when in transit | **R16-18:** No specific mitigation measures foreseen in the ECI Regulation<br>The organisers being in charge of the transit of the data and liable for relevant damages, they are presumed to implement the measures they consider relevant in application of the data protection |
| **R17:** Modification of citizens' data from ECI statements of support collected *on paper,* when in transit | |

[43] Commission Implementing Regulation (EU) No 1179/2011 of 17 November 2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative.

| Risk | Existing mitigation |
|---|---|
| **R18:** Destruction of citizens' data from ECI statements of support collected *on paper,* when in transit | legislation. |
| **R19:** Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when in transit | **R19-21:** Technical data security measures, foreseen in the technical specifications for online collection systems<br>The organisers being in charge of the process and liable for relevant damages, they are presumed to comply with the rules. |
| **R20:** Modification of citizens' data from ECI statements of support collected *online,* when in transit | |
| **R21:** Destruction of citizens' data from ECI statements of support collected *online,* when in transit | |

**Table 13: Likelihood of risk being realised: Ratings and rationales for each ECI risk.**

| Likelihood of risk being realised | | |
|---|---|---|
| **Risk** | **Rating** | **Rationale** |
| **R1:** Formulation of a fake ECI in order to collect and misuse personal data | **1: Highly unlikely** | Appropriate mitigation is in place as the process for formation and registration of an ECI provides a significant barrier, including verification of citizens forming an ECI committee. Furthermore, there are easier ways for malicious actors to collect, often more sensitive, personal data of EU citizens. |
| **R2:** Reduced ECI participation as citizens are required to provide too many data | **5: Highly likely** | A primary incentive for this study and findings confirm that the ECI's data requirements are perceived to be too many. |
| **R3:** Reduced ECI participation as citizens are required to provide data perceived as too sensitive | **3: Moderate likelihood** | A primary incentive for this study. Findings confirm mixed perceptions on the sensitivity of the ECI's data requirements. See Chapter IV for the relevant discussion. |
| **R4:** Fraudulent activities to increase support for an ECI | **2: Unlikely** | A serious, sophisticated attack that would change the outcome of an ECI is considered unlikely. A key factor is the fact that even if such an attack was conducted, it would likely have a minimal impact, given the non-binding character of the ECI instrument. |
| **R5:** Fraudulent activities to undermine an ECI | **1: Highly unlikely** | As above, a serious, sophisticated attack that would change the outcome of an ECI is considered highly unlikely. This is primarily due to the fact that the time and effort necessary to launch such an attack would not be worth it for any attacker. Additionally, appropriate mitigation is in place. R5 is considered less likely to occur than R4 as it requires a higher level of technical resource. |
| **R6:** Polarisation of Member State (and citizen) engagement with the ECI | **2: Unlikely** | At present, this is considered unlikely. No data analysed has indicated that this is a likely risk. However, if the data requirements stay the same, and ECI organisers become more aware of the variability in these requirements and the impacts of this variability, they may initiate targeted ECI campaigns along the lines of R6, knowing that statements of support might be more |

| Likelihood of risk being realised | | |
|---|---|---|
| **Risk** | **Rating** | **Rationale** |
| | | easily achieved in certain Member States. |
| **R7:** Interception / theft / loss of citizens' data from ECI statements of support collected on paper, when stored | **2: Unlikely** | **R7-9:** On the whole, such attacks would require more effort than the reward would deliver. In order to substantiate this rationale, it is necessary to further consider the motives of such attacks.<br><br>In this regard, it is considered that such attacks would be conducted to either: i) hinder an ECI; or ii) profit from selling or utilising the personal data collected (only relevant for R7).<br><br>The likelihood of R7-9 being realised in order to fulfil the first motive (i.e. to hinder an ECI) is considered to be low given the non-binding character of the ECI instrument<br><br>Regarding the second motive, it is important to consider other additional elements: namely, the opportunity and resources required to access and misuse the personal data, and the value of these data.<br><br>In the first instance, (unauthorised) access to stored paper statements of support would need to be achieved. This could be done by: i) an insider (i.e. an ECI organiser) or ii) an external attacker. In the case of the former, access would be simple but in the latter, access would require the opportunity and the resources to conduct such an attack.<br><br>Assuming minimal protection of paper statements of support – given no specific mitigation measures are foreseen in the ECI Regulation and the protection measures implemented by ECI organisers are unknown – an external attacker may *have opportunity* but would still require certain resources to gain access and further misuse these data.<br><br>Furthermore, although there is value in the personal data held by ECI organisers, the attractiveness of these data to an attacker is reduced by a number of elements, including that: i) the value of data held on paper are less attractive to potential buyers than digitalised data and any effort taken to digitalise the data adds to the resource required by an attacker; ii) the data is not particularly attractive in comparison with many sets of personal data accessible online (which include, for example, bank details or passwords) – this is particularly true in Member States that do not require personal identification (document) numbers; and iii) in many instances, the paper data are stored separately across different Member States, thereby reducing the total sets of data available in each location.<br><br>As such, the likelihood of R7 being realised for this motive is considered to be low. However, as stated above, the opportunities afforded to potential attackers can be easily reduced through the implementation of simple additional security measures and/or guidance (see section III.4.3. and section VI). |
| **R8:** Modification of citizens' data from ECI statements of support collected on paper, when stored | **2: Unlikely** | |
| **R9:** Destruction of citizens' data from ECI statements of support collected on paper, when stored | **2: Unlikely** | |

| Likelihood of risk being realised | | |
|---|---|---|
| **Risk** | **Rating** | **Rationale** |
| **R10:** Interception / theft / loss of citizens' data from ECI statements of support collected online, when stored (third-party hosting) | **2: Unlikely** | **R10-12:** In a similar fashion to the rationale for R7-9, such attacks would require more effort than the reward would deliver. This is particularly true in light of the easier ways of accessing, often more sensitive, personal data of EU citizens.<br>Furthermore, with regard to online statements of support, significant appropriate mitigation is in place. |
| **R11:** Modification of citizens' data from ECI statements of support collected online, when stored (third-party hosting) | **2: Unlikely** | |
| **R12:** Destruction of citizens' data from ECI statements of support collected online, when stored (third-party hosting) | **2: Unlikely** | |
| **R13:** Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | **1: Highly unlikely** | **R13-15:** In a similar fashion to the rationale for R7-9, such attacks would require more effort than the reward would deliver. This is particularly true in light of the easier ways of accessing, often more sensitive, personal data of EU citizens.<br>Furthermore, with regard to online statements of support, significant appropriate mitigation is in place.<br>R13-15 are considered to be slightly less likely than R10-12 due to the fact that third party hosting environments are only certified once (prior to collection of statements of support) – although it cannot be assumed that this translates to a less secure environment, there is no known, transparent, continuous monitoring as is the case for the Commission's hosting environment. |
| **R14:** Modification of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | **1: Highly unlikely** | |
| **R15:** Destruction of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | **1: Highly unlikely** | |
| **R16:** Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when in transit | **2: Unlikely** | **R16-18:** Such attacks would require more effort than the reward would deliver – the rationale being the same as for R7-9 (i.e. risks to stored paper statement of support data). It is important to restate, however, that minimal mitigation exists in relation to the transfer of paper statements of support – hence the likelihood for these ratings is slightly higher than for those risks related to the transfer of online statements of support.<br>Although this is not considered to sufficiently impact the likelihood of such an attack, the opportunity can be reduced through the implementation of simple additional security measures / guidance (see section III.4.3. and section VI). |
| **R17:** Modification of citizens' data from ECI statements of support collected *on paper,* when in transit | **2: Unlikely** | |
| **R18:** Destruction of citizens' data from ECI statements of support collected *on paper,* when in transit | **2: Unlikely** | |
| **R19:** Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when in transit | **1: Highly unlikely** | **R19-21:** As for R16-18, such attacks would require more effort than the reward would deliver. This is particularly true in light of the easier ways of accessing, often more sensitive, personal data of EU citizens.<br>Furthermore, with regard to the transfer of online statements of support, significant appropriate mitigation is in place. |
| **R20:** Modification of citizens' data from ECI statements of support collected *online,* when in transit | **1: Highly unlikely** | |
| **R21:** Destruction of citizens' | **1: Highly** | |

| Likelihood of risk being realised | | |
|---|---|---|
| **Risk** | **Rating** | **Rationale** |
| data from ECI statements of support collected *online,* when in transit | **unlikely** | |

**Table 14: Impact if risk is realised: Ratings and rationales for each ECI risk.**

| **Impact** if risk is realised | | |
|---|---|---|
| **Risk** | **Rating** | **Rationale** |
| **R1:** Formulation of a fake ECI in order to collect and misuse personal data | **5: Significant impact** | The potential misuse of the personal data of up to, or more than, 1 million EU citizens represents a significant impact – the added sensitivity of specific data in specific Member States further adds to the impact. |
| **R2:** Reduced ECI participation as citizens are required to provide too many data | **3: Moderate impact** | **R2-3:** These risks would result in reduced ECI participation; however, the extent to which participation would be reduced is variable and is influenced by a range of external factors (e.g. topic of the ECI, the Member States in which data are being collected etc.). |
| **R3:** Reduced ECI participation as citizens are required to provide data perceived as too sensitive | **3: Moderate impact** | |
| **R4:** Fraudulent activities to increase support for an ECI | **3: Moderate impact** | The realization of R4 will, in most cases, have minimal impact (i.e. the illegitimate success of an ECI leading to initiation of step 7 of the ECI process); however, if legislation is subsequently developed, the impact would be much greater – although such a decision would be the subject of significant political discussions and necessitate the Commission to initiate a legislative proposal thus validating the illegitimate ECI. |
| **R5:** Fraudulent activities to undermine an ECI | **2: Minor impact** | This risk could result in the illegitimate invalidation of an ECI but given that most ECIs do not achieve the required number of signatories, it is highly unlikely that the realisation of this risk would have such an impact. |
| **R6:** Polarisation of Member State (and citizen) engagement with the ECI | **2: Minor impact** | The realization of R6 will result in the targeting of specific Member States by ECI organisers and thus the restriction of ECI engagement with other Member States; however, it is unlikely to impact the success of an ECI. |
| **R7:** Interception / theft / loss of citizens' data from ECI statements of support collected on paper, when stored | **5: Significant impact** | The level of impact is considered to be the same for risks 7-21. The potential theft / modification / destruction of personal data of up to, or more than, 1 million EU citizens represents a significant breach of EU data protection law.<br>Furthermore, the realisation of any of risks 7-21 for a particular ECI may lead to the invalidation of that ECI.<br>However, as detailed in Box 3 below, this level of impact is variable and dependent on a range of factors, as stipulated in Article 83(2) by the |
| **R8:** Modification of citizens' data from ECI statements of support collected on paper, when stored | **5: Significant impact** | |
| **R9:** Destruction of citizens' data from ECI statements of support collected on paper, when stored | **5: Significant impact** | |
| **R10:** Interception / theft / loss of | **5: Significant** | |

| **Impact** if risk is realised | | |
|---|---|---|
| **Risk** | **Rating** | **Rationale** |
| citizens' data from ECI statements of support collected online, when stored (third-party hosting) | **impact** | GDPR, such as the number of data subjects and the types of personal data affected. |
| **R11:** Modification of citizens' data from ECI statements of support collected online, when stored (third-party hosting) | **5: Significant impact** | |
| **R12:** Destruction of citizens' data from ECI statements of support collected online, when stored (third-party hosting) | **5: Significant impact** | |
| **R13:** Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | **5: Significant impact** | |
| **R14:** Modification of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | **5: Significant impact** | |
| **R15:** Destruction of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | **5: Significant impact** | |
| **R16:** Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when in transit | **5: Significant impact** | |
| **R17:** Modification of citizens' data from ECI statements of support collected *on paper,* when in transit | **5: Significant impact** | |
| **R18:** Destruction of citizens' data from ECI statements of support collected *on paper,* when in transit | **5: Significant impact** | |
| **R19:** Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when in transit | **5: Significant impact** | |
| **R20:** Modification of citizens' data from ECI statements of support collected *online,* when in transit | **5: Significant impact** | |
| **R21:** Destruction of citizens' data from ECI statements of support collected *online,* when in transit | **5: Significant impact** | |

**Box 3: Impact ratings for R7-18 – potential influence of the GDPR.**

**Potential influence of the General Data Protection Regulation[44] on the impact ratings for risks 7-12 and risks 16-21[45]**

**EU data protection law does not differentiate between the risks described through risks 7-12 and risks 16-21** (i.e. risks that impact the confidentiality, integrity or availability of the personal data of EU citizens) – as such, the risk levels, in general, are considered to be the same. However, the gravity of a breach becomes a factor in any decision on associated penalties, which can be administered in addition to, or instead of, the corrective powers available to national level supervisory authorities, as detailed in Article 58(2), GDPR. Decisions on these additional penalties, termed 'administrative fines', are to be informed by the following article:

**Article 83(2), GDPR**

Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

b) the intentional or negligent character of the infringement;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

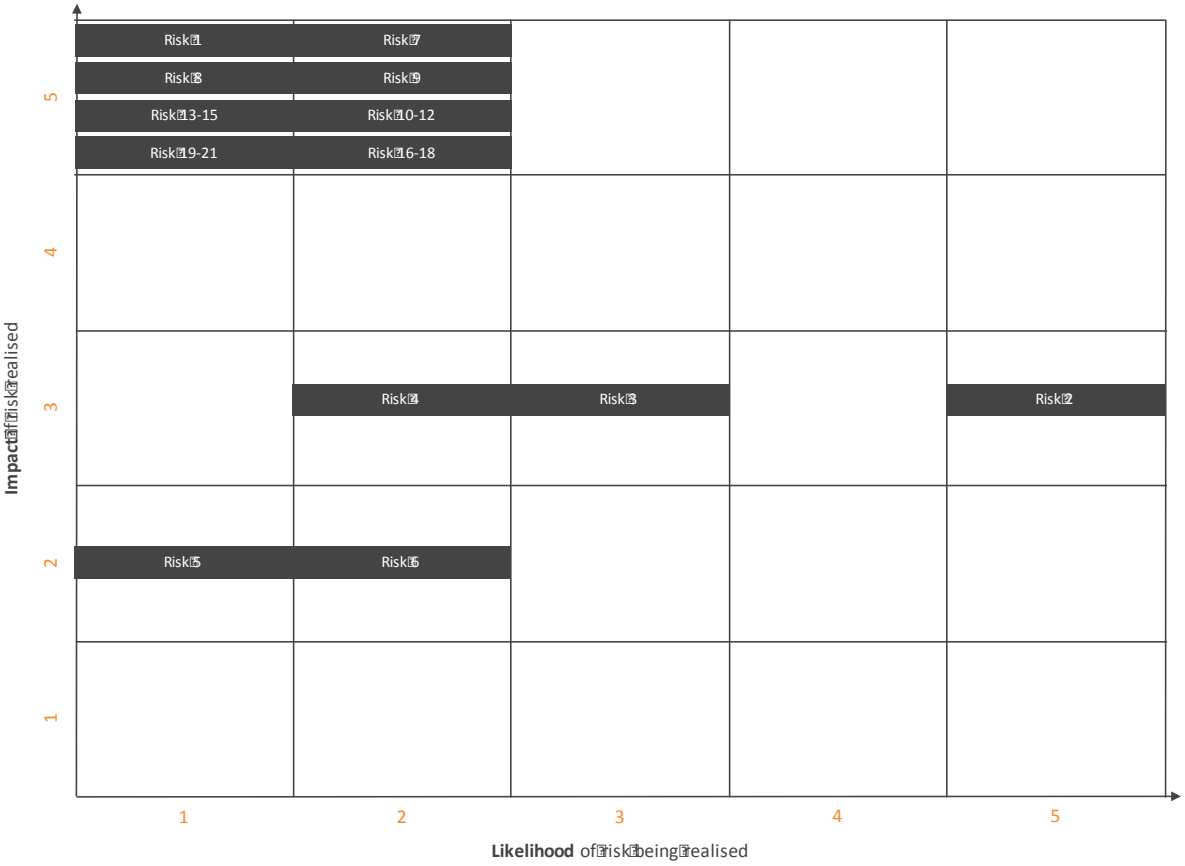
j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

[44] 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).

[45] Given the risks 13-15 relate explicitly to hosting of online statements by the European Commission, these risks will not be impacted by the GDPR. Instead, they are subject only to Regulation (EC) 45/2001.

**Figure 2: Matrix of identified risks: Likelihood of realisation (x axis) vs. Impact if realised (y axis).**




**As can be clearly seen in the above tables and the visualisation (Figure 2), the** majority of the identified risks have been assigned a low likelihood of occurring**; in fact, all but two risks (R2 and R3) have a low likelihood of being realised. The primary reason for this trend is that the reward is considered more than likely not worth the effort of instigating such an attack / activity, and thus instigating the risk. As detailed In Table 13, above, this rationale considers the motives of such attacks, namely to either: i) hinder an ECI; or ii) directly (i.e. to sell the data) or indirectly (i.e. use the data for further attacks) profit financially from the personal data obtained. The first potential motive is effectively ruled out due to the limited political impact of ECIs to date. The second potential motive is more complex as the opportunity and the resources required to access and misuses the personal data need to be considered alongside the value of the data to be collected. The considerations on these points are highlighted below in relation to both internal and external threats, and demonstrate the low likelihood of such an attack being worth the effort:**

- **Insider threat:** An inside attacker would likely have easy access to the personal data collected and would thus have **opportunity**, although this would depend on the specific data access and data handling procedures and processes implemented. However, in this case of online statements of support, certain technical knowledge (or **resources**) would be required, thus reducing the likelihood. Furthermore, although there is value in the personal data held by ECI organisers, the **value** of these data to an attacker is reduced by a number of elements: i) the value of data held on paper are less attractive to potential buyers than digitalised data and any effort taken to digitalise the data adds to the resource required by an attacker; ii) the data are not particularly attractive in comparison with many sets of personal data easily accessible online (which include, for example, bank details or key account passwords) – this is particularly true in Member States that do not require personal identification (document) numbers; and iii) in many

instances, the paper data are stored separately across different Member States, thereby reducing the total sets of data available in each location.

- **External threat:** An external attacker faces the same challenges with regard to the **value** of the personal data collected. In addition, an external attacker faces additional barriers related to **opportunity** and **resources**. For instance, an external attacker would need to spend time to find an opportunity (i.e. a vulnerability to exploit) and would need to have the required technical expertise to exploit such a vulnerability.

There are, however, two notable exceptions from this trend:

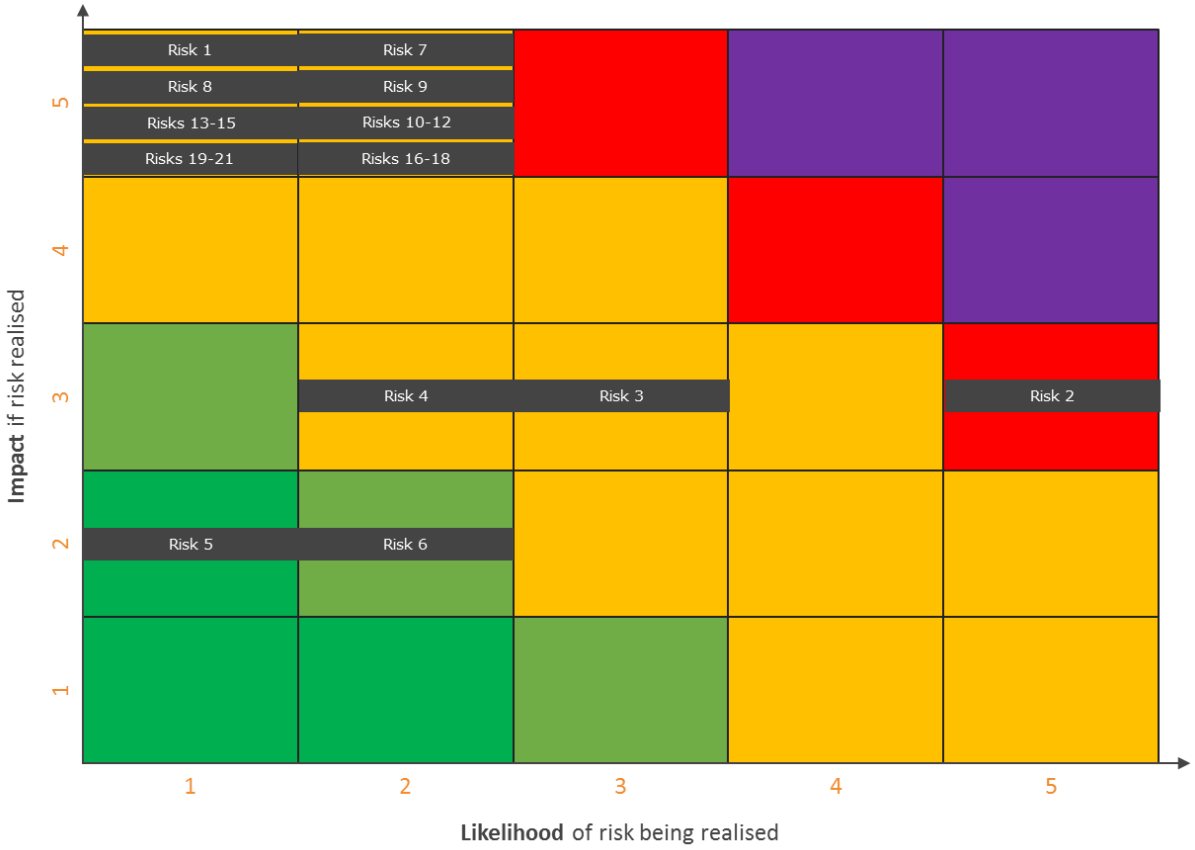
- **Risk 2 – the risk that the ECI requires too many data from signatories** is considered to have a *high likelihood* of being realised. This is due to the findings of this study, which highlight the perceptions of stakeholders that this risk is already being realised. Furthermore, as presented in the preceding analysis of Member State data collection and data verification requirements, it is considered that excessive data collection practices are currently being undertaken in select Member States.
- **Risk 3 – the risk that the ECI requires data that is considered too sensitive** is considered to have a *medium likelihood* of being realised. Although EU-level stakeholders and ECI organisers are concerned with the sensitivity of the data requirements in many Member States, and believe they hinder participation, data collected in the Member States suggests that, in most cases, the data collected and verified is not of a significantly sensitive nature.

Both risk 2 and risk 3 reflect key stakeholder concerns and are key premises on which this study has been commissioned.

With regard to the impact, it is considered that the **majority of the identified risks will have a high impact if realised**: 16 risks are considered to have a high impact if realised (R1, R7-21); however, 15 of these risks concern the data security risks related to the theft / loss / modification / destruction of personal data which all carry the same level of impact. These high impact ratings are predominantly due to the significant data protection breaches (affecting the personal data of EU citizens) likely to occur through the realisation of these risks. Beyond these high impact risks, three risks are considered to have a medium impact (R2, R3 and R4) and two risks are considered to have a low impact (R5 and R6).

The above analysis and mapping of the ECI risks by likelihood of occurrence and impact allows the prioritisation of the risks for treatment. Figure 3, below, visualises this prioritisation on the likelihood-impact matrix and Table 15 defines the priority scheme.

**Figure 3: Visualisation of ECI risk profile: Prioritisation guide.**




| Risk | Priority level |
|---|---|
| **Very high priority** | |
| **High priority** | |
| **Medium priority** | |
| **Low priority** | |
| **Very low priority** | |

As can be seen, the identified and assessed risks have the following priority levels.

**Table 15: Prioritisation levels of identified risks.**

| Risk | Priority level |
|---|---|
| **R1: Formulation of a fake ECI in order to collect and misuse personal data** | Medium priority |
| **R2: Reduced ECI participation as citizens are required to provide too many data** | High priority |
| **R3: Reduced ECI participation as citizens are required to provide data perceived as too sensitive** | Medium priority |

| Risk | Priority level |
|---|---|
| **R4: Fraudulent activities to increase support for an ECI** | Medium priority |
| **R5: Fraudulent activities to undermine an ECI** | Very low priority |
| **R6: Polarisation of Member State (and citizen) engagement with the ECI** | Low priority |
| **R7: Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when stored** | Medium priority |
| **R8: Modification of citizens' data from ECI statements of support collected *on paper,* when stored** | Medium priority |
| **R9: Destruction of citizens' data from ECI statements of support collected *on paper,* when stored** | Medium priority |
| **R10: Interception / theft / loss of citizens' data from ECI statements of support collected *online*, when stored (third-party hosting)** | Medium priority |
| **R11: Modification of citizens' data from ECI statements of support collected *online*, when stored (third-party hosting)** | Medium priority |
| **R12: Destruction of citizens' data from ECI statements of support collected *online*, when stored (third-party hosting)** | Medium priority |
| **R13: Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software)** | Medium priority |
| **R14: Modification of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software)** | Medium priority |
| **R15: Destruction of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software)** | Medium priority |
| **R16: Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when in transit** | Medium priority |
| **R17: Modification of citizens' data from ECI statements of support collected *on paper,* when in transit** | Medium priority |
| **R18: Destruction of citizens' data from ECI statements of support collected *on paper,* when in transit** | Medium priority |
| **R19: Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when in transit** | Medium priority |
| **R20: Modification of citizens' data from ECI statements of support collected *online,* when in transit** | Medium priority |
| **R21: Destruction of citizens' data from ECI statements of support collected *online,* when in transit** | Medium priority |

### III.4.3. Risk treatment

This section presents, where relevant and appropriate, risk treatment options for each identified risk. As per ISO/IEC 27005:2011 guidance, risk treatment options fall into one of the following four categories:

- A risk may be **transferred** from one stakeholder to another.
- A risk may be **avoided** by restructuring a process or procedure.
- A risk may be **mitigated** to an acceptable level.

- A risk may be **accepted**. If the impacts or likelihood of a risk occurring are sufficiently small, or existing mitigation is considered sufficient, it may be suggested that the risk is simply accepted and no action is necessary.

As can be seen above, three of the eighteen risks identified (R4, R5 and R6) are adjudged to be low priority based on the likelihood of the risk being realised and the impact if the risk is realised. The majority of the risks (14 of 18) identified are categorised as medium priority (R1, R3, R7-12 and R13-18) and one risk (R2) is considered as a high priority risk.

Although risk treatment options have been considered for all risks, the most pertinent to consider are those related to the high and medium priority risks. All the risks and related risk treatment options are presented in Table 14, below.

As can be seen, below, three of the eighteen identified risks are deemed to be at an acceptable level considering the priority assessment and an examination of existing mitigation measures (R1, R4 and R5). In addition, risks 7-18 could also be determined to be acceptable due to their low likelihood of occurrence. However, for these 12 risks, additional mitigation measures are proposed to further improve the acceptability of each risk. These additional measures will be discussed further in section VI, which presents the alternative options of the ECI data requirements. Furthermore, regarding the technical protections currently in place relating to risks 10, 11 and 12 (relating to the storage of online statements of support), this assessment is developed further by the caveat that regular risk analyses should continue to be undertaken for the European Commission's Online Collection Software and hosting environment and any recommendations from those analyses should be implemented.

Thus, key risk treatment options relate to the collection of personal data through statements of support; namely risks 2, 3 and 6. Mitigation of risk 2 requires the minimisation of these data requirements; mitigation of risk 3 requires the alteration of the data to be collected and the removal of more sensitive data; and mitigation of risk 6 requires the harmonisation of data requirements across the EU. As these risks all relate to the collection of personal data, their treatment should be designed coherently; this will be elaborated further in section VI.

**Table 16: Risk treatment options, by assigned priority level.**

| Risk | Priority level | Risk treatment options |
|---|---|---|
| **R2:** Reduced ECI participation as citizens are required to provide too many data | High priority | Further **minimise data requirements** through amendments to Annex III to the ECI Regulation but not the Regulation itself – this option is further elaborated in section VI and is complementary to the proposed mitigation options for R3 and R6. The minimisation of the data requirements targets the ECI vulnerability of the perceived excessive collection of personal data. |
| **R1:** Formulation of a fake ECI in order to collect and misuse personal data | Medium priority | This risk is considered to be a medium priority due to its potentially high impact. However, the **extensive existing mitigation is considered sufficient,** due to the significant formation and registration process for ECIs, and the vulnerability being exploited is a core provision of the ECI Regulation. As such, it is advised that this risk can be accepted. |
| **R3:** Reduced ECI participation as citizens are required to provide data perceived as too sensitive | Medium priority | **Minimise data requirements by requiring less sensitive data** in those Member States where this is considered an issue through amendments to Annex III to the ECI Regulation but not the Regulation itself – this option is further elaborated in section VI and is complementary to the proposed mitigation for R2 and R6. This treatment option targets the ECI vulnerability of the perceived excessive collection of sensitive personal |

| Risk | Priority level | Risk treatment options |
|---|---|---|
| | | data. |
| **R4:** Fraudulent activities to increase support for an ECI | Medium priority | The vulnerability being exploited here is the lack of verification against impersonation. Amendments to the verification process could be proposed – i.e. to include authentication guarding against impersonation. If such amendments are to be proposed, they should be assessed in light of this risk. Such amendments would require changes to the ECI Regulation.<br><br>Section VI further considers options along these lines including the use of authenticated signatures or e-IDs. Furthermore, automated analytics tools could be employed, as is discussed in the UK case study, to better identify suspicious statement of support patterns.<br><br>However, such changes also need to consider the level of verification that is appropriate given the outcomes associated with the ECI. Examples of similar national or regional instruments that have undertaken perceived good practices in this regard are presented through section V. |
| **R7:** Interception / theft / loss of citizens' data from ECI statements of support collected on paper, when stored | Medium priority | **R7-9:** Although the likelihood of risks 7 and 9 being realised is low (and for risk 8, it is very low), the potential impact is high and there are no existing measures in place to mitigate these risks. As such, it is considered that **further exploration could be conducted on the mechanisms in place to securely store and handle paper statements of support** and **best practice guidance could be developed for ECI organisers** along these lines, which would require no changes to the ECI Regulation – mitigation options include scanning or encoding of paper statements of support such that they benefit from the same technical controls as online statements of support. These options are further elaborated in section VI.<br><br>Additionally, the ECI Regulation places greater focus on the security of Online Collection Systems; as such, greater consideration of the storage of paper statements of support through an amendment of the ECI Regulation would also support the mitigation of this risk.<br><br>These mitigation options seek to address the vulnerability that the storage of paper statements of support is currently not subjected to any controls. |
| **R8:** Modification of citizens' data from ECI statements of support collected on paper, when stored | Medium priority | |
| **R9:** Destruction of citizens' data from ECI statements of support collected on paper, when stored | Medium priority | |
| **R10:** Interception / theft / loss of citizens' data from ECI statements of support collected online, when stored (third-party hosting) | Medium priority | **R10-12:** Current mitigation measures are extensive; however, there is currently no mechanism to assure the security of online collection systems hosted by third-parties beyond the point of certification, even though patches will need to be made periodically and the hosting party may wish to upgrade its system. |
| **R11:** Modification of citizens' data from ECI statements of support collected online, when stored | Medium priority | |

| Risk | Priority level | Risk treatment options |
|---|---|---|
| (third-party hosting) | | As such, potential treatment options include: i) the requirement for ECI organisers to undertake regular risk analyses on their hosting environments; or ii) the requirement for all ECI organisers to use the Commission's hosting environment. Further discussion, in particular on the second option, is presented in section VI. |
| **R12:** Destruction of citizens' data from ECI statements of support collected online, when stored (third-party hosting) | Medium priority | |
| **R13:** Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | Medium priority | **R13-15: Current mitigation measures are considered sufficient** so risk should be accepted – in particular, the continued use of strong encryption for data in storage is highly advised, as are the regular risk analyses of the European Commission's online collection software and hosting environment. Although, it should be noted that recommendations from the risk analyses of the Commission's online collection software should be implemented to ensure any vulnerabilities in the hosting environment are tackled appropriately. |
| **R14:** Modification of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | Medium priority | |
| **R15:** Destruction of citizens' data from ECI statements of support collected *online,* when stored (Commission hosting and software) | Medium priority | |
| **R16:** Interception / theft / loss of citizens' data from ECI statements of support collected *on paper,* when in transit | Medium priority | **R16-18:** No mitigation measures are currently explicitly foreseen in the ECI Regulation for R16-18 but organisers are presumed to design and implement appropriate measures in accordance with data protection legislation. As the likelihood of these risks being realised is considered to be low, it could be appropriate to simply accept the risk.<br>Possibly **guidance for ECI organisers could be developed** on the secure transmission of paper statements of support (e.g. it could be recommended that paper statements of support are **scanned** and submitted in electronic form using an encrypted memory card or that organisers use a dedicated **secure transfer mechanism** (see options below for R 19-21).<br>Furthermore, the ECI Regulation presently focuses primarily on the transfer of online statements of support; **additional focus on securing the transfer of paper statements of support** through amendments to the ECI Regulation would also support the mitigation of these risks.<br>These mitigation options are discussed further in section VI. |
| **R17:** Modification of citizens' data from ECI statements of support collected *on paper,* when in transit | Medium priority | |
| **R18:** Destruction of citizens' data from ECI statements of support collected *on paper,* when in transit | Medium priority | |
| **R19:** Interception / theft / loss of citizens' data from ECI statements of support collected *online,* when in transit | Medium priority | **R19-21:** The likelihood of R19-21 being realised is considered to be very low, in particular given the existing mitigation in place. It could therefore be appropriately determined that these risks should simply be accepted.<br>However, the **introduction of secure transfer mechanisms between all parties** would provide |

| Risk | Priority level | Risk treatment options |
|---|---|---|
| **R20:** Modification of citizens' data from ECI statements of support collected *online,* when in transit | Medium priority | further mitigation for these risks.<br><br>Furthermore, in instances where an ECI uses the Commission hosted Online Collection Software, it is currently necessary for the online statements of support to be sent from the Commission to the ECI organiser and then from the ECI organiser to the national authorities for verification. Although the introduction of secure transfer mechanisms is possible between all parties within this current process, additional mitigation could be implemented by **permitting the Commission to send the data directly to the national authorities. This will greatly reduce the attack surface within this transfer process**.<br><br>These changes could be implemented through amendments to the ECI Regulation. |
| **R21:** Destruction of citizens' data from ECI statements of support collected *online,* when in transit | Medium priority | |
| **R6:** Polarisation of Member State (and citizen) engagement with the ECI | Low priority | **Harmonisation of data requirements** across the Member States would adequately mitigate this risk and tackle the vulnerability envisages. Furthermore, this would complement the mitigation options proposed for R2 and R3 – these changes would require amendments to Annex III to the ECI Regulation but not the ECI Regulation itself.<br><br>Such amendments are elaborated further in section VI. |
| **R5:** Fraudulent activities to undermine an ECI | Very Low priority | Given the risk's priority level, it is considered that **current mitigation is sufficient.** |

# IV. Analysis of data sensitivity

*Chapter IV addresses the issue of the **sensitivity of the personal data** that are asked of supporters of European Citizens' Initiatives (ECIs) in the EU Member States. A key premise of this study is that some ECI organisers have experienced reluctance to support an initiative in Member States where a significant amount of personal data is required, particularly an ID number.[46] As such, a key objective of this study is the further exploration of this topic through the collection and assessment of the sensitivity of the data required by the ECI across the EU Member States and an analysis of the relationship between the sensitivity of the data required and participation.*

As explained in more detail below, the issue of "data sensitivity" is relative. Contrary to what the term itself suggests, the issue does not simply relate to the question of whether certain data are, in general or in certain countries, seen as inherently 'sensitive'. Rather, the question of 'sensitivity' is closely linked to issues of data security, as perceived by potential supporters of an ECI. The extent to which they are reluctant to provide certain data, such as ID numbers or ID document details, depends on the **context** in which they are asked for these data, and the **identity of the entity to which they are disclosing the data**.

It is therefore more appropriate to more generally **assess and analyse the concerns of data subjects about the provision of their personal data**, rather than focus on the supposed inherent sensitivity of each data points. As such, this section compares those concerns, as perceived at Member State level, by highlighting pertinent data sensitivity-related issues before listing possible remedial actions, to be developed further in section VI on alternative options for the ECI data requirements.

**Box 4: Methodological note: Defining the term 'data sensitivity'.**

**Methodological note: Defining the term 'data sensitivity'**

It is important to note that this assessment uses the word 'sensitive' in a general sense, related in particular to the question of whether individuals might be wary or reluctant to provide certain information (i.e. whether they might be sensitive to the use of the data or may have concerns about them). The word is not used in the technical formal sense, as relating to the term 'sensitive data' as applied in EU data protection law:

> *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"*
>
> Art. 9(1) GDPR, expanding on Art. 8(1) of the 1995 Data Protection Directive

## IV.1. Comparative analysis

Given the considerable discussions about the sensitivity of the data that individuals have to provide in order to submit a statement of support for an ECI, it is notable that for **most (21)**

[46] Technical Annex to the request for service JUST/SG.C.4/2016/01 – Study on Data Requirements for the European Citizens' Initiative, p.4. Ref. Ares(2016)3232195.

**EU Member States (Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Ireland, Italy, Lithuania, Luxembourg, Latvia, Malta, Poland, Romania, Slovakia, Sweden and the UK) it was reported by the stakeholders consulted (civil society organizations and public authorities) that there were no real concerns** about this issue.

More in line with expectations is the finding that insofar as there have been concerns in Member States about the sensitivity of the ECI data, those have mainly **focused on the requirement to provide national ID or ID document numbers**. Although the perceived sensitivity of such numbers is a (major) reason for not requiring the provision of these data in some countries, others, in which they are required, consider them uncontroversial. Furthermore, in some Member States, the concerns and sensitivities around the submission of data are altogether different. As such, the data sensitivity landscape across the Member States can be characterised as complex. An overview of the perceptions of Member States is provided in Table 17, below.

**Table 17: Overview of Member State perceptions on the sensitivity of the ECI data requirements, according to the stakeholders consulted and desk research.**

| Member State | Perceptions on the sensitivity of the ECI data requirements |
|---|---|
| **Austria** | No sensitivities noted regarding the provision of ECI data; however, concerns noted about legal-technical data sensitivity, in relation to revealing political views / beliefs of signatories. * |
| **Belgium** | No sensitivities noted regarding the provision of ECI data. |
| **Bulgaria** | Personal identification numbers are considered to be sensitive, in particular as these data have been misused in the past but not by ECIs. * |
| **Croatia** | No sensitivities noted regarding the provision of ECI data. |
| **Cyprus** | No sensitivities noted regarding the provision of ECI data. * |
| **Czech Republic** | No sensitivities noted regarding the provision of ECI data; however, it is noted that comparatively, personal identification numbers are considered to be more sensitive than the other data required by ECIs. |
| **Denmark** | No sensitivities noted regarding the provision of ECI data; however, it is noted that personal identification number would be considered particularly sensitive, if used. |
| **Estonia** | No sensitivities noted regarding the provision of ECI data. * |
| **Finland** | No sensitivities noted regarding the provision of ECI data. |
| **France** | Personal identification numbers are considered to be relatively sensitive in comparison with the other data required by ECIs. |
| **Germany** | No sensitivities noted regarding the provision of ECI data; however, concerns noted about legal-technical data sensitivity, in relation to revealing political views / beliefs of signatories. The list of data that is considered sensitive is largely dependent on the context of how and why this data was processed.* |
| **Greece** | No sensitivities noted regarding the provision of ECI data; however, concerns noted about legal-technical data sensitivity. |
| **Hungary** | Personal identification numbers are considered to be relatively sensitive in comparison with the other data required by ECIs. Similarly, Address was reported as sensitive depending on how and why it was processed. |
| **Ireland** | Sensitivity reported in relation to how an individual's date of birth is processed as well as regarding an extensive combination of the data required by ECI's as the risk of identity fraud with a requirement of all |

| Member State | Perceptions on the sensitivity of the ECI data requirements |
|---|---|
| | potential personal data points, was considered high.* |
| **Italy** | No sensitivities noted regarding the provision of ECI data; however, concerns noted about legal-technical data sensitivity, in relation to revealing political views / beliefs of signatories. |
| **Latvia** | Personal identification numbers are considered to be relatively sensitive in comparison with the other data required by ECIs*. Similarly, Address was reported as sensitive if it was used for verification. * |
| **Lithuania** | No sensitivities noted regarding the provision of ECI data. |
| **Luxembourg** | No sensitivities noted regarding the provision of ECI data. |
| **Malta** | No sensitivities noted regarding the provision of ECI data. |
| **Netherlands** | Some data is considered to be sensitive, particularly personal identification numbers but this is not currently required for participating in an ECI in NL. Name, Nationality, Fathers name, Name at birth and Place of birth are qualified as "special categories of personal data" because they can give information about a person's race. However, whether these are considered sensitive is largely dependent on the context of how and why this data was processed. * |
| **Poland** | No sensitivities noted regarding the provision of ECI data; however, concerns noted about legal-technical data sensitivity, in relation to revealing political views / beliefs of signatories. |
| **Portugal** | Personal ID number and address are considered to be relatively sensitive in comparison with the other data required by ECIs (name, nationality, date and place of birth).<br>E-mail is also considered to be slightly more sensitive than these other data (not required for ECI). |
| **Romania** | Personal identification numbers are considered to be relatively sensitive in comparison with the other data required by ECIs.* |
| **Slovakia** | No sensitivities noted regarding the provision of ECI data; however, it is noted that personal identification number would be considered particularly sensitive, if used. |
| **Slovenia** | Nationality and personal ID number are considered to be particularly sensitive in comparison with the other data required by ECIs. |
| **Spain** | According to a recent Spanish government barometer[47], published in February 2017, the majority of Spanish citizens (55%) are unwilling to provide their personal identification or passport number, indicating a high level of sensitivity. However, other data required by ECIs (namely, name and nationality) were considered to be much less sensitive. |
| **Sweden** | Personal identification numbers are considered to be relatively sensitive in comparison with the other data required by ECIs and have a special protection in the Swedish Personal Data Act as compared to other categories of data required by ECIs.* |
| **United Kingdom** | No sensitivities noted regarding the provision of ECI data; however, concerns noted about legal-technical data sensitivity, in relation to revealing political views / beliefs of signatories. * |

* Confirmed by National Data Protection Authority

[47] Centro de Investigaciones Sociológicas, (2017) Barómetro de Febrero 2017, Avance de resultados, Estudio no. 3168, Febrero 2017.

### Concerning national ID or ID document numbers

Eight of the above 14 Member States, in which there were reported to be no serious concerns about the ECI data, require the provision of national ID or ID document numbers (Austria, Croatia, Cyprus, Greece, Italy, Lithuania, Malta and Poland. The main reasons for not finding the demand for those numbers controversial or excessive in these countries are:

Croatia, Cyprus, Italy, Malta, Poland and Slovenia

i) that people are generally not very aware of digital / security issues or data protection issues (**Croatia**, in spite of the fact that there have actually been data abuses and losses in national petitions, detailed below);

ii) that although ID data is sensitive, asking for them shows that an ECI is a 'serious' matter (**Greece**);

iii) that the numbers are also asked for in national petitions (**Lithuania**);

iv) that people trust the government and government IT systems and data handling (**Latvia**).

However, in other Member States, national ID or ID document numbers are regarded as intrinsically sensitive. As established earlier, and following input from stakeholders and desk research, a negative correlation exists between the data requirement for signing an ECI and its level of participation. Whilst this correlation is difficult to quantify, we can conclude that including ID numbers, a sensitive personal data point that participants would be more reluctant to provide as compared to less sensitive data, in an ECI's data requirements, will effect participation. This includes both countries in which such data is currently being asked for and countries in which such data is not (or no longer) required but where the inclusion of such data has been considered or discussed. This correlation was supported by the fact that over 49% of the respondents to the Secretariat General's public consultation on the ECI across the EU, stated that they would be unwilling to provide their personal identification number when giving their support to an ECI, only behind driving license number at over 58%.

As above, the reasons vary but in many cases relate to the question of (lack of) trust – be that in state authorities generally, in (unknown) organisers, or in the security of the relevant paper or online collection systems.

At present, the reality is that no abuses (or losses) of data have been reported in relation to ECIs, although examples exist in relation to similar national or regional participatory instruments, as highlighted in Box 5. These national level experiences may explain the lack of trust reported in some Member States.

**Box 5: Data abuses and losses in national or regional participatory instruments.**

### Similar national or regional participatory instruments: Data abuses and losses

Abuses and losses of data have been reported in relation to national participatory instruments in several Member States but, as noted above, not in relation to ECIs. The information on these national data abuses and breaches is sparse, but in outline they are as follows:

**Bulgaria:** there have been cases where data provided for petition signatures have been used for additional purposes such as the registration of signatories in political parties or the initiation of referendums.

**Croatia:** in a number of national popular initiatives, there have been cases of statements of support (which could only be collected on paper) having been used for a different initiative than the one they were originally collected for.

**Slovenia:** there have been data breach incidents in relation to regional popular initiatives, including the public disclosure of the identity of signatories and the loss of around 100 statements of support.

By contrast, in **Germany**, where ID numbers are not required but where the ECI data are still generally regarded as sensitive, the strictness and strong enforcement of data protection law makes individuals less concerned about the providing of ECI data, and they would not object to the use of the new, secure e-ID as a means of participation. The same is true in **Estonia**, where the personal ID number is not asked for.

As noted above, the question of trust reaches beyond the state to the ECI organisers that collect the data – this is of particular relevance to the collection of paper statements of support. For instance, in **Bulgaria**, where ID numbers are required, people are wary of providing extensive data, and their ID numbers in particular, to "strangers in the street" (i.e. ECI organisers collecting paper statements of support). In that regard, in **Greece**, where ID numbers are also asked for, it was suggested that people collecting statements of support for an ECI should carry some form of official certification of their *bona fides*. In **Portugal**, too, it was reported that people were worried that if they provided the required data, they could be the victim of spamming or other invasions of privacy.

In several Member States, discussions were held on the inclusion of personal ID (document) numbers as a data requirement. In **Finland**, the use of personal ID numbers was specifically rejected in the course of the legislative process for the reasons that its use is legally restricted and that it is considered by many citizens to be sensitive personal data, and that consequently, citizens might be hesitant to disclose their personal ID for the purposes of and in the process of supporting an initiative. Notably, the national level equivalent to the ECI in Finland – the *Kansalaisaloite* – has also rejected the use of personal ID numbers as a data requirement for signatories. In **Luxembourg**, too, there was extensive discussion of the need for ID numbers, and although the government initially wanted to retain the requirement, the submission of ID numbers is now no longer required. In Luxembourg, it was specifically noted that collections of ECI data including national ID or ID document numbers would be particularly attractive to attackers, and any security breach would accordingly be much more serious. This was also acknowledged in the **Netherlands**. These kinds of concerns are also likely to explain the more generally expressed views that asking for ID numbers would likely reduce participation noted in **Denmark** (without further indication of why this would be so).

The same view was taken in **Hungary**, but there it was also noted that most people do not carry their ID documents with them and cannot, when asked at a stall or in a charity shop, recall the numbers of those documents, or their national ID number; and that requiring such details would consequently reduce participation.

### Concerning other data

In some Member States, there are special issues in relation to data other than ID or ID documents numbers.

In **Hungary**, for instance, individuals' home addresses are regarded as sensitive and invasive by many people, who consequently refuse to provide them. Also in **Hungary**, and **Slovenia**, for historical reasons, nationality is seen as a particularly sensitive datum.

There was a special issue in this regard in **Italy**, where organisers of the Right2Water ECI complained about individuals not being allowed to use their driving licenses for identification, as had been allowed for many other transactions previously; they claimed that this reduced the numbers of valid statements of support for that ECI by around 30%. However, this must be moderated by the results from the Secretariat General's recent public consultation on the ECI, where 42% of respondents in Italy placed their Driving license number, the highest of any type of personal data that they would not be willing to provide when giving their support to an ECI. 32% of Italian respondents were similarly unwilling to provide their personal identification number as well. However more of them are unwilling to provide their address (37%).

Another unique case is that of Slovakia, where the name at birth is the third most common type of data respondents were unwilling to provide, with 30% of respondents rejecting its use. Similarly, place of birth was the second and third most common type of data respondents were unwilling to provide in Slovenia and Sweden respectively.

Respondents from 13 Member States placed Address in the top three types of personal data they would be unwilling to provide to participate in an ECI. Additionally, within 7 countries

(Bulgaria, Croatia, Estonia, Latvia, Poland, Spain and Portugal), Address was the most common type of data respondents were unwilling to provide and in 2 additional countries (Italy, Cyprus), Address was the second most common after the driving license number.

In conclusion, the main concerns about the data required for the submission of statements of support for an ECI appear to relate more to **trust in the entity collecting the data**, than to the nature of the data. This is true even with regard to ID and ID document numbers.

In some countries, citizens trust the state and state authorities, the IT systems maintained by the state and the handling of personal data by the state. In those countries, they are therefore willing to provide even quite sensitive data for an ECI, including ID data – although it also tends to be a feature of such 'trusted' states that they have strong constitutional and statutory data protection safeguards, and are keen to minimise data requirements, also for ECIs. In any case, citizens of such states trust that the strict data protection rules and high civil servant ethos will ensure that the data are not abused.

In contrast, individuals are often wary to provide extensive data – and especially ID data – to "strangers in the street" (e.g. at an ECI-supporting stall or in a charity shop), whereas they would be less worried if the ECI was organised (or backed) by a well-known national or international NGO. Again, the extent to which such individuals are aware of the national and EU data protection rules and restrictions, in general, and in relation to ECIs, in particular, plays a role here, as does the level of trust they have in such rules being adhered to (by organisers of ECIs or state authorities involved in ECIs).

# V. Comparative analysis

*Chapter V provides an overview of national and regional participatory instruments that are similar to the ECI, analysing the outcomes and verification mechanisms of such instruments. The section then presents a comparative analysis of the data required by ECI statements of support and the data required to support these similar instruments identified at national or regional level in each Member State. It concludes with a summary of the positive and negative aspects identified through the data collected in the country fiches and the country case studies.*

## V.1. Typology of similar national or regional instruments

This section first presents a full typology of different national or regional participatory instruments, as developed by the civil society organisation *Direct Democracy*. Secondly, focusing on the specific types of instrument that resemble or reflect elements of the ECI, this section presents an analysis of national or regional participatory instruments identified across the EU. This analysis focuses on identifying trends in the practices employed by the identified national or regional participatory instruments, with particular focus on the outcomes of the instruments and the methods used for the verification of statements of support. Comparisons are drawn with the ECI where relevant. Subsequently, an examination of e-petition schemes, which are not included in the full typology established by *Direct Democracy* but exhibit similarities to the ECI, is presented.

Section V.3 then presents a dedicated comparative analysis of the data collection and data verification requirements for the ECI and the examined national or regional participatory instruments.

### V.1.1. Full typology of national or regional participatory instruments

The civil society organisation *Direct Democracy* is conducting an ongoing analysis of direct democracy schemes (including participatory instruments) across the EU, and globally. This analysis separates these instruments into 10 categories. Box 6, below, presents the definitions for these categories and lists the numbers of related "legal designs" that reflect each category world-wide.[48]

**Box 6: Types of direct democracy schemes in existence globally, as compiled by the civil society organisation *Direct Democracy.***

**Types of direct democracy scheme**

**1. [Simple] Popular or Citizens Initiative** (PCI) defined as:

A popular vote procedure and a political right that allows a given number of citizens to put their own proposal on the political agenda. The procedure is initiated by a prescribed number of

[48] http://www.direct-democracy-navigator.org/democratic_instruments.
Definitions have been slightly amended for the purpose of the present study, but without changing their substance or scope. The front page of this website shows a world map with links to countries with such schemes, through which detailed information on all the schemes can be found, country by country: http://www.direct-democracy-navigator.org/

eligible voters. The sponsors of a popular initiative can force a popular vote on their proposal (assuming that their initiative is formally adopted). The initiative procedure may include a withdrawal clause, which gives the sponsors the possibility to withdraw their initiative, for example in the event that the legislature has taken action to fulfil the demands of the initiative.

*(142 legal designs world-wide)*

**2. Popular or Citizens initiative including an Authorities Counter-Proposal** (PCI+), defined as:

A Popular or Citizens Initiative process within the framework of which a representative authority (normally parliament) has the right to formulate a counter-proposal to the initiative proposal. Both proposals are then decided on at the same time by a popular vote. If both proposals are accepted, the decision on whether the initiative proposal or the authority's counter-proposal should be implemented can be made by means of a special deciding question.

*(55 legal designs world-wide)*

**3. Agenda-Setting Initiative** (PAX), defined as:

A process allowing a specified number of eligible voters to propose to a competent authority the adoption of a law or measure; the addressee of this proposal and request is not the whole electorate but a representative authority. In contrast to the Popular or Citizens Initiative, it is this public authority which decides the future progress of the initiative, not the citizenry.

An Agenda-Setting Initiative can be institutionalized in a variety of ways: for example, as an Agenda-Setting Initiative without popular vote; as an Agenda-Setting Initiative combined with the possibility of a consultative or binding plebiscite; or as a Popular Motion ("*Volksmotion*"). The Popular Motion can be regarded in law as the equivalent of a Parliamentary Motion (a motion by a Member of Parliament); if adopted, it can also be treated like a Popular or Citizens Initiative (the latter is the case in the canton of Obwalden, Switzerland).

It is important to note that *Direct Democracy* classifies the ECI as belonging to this category, presumably within the sub-category of an Agenda-Setting Initiative without popular vote.

*(244 legal designs world-wide)*

**4. Authorities Minority Veto-Plebiscite** (MVP), defined as:

A popular vote procedure characterized by the right of a minority of a representative authority (typically, a national or regional parliament or council) to put a decision made by the majority in the same authority before the voters for approval or rejection. This procedure enables a minority of a representative authority to step on the brakes and give the final say to the voters.

(7 legal designs world-wide)

**5. Authorities' Minority Plebiscite** (MTP), defined as:

A popular vote procedure and a political right that allows a specified minority of an authority (e.g. one third of the parliament) to put its own proposal on the political agenda and let the people decide on it by a popular vote.

(26 legal designs world-wide)

**6. Plebiscite** (ATP), defined as:

A popular vote procedure whose use lies exclusively within the control of an authority. In this form the author of the ballot proposal and the initiator of the procedure are the same (for example, parliament or president).

(339 legal designs world-wide)

**7. Veto-Plebiscite** (AVP), defined as:

Another popular vote procedure whose use lies exclusively within the control of the authorities. In this form the author of the ballot proposal and the initiator of the procedure are *not* the same. For example, a government or a president may oppose (veto) a decision of parliament

and refer it to a popular vote; hence the name veto plebiscite.

(52 legal designs world-wide)

**8. Obligatory Referendum** (LOR), defined as:

A popular vote procedure that is triggered automatically by law (usually the constitution) which requires that certain issues must be put before the voters for approval or rejection. A conditional obligatory referendum means that a specified issue must be put to the ballot only under certain conditions. Unconditional referenda are referenda that must be held without specifying any such conditions.

(510 legal designs world-wide)

**9. Popular or Citizen-Initiated Referendum** (PCR), defined as:

A popular vote procedure and a political right that allows a specified number of citizens to initiate a referendum and let the whole electorate decide whether, for example, a particular law should be enacted or repealed.

This procedure acts as a corrective to parliamentary decision-making in representative democracies and as a check on parliament and the government.

(159 legal designs world-wide)

**10. Popular Referendum including an Authorities' Counter-Proposal** (PCR+), defined as:

A popular vote procedure that combines a popular referendum against a decision by an authority with a referendum on a counter-proposal. If both proposals are accepted, the decision between the two can be made by means of a deciding question.

(7 legal designs world-wide)

### V.1.2. Typology of identified national or regional participatory instruments

This section focuses on the categories of instruments that most strongly reflect the ECI. Most prominently, this relates to the **Agenda-Setting Initiatives (PAX)**, which, as noted above, is the category in which the ECI rests. Specifically, national and regional schemes related to the first variant of this category will be examined: **Agenda-Setting Initiatives without popular vote**. In addition, certain **Simple Popular or Citizens' Initiatives (PCI)** will be examined as, although the outcomes related to such initiatives differ significantly from the ECI, similarities exist in the related processes. This section first analyses the existence of these identified instruments across the EU Member States before examining the outcomes and verification methods associated with these national or regional instruments. Comparisons are drawn with the ECI where relevant.

With this scope in mind, **56 national or regional participatory instruments** have been identified across the EU Member States. Table 18, below, illustrates the number and type of such instruments across the Member States, as well as the level at which the instruments operate (i.e. national or regional).

**Table 18: Number and type of PCI and PAX schemes in the EU Member States.**

| Member State | PAX | | PCI | |
|---|---|---|---|---|
| | National | Regional | National | Regional |
| **Austria** | 1 | | | |
| **Belgium** | 1 | 3 | | |
| **Bulgaria** | 1 | 1 | 1 | |
| **Croatia** | | | 1 | |

| Member State | PAX | | PCI | |
|---|---|---|---|---|
| | National | Regional | National | Regional |
| **Cyprus** | | | | |
| **Czech Republic** | 1 | | 1 | 1 |
| **Denmark** | | | | |
| **Estonia** | 1 | | | |
| **Finland** | 1 | | | |
| **France** | | | | |
| **Germany** | | 10 | | |
| **Greece** | | | | |
| **Hungary** | | | | |
| **Ireland** | 1 | | | |
| **Italy** | 1 | | | |
| **Latvia** | | | | |
| **Lithuania** | 2 | | | |
| **Luxembourg** | 1 | | | |
| **Malta** | | | | |
| **Netherlands** | 1 | | | |
| **Poland** | 1 | | | |
| **Portugal** | 1 | | | |
| **Romania** | 1 | | | |
| **Slovakia** | 1 | | | |
| **Slovenia** | 1 | 1 | | |
| **Spain** | 1 | 17 | | |
| **Sweden** | | | | 2 |
| **United Kingdom** | | | | |
| **Total** | 18 | 32 | 3 | 3 |

As mentioned above, the majority of these national or regional instruments fall into the category of **Agenda-Setting Initiatives** (PAX) – i.e. they work to propose a legislative initiative or measure to a public authority, which decides the outcome of such a proposal. In fact, **50 (89%)** of the instruments identified fall into this category, spanning 18 Member States. 18 are implemented at the national level compared to 32 at the regional level. However, it should be noted that the latter number is largely bolstered by the implementation of regional instruments across many German Länder and Spanish provinces – these examples comprise 27 of the 32 regional PAX schemes identified.

In addition, **six (11%)** instruments reflecting the **Simple Public or Citizens' Initiative** (PCI) category were identified, spanning four Member States (BG, CZ, HR, SE); three at the national level and three at the regional level.

Overall, 21 (38%) of the 56 schemes identified are implemented at **national level**, with the majority implemented at **regional level (35, 63%)**. However, as previously mentioned, this latter figure is inflated by the implementation of regional initiatives across Germany and Spain. Table 19 presents a full list of the 56 schemes examined:

**Table 19: List of PAX and PCI national / regional participatory instruments identified and examined.**

| MS | Type | Level | Name |
|---|---|---|---|
| AT | PAX | National | Volksbegehren |
| BE | PAX | National | National petition right |
| BE | PAX | Regional | Regional (Brussels) petition right |
| BE | PAX | Regional | Regional (Flanders) petition right |
| BE | PAX | Regional | Regional (Wallonia) petition right |
| BG | PCI | National | (Petition) for a) Referendum |
| BG | PAX | National | Citizens' Initiative |
| BG | PAX | Regional | Citizens' Initiative |
| CZ | PCI | Regional | Referendum |
| CZ | PCI | National | Referendum |
| CZ | PAX | National | Petition |
| DE | PAX | Regional | Volksantrag (Petition for a legislative proposal) Baden-Württemberg |
| DE | PAX | Regional | Volksinitiative (Petition for a legislative proposal) Berlin |
| DE | PAX | Regional | Bürgerantrag (Petition for a legislative proposal) Bremen |
| DE | PAX | Regional | Volkspetition (Petition for a legislative proposal) Hamburg |
| DE | PAX | Regional | Volksinitiative (Petition for a legislative proposal) Lower-Saxony |
| DE | PAX | Regional | Volksinitiative (Petition for a legislative proposal) Mecklenburg-Vorpommern |
| DE | PAX | Regional | Volksinitiative (Petition for a legislative proposal) North-Rhine Westphalia |
| DE | PAX | Regional | Volksinitiative (Petition for a legislative proposal) Rhineland-Palatinate |
| DE | PAX | Regional | Volksinitiative (Petition for a legislative proposal) Saxony-Anhalt |
| DE | PAX | Regional | Bürgerantrag (Petition for a legislative proposal) Thuringia |
| EE | PAX | National | Rahvaalgatus (Collective Address) |
| ES | PAX | National | Iniciativa Legislativa Popular (Popular Legislative Initiative) |
| ES | PAX | Regional | Popular legislative initiative (region of Andalusia) |
| ES | PAX | Regional | Popular legislative initiative (region of Aragon) |
| ES | PAX | Regional | Popular legislative initiative (region of Asturias) |
| ES | PAX | Regional | Popular legislative initiative (region of Balearic Islands) |
| ES | PAX | Regional | Popular legislative initiative (region of Basque Country) |
| ES | PAX | Regional | Popular legislative initiative (region of Canary Islands) |
| ES | PAX | Regional | Popular legislative initiative (region of Cantabria) |
| ES | PAX | Regional | Popular legislative initiative (region of Castilla and Leon) |
| ES | PAX | Regional | Popular legislative initiative (region of Castilla-La Mancha) |
| ES | PAX | Regional | Popular legislative initiative (region of Cataluña) |
| ES | PAX | Regional | Popular legislative initiative (region of Extremadura) |
| ES | PAX | Regional | Popular legislative initiative (region of Galicia) |
| ES | PAX | Regional | Popular legislative initiative (region of La Rioja) |
| ES | PAX | Regional | Popular legislative initiative (region of Madrid) |
| ES | PAX | Regional | Popular legislative initiative (region of Murcia) |
| ES | PAX | Regional | Popular legislative initiative (region of Navarre) |
| ES | PAX | Regional | Popular legislative initiative (region of Valencia) |
| FI | PAX | National | Kansalaisaloite (citizens' initiative) |
| HR | PCI | National | Scheme to call a referendum |
| IE | PAX | National | Joint Committee on Public Petitions |
| IT | PAX | National | Citizens' Initiative |
| LT | PAX | National | Right of referendum |
| LT | PAX | National | Right of legislative initiative |
| LU | PAX | National | Public Petitions |
| NL | PAX | National | Burgerinitiatief (popular petition) |
| PL | PAX | National | Inicjatywa ustawodawcza (citizens' initiative) |
| PT | PAX | National | Iniciativa Legislativa de Cidadãos (Citizens' Legislative Initiative) |
| RO | PAX | National | Citizens' Legislative Initiative |

| MS | Type | Level | Name |
|---|---|---|---|
| SE | PCI | Regional | Folkinitiativ (Regional) |
| SE | PCI | Regional | Folkinitiativ (Municipal) |
| SI | PAX | National | Popular initiative |
| SI | PAX | Regional | Popular initiative |
| SK | PAX | National | Petition Right |

### Outcomes of national / regional participatory instruments

As indicated by the definitions detailed above, the **outcomes** related to the different types of national or regional schemes are as follows:

- **Agenda-Setting Initiatives (PAX):** representing the majority of schemes identified and the category in which the ECI sits, PAX schemes primarily result in the delivery of a proposed new law; amendment to, or abolishment of, existing laws; or measure on which the initiative is based to a relevant public authority. In most cases, this public authority is the national or regional parliament but can also be a specific parliamentary committee or specific government department. Most of the initiatives identified vary slightly from this blueprint. For instance, the **Finnish** citizens' initiative (*Kansalaisaloite*) results in the submission of an initiative to the Parliament – such an initiative can be either a proposal for a legislative act, a proposal to start drafting a legislative act, or a proposal to amend or repeal an existing act. In **Bulgaria**, however, it is also possible to submit the content of a citizens' initiative to bodies of the central executive branch, as well as the National Assembly. To demonstrate further variation, in **Ireland**, the Public Petitions scheme simply places a topic on the agenda of parliament with no requirement for legislative content.
- **Simple Public or Citizens' Initiative (PCI):** representing a small minority of the schemes identified, these types of scheme differ from the ECI specifically on this point; the progress of a successful initiative is decided by the citizenry, not a public authority. As such, a successful PCI leads to a public vote, often in the form of a referendum. However, slight variations occur in the practical implementation of PCI schemes. For example, in **Croatia**, the collection of sufficient signatures immediately results in the calling of a referendum by the Croatian Parliament. In **Sweden**, however, both the regional and municipal *Folkinitiativ* require an intermediate step before a referendum is called. The relevant regional / municipal councils are required to vote on whether a referendum should be called; a qualified majority is required to prevent such a referendum.

### Verification of statement of support data for national / regional participatory instruments

This section details the purposes and mechanisms in place for verifying statement of support data in the examined national and regional participatory instruments. However, it should be noted that data on all the elements related to verification is not comprehensively and comparably available across all the participatory instruments examined. As such, the number of national or regional schemes included in each element of the analysis will be highlighted to ensure transparency of the datasets being used. Throughout the analysis, appropriate comparisons are drawn with the verification mechanisms used by Member States for the ECI, as detailed in section III.2.

A key difference identified across the examined national and regional participatory instruments relates to the eligibility criteria for signatories and, tied to this, the **use of electoral rolls / voter's registers and / or population registers as the basis for verifying the data submitted by signatories**. Of the 47 national and regional instruments for which relevant data is available, the majority (32, 68%) base verification *solely* on the right of a signatory to vote in the country / region; as such, for these initiatives, verification is conducted against the relevant electoral roll or voter's register. Examples of these initiatives are presented in Box 7.

**Box 7: National or regional participatory instruments: verification based on eligibility to vote.**

**National and regional participatory instruments with verification based on voting eligibility: e.g.**

**Croatia:** The PCI scheme to call a referendum, as stipulated in Article 87 of the Croatian Constitution, requires that, upon the collection of statements of support from at least 10% of the total electorate, the Croatian Parliament calls a referendum on the issue of the initiative. Signatories to such a initiative must be Croatian citizens and must submit their name and personal identification number. These data are verified against the register of voters by the Croatian Ministry of Public Administration.

**Germany:** In seven German Länder, a key criterion to support a petition for a legislative proposal is the eligibility to vote in the elections of the Länder. This is true for the Volksantrag in Baden-Wurttemberg; the Volksinitiative in Lower-Saxony, Mecklenburg-Vorpommern, North-Rhine Westphalia, Rhineland-Palatinate, Saxony-Anhalt; and the Bürgerantrag in Thüringen. In Mecklenburg-Vorpommern's *Volksinitiative*, for instance, signatories must be entitled to vote in Länder's elections – i.e. they must be at least 18 years of age, of German nationality and resident in the Länder. These details are verified by the Mecklenburg-Vorpommern Election Commissioner, in collaboration with the municipalities.

**Romania:** The Citizens' Legislative Initiative, a national level PAX scheme, is enshrined in Article 74 of the Romanian Constitution. It determines that, with the support of at least 100,000 citizens entitled to vote, the Romanian citizenry may propose a legislative initiative to the Chamber of Deputies (i.e. parliament). Interestingly, in a similar fashion to the ECI, the statements of support must span one quarter of Romania's counties and each of those counties must contribute at least 5,000 statements of support. Furthermore, the verification mechanisms are considered by local civil society organisations to be inefficient – verification is initially conducted by the local mayor or local administration before further checks are conducted by the Constitutional Court.

Of the remaining instruments examined, 10 (21%) use population registers for the verification of the submitted data; three use a combination of eligibility of signatories as a voter and presence on a population register; and two initiatives conduct no, or very limited, verification. Regarding the latter two initiatives, these are presented in Box 8, with other examples of initiatives that implement an inconsistent approach to verification.

**Box 8: National or regional participatory instruments with limited verification of statements of support.**

**National and regional participatory instruments with limited verification**

**Ireland:** The national level, agenda-setting Public Petitions instrument requests that signatories submit their name, address, e-mail, mobile and home phone numbers and select their preferred method of contact. However, no verification is employed to ensure the data provided by signatories is accurate or relates to an Irish citizen or even a natural person. As mentioned above, however, Ireland's Public Petitions instrument has limited impact, as it only provides for citizens to place topics on the Irish Parliament's agenda; which may explain the lack of focus on verification of signatories.

**Slovakia:** The Petition Right, as stipulated in Article 95 of the Slovakian Constitution, provides for citizens to submit a petition to a relevant public authority, which is obliged to provide a response following its enquiries into the subject of the petition. However, the veracity of data submitted by supporters of a petition is not verified. Instead, petitions are checked for the presence of the required data (i.e. name, address, signature) and duplicate signatures.

Furthermore, the **Swedish** municipal and regional *Folkinitiativs*, that are recorded in the above

as relying solely on the eligibility of a signatory as a registered voter, as well as the four **Belgian** instruments, which are recorded above as initiatives that utilise the Belgian population register, do not apply a consistent or documented verification processes.

Instead, these six initiatives verify statements of support through ad-hoc processes developed by the appropriate authority for each specific initiative and, in some cases, do not conduct any verification.

The above analysis paints a different picture to the use of databases by Member States for the verification of ECI statements of support, as detailed in section III.2. For the ECI, the majority of Member States rely on population registers, with only five Member States utilising electoral or voter registers (EL, HR, HU, IE and SI), some of them in addition to the population registers. **For national or regional instruments, however, there is a much greater reliance on voter registration with regard to both eligibility criteria and verification mechanisms**. Furthermore, the above examples demonstrate the variance in verification practices that exist between the national and regional instruments examined – some employ practices similar to the ECI, while others exhibit significant variations.

Another key difference identified between the ECI and the national and regional participatory instruments examined relates to the use of paper versus online formats for the collection of statements of support. As is clearly detailed through section III, the ECI requires that individuals may provide support to an ECI through a paper or online statement of support. **In contrast, the majority of national and regional level initiatives with available data (34, 63%, N=54) only permit paper statements of support.** Of the remaining initiatives, all 20 (37%) provide for the submission of both paper and online statements of support. No initiatives identified provide solely for the submission of online statements of support.

Further increasing the contrast with the ECI, **22 (42%, N=52) of the examined national or regional participatory instruments require in-person authentication of signatories for paper statements of support**. However, it should be noted that the majority of these examples relate to the 17 provincial and one national initiatives implemented in Spain. Examples of in-person authentication processes are detailed in Box 9.

**Box 9: National or regional participatory instruments: In-person authentication.**

**National and regional participatory instruments with in-person authentication**

Authentication of signatories is conducted to ensure the individual submitting a statement of support is the same individual whose personal data is being provided, and thus to prevent fraud or impersonation. As detailed in section III.2, authentication of signatories is not a verification condition stipulated by the ECI Regulation. However, with regard to national or regional level participatory instruments, 22 were identified that require in-person authentication of signatories: e.g.

**Spain:** For the one national and 17 provincial participatory instruments examined, all require in-person authentication of paper statements of support.

For example, in the province of **Andalusia**, the details of the *Iniciativa Legislativa Popular* are stipulated in Organic Law 2/2007, of 19 March, on the reform of the Statute of Autonomy for Andalusia and the Law of the Popular Legislative Initiative (*Iniciativa Legislativa Popular*) and of the Town Halls, 5/1988, 2011. Organic Law 2/2007 states the right of the Andalusian people to undertake such popular legislative initiatives, with the process of the scheme established in law 5/1988, 2011. This law states that statements of support are required from at least 40,000 individuals that are enrolled in the existing Andalusian electoral rolls and are at least 18 years old. These statements of support are required to be authenticated by a notary, court clerk or the Secretary of the Town Hall in whose electoral roll the signer is registered (Art. 11(2), 5/1988). Alternatively, statements of support may be authenticated by special jurymen appointed by the promoter Commission of the initiative in question. To acquire the status of special juryman in Andalusia, individuals must swear or promise before the regional Election Board on the authenticity of the signatures and must be in full possession of the appropriate civil and political

rights (Art. 12(2), 5,1988).

**Slovenia:** Both the national and regional Popular Initiatives in Slovenia require the in-person authentication of signatories. For paper statements of support, signatories must attend the offices of the administrative unit where an officer of the unit will authenticate the identity of the signatory. Signatories that support an initiative online are not required to undergo in-person authorisation but are required to sign using a secure e-signature, verified by a qualified certificate.

The final characteristic noted in the analysis of the national or regional participatory instruments identified does not exist in a large number of initiatives but is noticeable due to its difference to the ECI, as well as national and regional level voting procedures. This trend relates to the **permittance of signatories from a younger age group compared with national electoral norms**. Three national and six regional instruments, identified across four Member States, permit the submission of statements of support by individuals of a younger age than the voting age for general elections. These examples are summarised in Table 20.

**Table 20: National or regional participatory instruments with reduced age criteria.**

| National or regional participatory instruments with reduced age criteria |
|---|
| **Belgium:** Compared with the voting age of at least 18 years old for elections, the national petition right, as well as the regional petition rights for Brussels, Flanders and Wallonia permit the submission of statements of support by individuals that are at least 16 years of age. |
| **Estonia:** For the Rahvaalgatus initiatives, the minimum age limit for signatories is 16 years old. Although the voting age for local elections is 16 in Estonia, this differs from the voting age for general elections, which is 18. |
| **Germany:** Compared with the voting age of at least 18 for federal elections, the regional participatory instruments implemented in Berlin and Bremen permit signatories to be at least 16 years of age and the regional participatory instrument of Hamburg does not specify an age limit for signatories. However, it is noted that these reduced age criteria do match the eligibility criteria for municipal elections in Berlin, Bremen and Hamburg, as well as state elections in Bremen and Hamburg. |
| **Luxembourg** has a voting age of 18 and, in 2015, rejected (with 81% "no" votes) a proposal to lower the voting age to 16. However, the national Public Petitions instrument permits the submission of statements of support by natural persons of at least 15 years of age. |

### V.1.3. e-Petition instruments

With regard to e-petition instruments, a distinction should be made between **official and private e-petition instruments**.

Beginning with the former, **official e-petition instruments** are operated by public bodies and permit citizens to petition a relevant public body (e.g. parliament, regional parliament or local body) to discuss a certain issue. It should be noted that official e-petition instruments are, in many cases, not that different from the Agenda-Setting Initiatives without popular vote discussed above, except that they put an "issue" rather than a specific proposal on the relevant authority's agenda. Given the isolated development of the national or regional participatory instruments examined, and thus the variations in existence, it is not surprising that clarity of categorisation is a difficult characteristic to obtain.

**Private e-petitioning instruments** are means offered by private entities (commercial or not-for-profit) through which citizens can petition public bodies to discuss, or take action on, a certain issue. There are both national and international (cross-national) schemes of this type and several take the form of offering a platform for organisers of e-petition schemes to use.

Box 10, below, provides examples of official and private e-petitioning instruments.

**Box 10: Official and private e-petitioning instruments.**

**National and regional *official* e-petitioning instruments**

**UK parliamentary e-petitions**: since 2015, and reviving an earlier system an e-petition instrument has been available at: https://petition.parliament.uk/. On its face, the instrument is considered to be successful, particularly with regard to engagement. For example, as many as 26,462 petitions have been opened; 372 petitions with more than 10,000 signatures got a response from Government and 47 with more than 100,000 signatures have led to a debate in the House of Commons. An important step, which mirrors the political screening in existence in the ECI, is the screening process conducted by a committee of MPs, the Petition Committee. However, "critics question the value of the website, claiming that it creates false expectations. Of the ten campaigns that garnered most signatures in 2016, four were denied a debate and none has so far succeeded in obtaining its intended outcome or implementing real change." In this way, its criticisms also mirror those levied at the ECI. To sign a petition, signatories must be either a UK citizen or resident in the UK and must provide their name, address and e-mail address. An interesting feature of the UK e-petition instrument is the inclusion of e-mail address, which allows signatories to be regularly updated on the progress of the petition they have supported.

In addition to the UK parliamentary e-petitions instrument, Scotland and Wales also have regional e-petition instruments. In **Scotland**, for example, the **e-petitioners system** has been in use since 1999. The e-petitioners system is actually a platform, offered to public and private bodies that want to organise petitions. In Scotland, the system operates under a partnership between the Scottish Parliament's Public Petitions Committee and industry (ITC and BT Scotland). The system is of particular interest because of its built-in verification and fraud prevention measures: "Signatories' names are displayed for transparency, but addresses are stored privately, ensuring that the system complies with data protection laws. The system automatically deletes duplicate signatures and provides administrators with graphical indicators of confidence in the validity of signatures, based upon automated checks. These compare IP addresses, e-mail addresses and check the name against a list. These indicators support the administrator's scrutiny of input. Administrators may also remove signatures which are offensive. Once the petition has run for its period, the system automatically generates figures of the numbers of signatures made (valid and invalid) as well as the regions from which these signatures came."

**Germany:** public-issue petitions to the German Lower House of Parliament (*öffentlichen Petitionen*, as distinct from individual petitions) are permitted on the basis of Article 17 of the German Constitution. Public petitions are open to all registered users of the petitions-portal. Similarly to the UK system and the ECI, the German instrument includes a parliamentary screening committee. Notably, individuals can support public petitions through other private e-petitioning fora such as OpenPetition and Avaaz.

**Trans-national *private* e-petitioning instruments**

**openPetition:** in operation since 2010, openPetition is a not-for-profit platform for e-petitions aimed mainly at the German-speaking parts of Europe but also accessible from other EU Member States: https://www.openpetition.de/. openPetition helps organisers to organise e-petitions and allows members of the public to sign up to the website; they are then kept informed of any new e-petitions. In 2015, openPetition announced that it wanted to make its platform available in all EU Member States' official languages and thereby make it available for ECIs. However, it does not appear that its system has been submitted for verification as an ECI online collection system. openPetition claims to reach 6 million people and receive 1 million visits

to its website each year; it started 3,500 new petitions in 2015 and collected 3,400,000 signatures in total[49]. Of particular interest is the fact that since August 2012 signatures for e-petitions in Germany submitted through the openPetition website can be verified by means of the new German e-ID card. The German Federal Printing Office has assured the security and reliability of the ID-verification function, which has been added to the new e-ID card. However, the use of the e-ID function when supporting a signature is optional.

**Change.org**: a commercial platform for e-petitions that can be used by campaigning organisations in a range of countries. It is known to be used by Amnesty International (US) and other organisations across France, Germany, Spain, Canada, the Philippines, the US and the UK. However, it has received significant criticism for its commercial approach and for exposure and even sale of personal data.

## V.2. Comparison of the personal data required by the ECI and similar national or regional participatory instruments

A key objective of the present study is to present a detailed and dedicated analysis of the data required by the ECI at the collection and verification stages, and how these requirements compare with the national or regional participatory instruments identified and detailed above. This section presents that comparison, focusing first on the data requirements for statements of support. Subsequently, the extent to which the verification and collection data requirements are aligned within the identified national or regional participatory instruments is examined and this alignment is compared to the alignment of the ECI data collection and data verification requirements, as analysed in section III.2.

### ECI statement of support data requirements vs. similar national or regional participatory instruments

As only 20 Member States have similar national or regional petitioning instruments that conduct verification, findings will be presented in percentages from this point to ensure comparability. Furthermore, for Member States that have more than one similar petitioning instrument, this analysis considers the instrument with the most stringent data requirements, with relevant context provided where necessary.

**Key to this analysis is the finding that similar national or regional petitioning instruments require signatories to provide fewer data[50] than the ECI.** In fact, 75% of the 20 Member States where national or regional participatory instruments have been examined require signatories to provide fewer data than for the ECI. Lithuania is the only Member State that requires signatories to provide more data for their national initiative (in this case, the Right of Referendum PAX instrument) than for the ECI.

Furthermore, the average number of data categories required for these similar participatory instruments is 3.2, compared with 4.5 for the ECI. Additionally, six of the data types (personal identification (document) number, nationality, date of birth, place of birth, name at birth and father's name) are required by fewer Member States for similar petitioning instruments than for the ECI. For example, 34% fewer Member States require a signatory's place of birth for similar participatory instruments (5%, i.e. 1 of 20 Member States) compared with the ECI (39%, i.e. 11 of 28 Member States). The range for the number of data required across the national or regional participatory instruments is also smaller than the comparable figure for ECIs – a difference between the initiative with the most and least data required is 3 compared with 4 for ECI implementation across the Member States).

[49] https://www.openpetition.de/blog/wpcontent/uploads/2 016/07/OpenPetition_Jahres-_und_Transparenzbericht_2015.pdf

[50] The data types considered for this analysis are categorised as follows: person identification (document) number; name (first and family); nationality; date of birth; place of birth; address; name at birth; father's / mother's name; e-mail; and any additional data types not listed but required / verified.

The type of data required most commonly in national / regional participatory instruments are name (100% of Member States, N=20), address (80%, 16 Member States), personal identification (document) number (50%, 10) and date of birth (55%, 11). The least common data required are name at birth (0%, 0), father's name, place of birth (both 5%, 1) and nationality (15%, 3). Furthermore, certain Member States require additional information such as the commune of which the signatory is registered to vote (IT).

Based on this analysis, it is clear that **similar national or regional participatory instruments require fewer data than the ECI.**

### Alignment of the data collection and data verification requirements

**For the national or regional participatory instruments examined, the key finding related to this sub-section is that the majority of Member States use all the data collected via statements of support for verification**. In fact, 85% (17 of 20) of Member States verify *only* the data required by a statement of support, and five of the 10 categories of data are verified in the same number of Member States as they are collected.

Two Member States verify fewer data than they collect (BG, LU) and Latvia appears to verify more data than it collects. In the case of Latvia, it is presumed that the signatories' personal identification card number, which they are required to provide, is tied to other relevant data (e.g. nationality, date of birth and address) which can be used to ensure each signatory meets the eligibility criteria.

The connection demonstrated (between the initial data requirements and the data required for verification) is further illustrated by the similarity of the average number of data (3.2 for statement of support data; 3.25 for verification data).

**For the ECI, the picture looks very different and the connection between the data collection and data verification requirements is a lot less consistent**. Compared with the 85% of national or regional instruments that verify all and only those data collected, the national level implementation of the ECI only achieves this in 57% (16 of 28 Member States). Therefore, for the ECI, 12 Member States verify fewer or more data to those collected.

In **conclusion**, the ECIs data requirements are more extensive than those required for similar national or regional participatory instruments, requiring, on average, more than one additional category of data. Although most Member States verify all the data collected by an ECI statement of support (and no more), 43% (12) of Member States do not, either verifying fewer or more data. As such, the data (required and verified) are more closely connected in national/regional participatory instruments, with only 15% (3) of Member States requiring different categories of data for verification as opposed to collection.

Moreover, stakeholders' familiar with both the ECI and national / regional participatory instruments have highlighted that the types of instrument, in terms of political and legislative influence, should govern the amount of data required. As such, the ECI is currently perceived to require more data than its influence as an agenda setting instrument suggests.

## V.3. Case study analysis

Whilst the full case studies are included as Appendix VIII.3, summaries of the analyses are provided below as they represent important inputs into the assessment of alternative options for the ECI data requirements detailed in section VI.

### United Kingdom of Great Britain and Northern Ireland

The UK online petitions website was launched in 2015 by the lower house of the UK Parliament, the House of Commons. It allows five members of the public to open an online petition, to which all British citizens and UK residents can add their name through a simple interface.

Petitions with over 10,000 signatures receive a response from the Government (although this is often just a one sentence response). The H/C Petitions Committee can (but is not required to) recommend that a petition be debated in Parliament and generally considers this for petitions that receive more than 100,000 signatures. Such debates have happened 56 times.

The only data asked for in the course of signing a petition on the e-petition website are: name; nationality (although this is not verified and there is no requirement to support proof of nationality or residence); address; and email address. These data are checked for duplication only: there is no other individual verification of the data. However, it is likely that the online system has a built-in, automated system to identify bots and fraud; although, documentation on these mechanisms is not disclosed.

The scheme can be said to constitute best practice in terms of ease of use, minimal data requirements and minimal data verification requirements, but with a built-in automated system to identify bots and fraud.

### Finland

The Finnish citizens' initiative, *Kansalaisaloite*, requires at least 50,000 Finnish citizens, who are entitled to vote, to submit an initiative for the enactment of an Act to the Parliament. The Parliament is obliged to take the citizens' initiative up for consideration, but thereafter it is at the Parliament's discretion whether the initiative will be approved or if it shall be amended in some way.

The most significant best practice that could be applied to the ECI is the link between the minimal data requirements of the *Kansalaisaloite*, the government platform used to host and organise initiatives and their effects on the participation of initiatives.

Similarly, the minimal data requirements for supporting an initiative have encouraged signatories to support initiatives, evidenced in part by the fact that approximately one third of all eligible Finnish citizens have participated in at least one initiative.

Finally, the government hosted online platform (www.kansalaisaloite.fi) for organising initiatives and collecting signatures has had a significant impact on the high level of participation in Finland, particularly among younger citizens.

### Berlin

Regarding Berlin two types of procedures for civic participation, the *Volksinitiative* and the *Volksbegehren* have been examined.

The *Volksinitiative* is a procedure of civic participation that allows the citizens to introduce a legislative proposal. Once the required number of signatures is reached, the parliament is obliged to take this proposal into consideration. The parliament is, however, free to decide on the outcome it gives to the popular petition.

The *Volksbegehren* is also a procedure that allows citizens to introduce a legislative proposal. Yet contrary to the popular petition, the *Volksbegehren* is only the first stage of a procedure for a referendum. If the parliament decides not to adopt the proposal of the *Volksbegehren*, a referendum will follow.

The most significant best practice that could be applied to the ECI is the link between proportional data requirements and the impact of the instrument, as evidenced by the reduced data requirements for participation in an *Volksinitiative* and a similar level of impact when compared to the ECI. In contrast, the *Volksbegehren* goes further than the *Volksinitiative*, offering a binding referendum in response to a rejection of the legislative proposal, with the same data requirements.

Another best practice example from the *Volksbegehren* is the fact that the instrument acts as the first stage of a referendum, requiring a small number of signatures to bring the proposal to the House of Representatives and an option to further pursue this proposal through a referendum should the authorities reject the legislative proposal.

### Switzerland

The Swiss Federal Popular Initiative is an instrument that enables citizens to propose changes to the Swiss Federal Constitution through 100,000 citizens signing a form in support within 18 months. The federal Parliament is obliged to discuss the initiative and to decide to recommend or to reject the initiative, or to propose an alternative. Whatever the Parliament chooses, all citizens will decide in a referendum whether to accept the initiative, the alternate proposal or to reject any changes.

The most significant best practice is the link between the high level of potential impact of the instrument and the resulting high level of participation in such initiatives.

Significantly, the extended period between the successful collection and verification of the signatures for an initiative and the popular vote on the initiative that it triggers assists in helping to ensure no changes are made to the Constitution based on temporary electoral pressures such as the recent upswing in nationalist feeling across Europe.

The binding nature of the subsequent vote on a successful initiative and its subsequent permanent changes to the Swiss Federal Constitution offer an instrument that carries real impact but is sheltered from short term electoral pressures.

### Slovenia

There are two participatory instruments in Slovenia similar to the ECI; both called the "popular initiative". They are recognised at local and national level as a citizens' participatory tool in public decision-making, including the possibility to suggest proposals amending the Constitution.

Slovenian citizens can propose a draft law to the National Assembly and participate in the legislative process that they originate. The proposed draft law must be supported by a minimum of 5,000 citizens/voters.

The best practice that could be applied to the ECI is the introduction of eID for statements of support which is currently used for pre-verification in the Slovenian popular initiative. The use of the national e-government portal (*e-uprava*) to securely register signatures of support presents an interesting case for the Member States that have existing e-government portals that use eID verification methods for citizens to access other government services. National level stakeholders consulted in Slovenia believe that the introduction of an eID would increase the public participation in the ECI. The use of existing national e-government systems offers the higher level of security against fraud that can eID can provide as well as potentially improving signatories' confidence in the security of their data and any resulting impact on participation that would incur.

## V.4. Best practices and negative elements: Similar participatory instruments

Building on the analyses presented above, this section first highlights best practices identified amongst the similar national or regional participatory instruments examined. These best practices will relate to both: i) the data requirements for these similar national or regional participatory instruments, as compared with the ECI; and ii) the verification mechanisms used by these similar participatory instruments, as compared with the ECI. Subsequently, this section presents common practices employed by similar participatory instruments that are not applicable to the ECI. Many of the practices highlighted below have influenced the alternative options for the ECI, described in section VI.

Regarding **best practices related to the data requirements**, it is key to note, as evidenced in section V.2, that the similar participatory instruments examined require fewer types of data at both the collection and verification stages. As such, there are some notable practices within these similar instruments that could provide insight for the future of the ECI, particularly with

regard to minimising data requirements as a result of suitably interconnected national authority information systems.

A prime example of this is the **Latvian** national instrument for referenda. Firstly, it requires that signatories only submit two types of data: their personal ID number and name. Although this is only one fewer than Latvia requires for the ECI, this is greatly reduced from the average number of data required for the ECI (4.5). Secondly, these two types of data are used, through the interconnection of relevant systems, to verify the signatory based on five separate but linked data: personal ID number, name, nationality, date of birth and address. This provides significant benefits to signatories and organisers, as it allows for a reduction in data requirements while maintaining the national authorities' ability to verify all the necessary data. In Slovakia, significantly fewer data are required for the National Petition Right than for the ECI. Signatories to a petition are required to provide only two data: their name and address, whereas Slovakian signatories to an ECI are required to six data: their name, nationality, date of birth, place of birth, address and name at birth.

Although not necessarily a best practice, it is interesting to note the apparent **trade-off, currently found in the ECI, between the number of data required and the harmonisation of the data required across the Member States**. It is clear that fewer data are necessary in Member States where a personal ID (document) number is required (average of 4.3 data), as compared with those Member States that do not require such a number (average of 4.9 data). However, it is also clear that the latter group of Member States present more harmonised data requirements (standard deviation from the mean of 0.7 data) than the former (standard deviation from the mean of 1.3 data).

Another practice of interest relating to the data requirements of the ECI and similar national or regional petitioning instruments concerns the **minimisation of data requirements** upon consideration of the intent and goal of the instrument in question. It has been found that in a several Member States, most notably the **Netherlands, Ireland and the UK**, national petitioning instruments have similar goals and deliver similar outcomes to the ECI (i.e. they are legislative agenda setting tools with the potential for legislative developments). However, these national petitioning instruments consider the need for greatly reduced data requirements, as well as simplifications of other elements of the process when compared with ECIs.

For example, the **Dutch** *Burgerinitiatief* (a popular petition instrument) requires that, in a similar manner to the ECI, organisers collect the required number of statements of support to bring the petition proposal to the Dutch Parliament. The Parliament are then required to discuss successful petitions. Key considerations in the establishment of the *Burgerinitiatief* included lowering the threshold for participation and reducing the workload for the parliamentary administration; this is evidenced by the fact that the Burgerinitiatief requires signatories to provide half the data required by the ECI. The Dutch national instrument requires that signatories provide their name, date of birth and address, whereas Dutch signatories to an ECI are required to provide their name, nationality, date of birth, place of birth, address and name at birth.

In addition, the **UK's** national petitioning instrument, *petition.parliament.uk*, is an online-only platform that allows British citizens, as well as UK residents, to petition the UK government on specific issues. At 10,000 signatures, the UK government is required to provide a response and at 100,000 signatures, the petition is considered for debate in the British Parliament. Signatories are required to provide their name, nationality, address and e-mail address. Although the data collected do not differ greatly from those collected for the ECI, limited verification is conducted, thus differentiating the UK petitioning instrument from the ECI. Signatures are simply checked to ensure persons have not signed multiple times or that automated attacks have not been conducted to add fraudulent signatures. In addition, similar regional initiatives, which require fewer types of data, exist in Scotland and Wales.

A similar relationship between the impact of an instrument and reduced data requirements is experienced in the regional participatory instruments of **Berlin, Germany** (i.e. the *Volksinitiative* and *Volksbegehren* – see full case study at Appendix VIII.3.3.). In fact, the *Volksbegehren,* which acts as the first stage of a referendum, represents a greater political outcome than the ECI; however, the data requirements are still reduced in comparison to the ECI. The *Volksbegehren* and the *Volksinitiative* require signatories to provide their name, date of birth and address.

Such national or regional participatory instruments are considered by many stakeholders to provide a **more coherent link between the data requirements for collection and verification and the goal or outcome of the instrument**, as compared to the ECI.

Regarding **best practices for verification**, the key finding relates to the **increased coherence found between the data collected and the data verified** for national and regional participatory instruments as compared with the ECI. In fact, 85% of the Member States, in which national and regional participatory instruments were examined, verify only the data they collect. For the ECI, however, only 57% of Member States verify the exact data they collect.

Another key trend that brings efficiency benefits to ECIs and the similar participatory instruments relates to the **use of technology to facilitate verification**. It has been found that several Member States use specialised software to automate the verification of online statements of support, and to facilitate the processing of paper statements of support. Furthermore, for similar participatory instruments in several Member States, the specialised software is also capable of providing (near) immediate verification.

For instance, in **Finland**, software is used in both the ECI and the *Kansalaisaloite* (the Finnish citizens' initiative established in 2012) to automate the verification of online statements of support. This software works by automatically matching the personal data from the statements of support to the population register. Furthermore, the software generates statistics on invalid statements of support, allowing quick identification and manual checks of invalid statements. An additional positive aspect of the Finnish *Kansalaisaloite*, although not related to verification, is the role of the government hosted online platform (www.kansalaisaloite.fi), developed to factilitate the organisation of such initiatives, and the complementary grassroots debating platform (www.avoinministerio.fi). These platforms provide a dedicated location for the organisation and participation in the initiative, as well as a location for discussions on related topics. Similarly, the **German** instrument for submitting public-issue petitions to the Lower House of Parliament (*öffentlichen Petitionen*) demonstrates interactions between the state and private websites, as it permits signatories to submit statements of support through private e-petitioning fora such as OpenPetition and Avaaz.

Returning to the relevant applications of technology, **Slovenia** further develops the capabilities on offer in the Finnish system, although only for the so-called popular initiative (i.e. a national participatory instrument) and not for the ECI. For the popular initiative, statements of support are collected through the *e-uprava portal*, which requires a secure e-signature, verified by a qualified certificate. The signatory is then notified immediately if his/her statement of support is refused. In **Lithuania**, for both the ECI and the similar national participatory instruments (i.e. the citizens' right of legislative initiative, the right of petition and the referenda), the verification of paper statements of support is facilitated by the scanning of these statements of support such that the data is contained electronically.

Although these mechanisms do not provide further simplicity, due to the need for the development of software, they do bring significant efficiency savings to the verification of statements of support and, in relation to the ECI, can improve the security of paper statements of support in transit from ECI organisers to the national verification authorities. Such security improvements would be delivered by the fact that paper statements of support, when being transferred in digital format, would be able to take advantage of the established security measures currently in place to secure online statements of support in transit.

Beyond these practices, which could benefit the ECI (as discussed further in section VI), it is considered that **many characteristics of the similar national and regional participatory instruments examined are not applicable to, or would not benefit, the ECI, if implemented**. These relate to the focus of many national and regional participatory instruments on the following elements:

- **Voter registration as an eligibility criteria:** this is a key eligibility criteria for a large proportion of the national and regional instruments examined. In fact, 68% of the instruments examined include voter registration as an eligibility criteria or rely on electoral rolls for verification. If implemented in the ECI, this approach is likely to exclude EU citizens from participating, particularly in those Member States where voter registration is not mandatory. **Only using paper statements of support:** as detailed above, 63% of the national and regional participatory instruments examined rely solely

on the collection of paper statements of support. Given the ECI's firm commitment to collecting online statements of support, and the related benefits highlighted above, there is limited applicability of national and regional practices in this respect. Furthermore, significant comment has been made on the benefits of using both paper and online statements of support for ECIs. Regarding online statements of support, national authorities agree that, from an efficiency point of view, online statements of support are much easier to verify than paper ones. Moreover, several officials felt that it would be a significant improvement if citizens and residents could use their official (state-issued) e-ID in the process, as that would greatly facilitate verification. Regarding paper statements of support, however, ECI organisers see paper collection as a key aspect of the process for a number of reasons. Firstly, it allows for a clear explanation to the potential signatory of the reasons why the data is needed. Secondly, paper collection campaigns are key to ensuring the ECI's message is advertised.

- **In-person authentication:** linked to the reliance of paper statements of support, 42% of the national and regional instruments examined require in-person authentication of signatories. Firstly, authentication of signatories is not a verification purpose under the ECI Regulation. Secondly, the mechanisms in place for this (i.e. making a dedicated in-person appearance at the relevant national authority building or including an official authenticator in each team collecting statements of support) would add complexity to the implementation of ECIs and are thus not considered to be applicable.
- **Limited (i.e. tick-box or ad-hoc) verification mechanisms:** in a small number of Member States (Belgium, Slovakia and Sweden), the national and/or regional participatory instruments examined implement verification mechanisms that are considered to be insufficient in comparison to the ECI. For instance, stakeholders in **Sweden** remarked that, given the lack of a formalised process, it is highly unlikely that the verification for any two *Folkinitiativ* People's Initiatives are conducted in the same way. Similarly, in **Slovakia**, the verification mechanisms only check that the relevant data have been entered with no check on the veracity of the data, and the law enacting the national petitioning instrument dictates no formal requirements for a minimum number of signatories and no minimum age of signatories. **Belgian** stakeholders add to this sentiment, commenting that the ECI is more advanced than the national and regional petitioning instruments, and thus could learn no lessons from them. The verification mechanisms for the Belgian national and regional instruments are devised in an ad-hoc fashion, and sometimes not at all.

# VI. Alternative options for the ECI data requirements

*Chapter VI presents possible options for the simplification of data requirements both within the context of the current legislative framework (i.e. the current ECI Regulation) and outside of it.*

## VI.1. Overview

In line with the Commission's Better Regulation Guidelines, policy options for any legislative change need to be identified in order to achieve policy objectives. The general objective of the ECI should be to ensure the application of Article 11(4) TEU. In order to do so effectively, the ECI's specific objectives (as set out in the recitals of the current ECI Regulation) in relation to the collection of statements of support should be to ensure that (i) the procedures and conditions are clear, simple, user-friendly and proportionate to the nature of the citizens' initiative, so as to encourage participation by citizens; (ii) the protection of the personal data of signatories is ensured; and (iii) fraud is avoided. These objectives can be further laid out in the following operational **policy objectives**:

- To simplify the data requirements for signatories of statements of support (proportionally to the outcome);
- To ensure all eligible EU citizens are able to support an ECI;
- To ensure only eligible citizens are able to support an ECI while minimising the burden of verification;
- To ensure that the personal data of supporters is safeguarded.

On the basis of the research undertaken for this study, a number of policy options have been developed to achieve these policy objectives. The options presented below were developed on the basis of:

- best practices for simplification/efficiency at both stages of completing the statement of support by signatories; and verification by national authorities for ECIs;
- best practices from other similar national, regional and local participatory instruments;
- risk treatment options identified through the data protection and security risk assessment;
- alternative options put forward by stakeholders consulted as part of the study.

Each of the options is described in greater detail below, with the advantages and disadvantages highlighted, before being assessed against the **policy objectives**. Furthermore, the below assessments present whether the option would **require changes** to the ECI Regulation and or Annex III. and what is the impact of such option on the different key risks identified in the Risk Assessment under Section III.4. When risks are not discussed in relation to the specific options, it is to be understood that the analysed option has no impact on these risks.

Options 1.1 and 1.2 are stand-alone. They cover both the collection on paper and online and focus strictly on the data to be provided by signatories. Options 2 and 3 relate to the responsibility for the collection and/or the transfer of the signatories' data.

## VI.2. Policy options for the simplification/harmonisation of data requirements

On the basis of the assessment undertaken as part of this study, a number of overarching principles need to be taken into account when identifying and assessing possible options:

- The **current levels of verification are considered appropriate** in terms of verification mechanisms. Consequently, the options entailing substantial lowering or substantial increase in the verification standards have been excluded from further analysis;
- **Paper collection should continue** – there is a consensus amongst all stakeholders that while the online collection of statements of support is important, paper collection should continue. This is seen as one of the strengths of the ECI and is also considered by organisers as an important tool to gather support for their campaign;
- **Streamlining the data required** – on the basis of the two points above, there is a need to ensure that data collected is limited as much as possible and that they are harmonised and streamlined as much as possible.

### VI.2.1. Option 1: Simplification and harmonisation of the data requirements

Based on the research undertaken, the recommendation of this study would be to follow the **nationality principle** when deciding whose statement of support national authorities should verify.

While adopting a mixture of both the residence and the nationality principle seems appealing at first, a number of arguments favour the use of the nationality principle only.

The majority of registers used by Member States for the purpose of verification are national registers of **citizens** from that Member State (as opposed to **residents**). Whilst these frequently include **all residents** of the relevant Member State, both their own and foreign nationals, as well as all nationals of the Member State regardless of their residence, this is not homogeneous across the Member States.

Furthermore, some Member States do not require non-national EU citizens to register. In addition, as a result of the principle of free movement, there is an increasing difficulty for Member States to keep track of residents (even when they are required to register) and citizens alike. In practice, the records of these residents are not always regularly updated.

Moreover, in practice the use of both criteria increases the risk of citizens supporting an ECI twice as well as requiring additional data in order for national authorities to undertake the verification.

On the other hand using the residence principle only would exclude citizens residing outside of the EU.

Therefore, the use of the nationality principle in deciding who should verify citizens' statements of support would be most appropriate.

It would ensure the use of existing registers by national authorities, and therefore incur no additional difficulty or cost in gathering new data on residents or citizens.

While it would require two Member States (UK and Ireland) to adapt their verification mechanisms, it would be the least invasive and obstructive change to the current situation.

<u>Option 1 – Description</u>

Two sub options have been identified; Option 1.1 where one set of data is accepted by all Member States, and Option 1.2. where two sets of data would be developed, one for Member States requiring a personal ID (document) number and one for those not requiring such data. This section discusses the verification mechanisms and the registers available in all Member States for statements of support in order to assess in which ways the data required could be simplified.

Option 1.1:

When comparing the level of data requested to support an ECI by Member States with the level of available information on citizens in registries across all Member States (including registries not currently used in the context of the ECI), it first appears that there is scope for a reduction of these data requirements. The **name**, **surname**, **address** and **date of birth** of citizens form the core of the population registers across the Member States, with competent national authorities having access to this information in all Member States through their primary or secondary register used for verification or through another existing register (such as the electoral roll in France).

This information would allow for the verification of condition 2 (the natural person is supporting an ECI is an EU citizen). Similarly, using the date of birth, authorities would be able to verify that the signatory was of the age to be entitled to vote in elections to the European Parliament, as per condition 3.

The majority of Member States maintain event-based public registers, i.e. ones formed of information given at specified events (such as birth and marriage or elections). This does raise some concerns over the accuracy of some of the data due to the irregular intervals of updating the information. Conversely, this ensures that all relevant persons are included in the register from birth or from the date they become eligible to vote in the European elections. Consequently, the use of **addresses** as part of the verification is questionable using these registers.

Whilst the accuracy of the address listed for citizens on the relevant register is in turn affected by the fact that the information stored in the register was given at these specified moments and could therefore be inaccurate, citizens are often required to notify the relevant authorities of a change in their address. Similarly, some of these registers act as the local electoral roll as well as a population register, and so hold the same level of accuracy as electoral registers hold. In other Member States (such as France for instance), the electoral roll maintains an up-to-date record of citizens' addresses but might not hold all the information held in the public register.

In case Member States use these registers as their electoral rolls, the information held within them must be (at least at the time of elections) of an acceptable level of accuracy to the national authority. It can therefore be taken as a similarly acceptable level of accuracy for the purpose of verification for an ECI given the proportionality principle (i.e. what is acceptable for a national election should be acceptable for supporting an ECI). This is supported by the fact that citizens in several Member States access local public services and therefore need an accurate address for correspondence or registration. Furthermore, as stated above, in some Member States, foreign EU nationals who are residents are not required to register with local or national authorities. This further supports the use of the nationality principle, as the data on foreign EU nationals that are resident in a Member State are likely to be more inaccurate, especially with regard to recent foreign EU national residents.

In assessing the applicability of similar national and local level instruments, Berlin's *Volksinitiative* presents an interesting comparison in proportionality of data requirements and impact due to the fact that it has minimal data requirements of signatories', in line with the proposed reduction under this option, and an almost identical level of limited impact on the local level, simply prompting a debate in the House of Representatives with no certain recourse.

In summary, the analysis of national population registers highlights a common minimum set of data available to Member States' competent authorities for the purpose of verification. Furthermore, it highlights the fact that significantly reduced data requirements could be implemented across Member States due to the fact that conditions 2 and 3 of the verification process can be met with minimal data points for signatories if the nationality principle is considered. This would of course assume that in addition to the **name**, **surname**, **address** and **date of birth,** supporters be asked their **nationality** in order for the statements of support to be directed to the right verification authority.

A potential risk that could impact the rate of rejection for statements of support and result in wrongful invalidation would be the accuracy of the address in the national registers. The frequency at which the national registers are updated depends on the Member State and there is a concern over the accuracy of this data set across all Member States.

However, when assessing the availability of addresses, and in particular the extent to and the regularity at which they are updated, the situation becomes more problematic, especially in the case of nationals living abroad. In a number of Member States, such as France, the address of nationals' living abroad is only available either through the (non-compulsory) register of people living aboard, or through the electoral registry. This implies however, that some people would be excluded (although the number would be limited – there were 49 million French citizens above the age of 18 according to the INSEE in 2017, and 47 million people registered to vote). In other Member States such as Greece or Ireland, citizens living abroad are either established in the community in Greece they were previously registered in; given voting is compulsory in Greece, an address even in the country would be available. In Ireland, citizens abroad are not included in the register because there is no requirement for them to register to vote and they are not entitled to vote if they live overseas. These examples show how the reduction in the number of data points under this option would result in the need to loosen the verification conditions and therefore go against the policy objective of ensuring that all eligible EU citizens are able to support an ECI.

It is important to highlight that, as discussed in section IV, one's address is considered in some Member States to be as sensitive or indeed more sensitive than the personal ID (document) number. Furthermore, while this proposed set of data would reduce the number of data points in the majority of Member States, it would increase it for six Member States who currently require less data (generally full first names, family names, nationality and personal identification (document) number) – see section III.2.2. For those Member States currently requiring a personal identification (document) number, this option would also increase the burden of verification as what is currently a relatively easy process might become more complicated. Most importantly, and as mentioned above, the main issue with this option is that, following the nationality principle, UK and Irish citizens living abroad would fall outside of the system and would therefore de facto be excluded from supporting an ECI.

Option 1.2:

As an alternative, option 1.2 would therefore require two sets of data, the first one for Member States able to identify their nationals simply on the basis of the set of data listed under option 1.1 (**name, surname, residence/address, date of birth** and **nationality),** the second one for those Member States not able to verify addresses either for all citizens or only for those living abroad. For those, the data required would not include the address and date of birth, but the passport or ID number instead.

In other words, under this option, two sets of data could be used:

- Nationality, name, surname, residence/address and date of birth;
- Nationality, name and personal ID (document) number (or last three or four characters only)

The rationale behind the second (simplified) set of data relates to the fact that the personal ID (document) number would allow verification authorities to check the conditions of validity of a supporter (notably age) without the need to ask the supporter for additional information.

In order to further simplify the data and to address the fact that providing a personal identification number is seen in some countries as more sensitive than providing other data, one possibility would be to ask supporters to only submit the last three or four characters of their personal ID (document) number. On the basis of the numbers required, there does not appear to be any technical issue with this option, given each of these numbers are given at random and are not related to either the date of birth of the citizen, or the location of their residence (see Table 1 - Personal identification (document) number requirements, per Member State, and availability of those numbers to non-national EU citizens).

This option has also the following advantages:

- It would allow to take into account any preference at national level in relation to the sensitivity to provide certain types of data (ID number vs. address)
- It would not lead to an increase in the number of data to be provided in any country

- It would ensure a more reliable verification process based on data sets closer to the current system. It is therefore likely to create less burden for Member States to adapt their verification process.

Almost all Member States would be able to introduce either of these checks without need for additional information. The two exceptions are the UK and Ireland, where, as described above, nationals residing abroad are not in any population register. One possibility would be for those two countries to have a different approach and ask for the first set of data (i.e. including the address) to nationals residing in the country, and the second set of data (including passport number) to their citizens residing abroad.

**Table 21: Data available in national registries the list of relevant registries can be found in Appendix VIII.5 (those registries are not necessarily the ones currently used in the context of the ECI)**

| | Full first names | Family name | Mothers/Father's name and other identifiers | Residence | Date of birth | Place of birth | Nationality/ citizenship status | PINr / PI Doc & nr./Passport | Sex | Country of origin | Registration number | Resident status | Issuing authority/ Registration address |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **MS that do not require personal ID numbers/personal ID document details:** | | | | | | | | | | | | | |
| IE | X | X | | X | X | | X | | | | | | |
| UK | X | X | | x | X | | | | X | | | | |
| EE | X | X | X | X | X | X | X | X | X | X | X | X | |
| NL | X | X | | x | X | X | X | | x | | | | |
| SK | X | X | | x | X | X | X | x | | | | | |
| FI | X | X | X | X | X | | X | X | X | X | | | |
| BE | X | X | | x | X | X | X | | x | | X | x | |
| DK | X | X | | x | X | X | X | x | x | | | | |
| DE | X | X | | x | X | X | X | | x | | | | |
| LU | X | X | | x | X | X | X | x | | | | | |
| **MS that do require personal ID numbers/personal ID document details:** | | | | | | | | | | | | | |
| BG | X | X | X | X | x | x | | X | x | | | x | |
| CZ | X | X | | x | x | | | X | | | | x | |
| EL | X | X | x | x | X | | | | x | | x | | |
| ES | X | X | | x | X | x | | X | x | | | | |
| FR | X | X | | x | X | X | | | x | | x | | x |
| HR | X | X | | x | x | | X | X | x | | | | |
| IT | X | X | | x | X | X | X | x | x | | | | |
| CY | | | | | | | | | | | | | |

| | Full first names | Family name | Mothers/Father's name and other identifiers | Residence | Date of birth | Place of birth | Nationality/ citizenship status | PINr / PI Doc & nr./Passport | Sex | Country of origin | Registration number | Resident status | Issuing authority/ Registration address |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| LV | X | X | | x | X | | X | X | x | | | | |
| LT | X | X | | x | x | | | X | | | x | | |
| HU | X | X | x | x | x | x | X | X | x | | | | |
| MT | X | X | x | x | X | | | X | x | | | | |
| AT | X | X | | x | X | X | X | X | x | X | x | x | |
| PL | X | X | x | x | x | x | X | X | x | | | | x |
| PT | X | X | x | x | X | | X | X | x | | | | |
| RO | X | X | | x | X | | X | X | | | | | |
| SI | X | X | x | X | X | X | X | X | x | | | x | |
| SE | X | X | | x | X | X | X | X | | | | | x |

Option 1 - Data to be collected

As a result of the discussion above, the data to be collected under this option would include:

- Option 1.1:
  - Name;
  - Surname;
  - Residence/address;
  - Date of birth;
  - Nationality.
- Option 1.2:
  - Name;
  - Surname;
  - Last three or four characters of the personal ID (document) number
  - Nationality.

Option 1 – Ways in which the option addresses the policy objectives

| Policy Objective | Option 1.1 | Option 1.2 |
|---|---|---|
| **To simplify the data requirements for signatories** | Increased simplification and harmonisation of the ECI data requirements will allow citizens to be more comfortable with the data they are providing.<br>Increased simplification and harmonisation would significantly increase the ease with which ECI organisers can collect statements of support.<br>Increase in the number of data to be provided in some countries | Increased simplification and harmonisation of the ECI data requirements will allow citizens to be more comfortable with the data they are providing, they will however still need to provide all or part of their personal ID (document) number, which they might not know.<br>Increased simplification and harmonisation would significantly increase the ease with which ECI organisers can collect statements of support. |
| **To ensure all eligible EU citizens are able to support and ECI** | Some categories of citizens might experience difficulties in supporting an ECI, in countries where addresses are not regularly updated in the registers or if they have lived abroad for some time. UK and Irish citizens living abroad would be excluded. | All eligible citizens would be allowed to support an ECI. |
| **To ensure only eligible citizens are allowed to support an ECI with a minimal burden of verification** | Option 1.1 would be negative due to the inability of some verification authorities to use the address for verification purposes.<br>It is possible that this will require amendments to current processes and/or data sources in some Member | This option provides for a reliable verification process in all countries. This option might require amendments to current processes and/or data sources in some Member States, also to a lesser extent than option 1.1. As no significant changes are foreseen, this should not lead |

| Policy Objective | Option 1.1 | Option 1.2 |
|---|---|---|
| | States. | to significant additional costs. |
| **To ensure that the personal data of supporters is safeguarded** | As fewer data would be collected under this option, the risks to personal data would be more limited. | As fewer data would be collected under this option, the risks to personal data would be more limited. |
| | **The likelihood of Risk 2 being realised (**Reduced ECI participation as citizens are required to provide too many data) reduces | **The likelihood of Risk 2 being realised (**Reduced ECI participation as citizens are required to provide too many data) reduces |
| | **The likelihood of Risk 3 being realised (**Reduced ECI participation as citizens are required to provide too sensitive data) reduces | **The likelihood of Risk 3 being realised (**Reduced ECI participation as citizens are required to provide too sensitive data) reduces |
| | Given the significant harmonisation of data requirements, the future **likelihood of Risk 6 being realised reduces**. | Given the significant harmonisation of data requirements, the future **likelihood of Risk 6 being realised reduces**. |

Option 1 – Changes to the Annex III or the Regulation

This would require changes to annex III to the ECI Regulation. The Commission can make these changes itself, without having to follow the full legislative process that would be needed for amendments to the Regulation proper, but it may only do so only after "appropriate consultations during its preparatory work, including at expert level" (Recital 24) and provided it "tak[es] into account information forwarded to it by Member States." (Recital 12). The EP and the Council can object to such changes (Art. 19). In practice, it would be very difficult to make such substantial changes to the data requirements without wide agreement on this by the Member States.

Option 1 – Conclusion

Overall, option 1 presented above proposes a significantly improved ECI in terms of meeting its policy objectives, of reducing data to be collected from statements of support and of improving the risk assessment of the ECI.

Following the causal link between data requirements and participation, any resulting increase in participation in the ECI can, in part, be attributed to the reduced requirements of the proposed option. Similarly, due to the removal of potentially sensitive data, the likelihood of a reduced participation due to the provision of sensitive data is reduced from medium to low.

Following the analysis of the national registers of the Member States, we know the proposed minimum sets of data are available to the relevant authorities for the purpose of verification. As discussed above, the risks to personal data would be further limited by this policy option, as the reduced requirements offer a less attractive target for data breaches and fraud.

While Option 1.1 would go a long way in simplifying and harmonising the data requirements for supporters of ECIs, it has one crucial flaw exposed above: the increased number of citizens excluded and therefore *de facto* excluded from exercising their Treaty rights. Furthermore, not all Member States would be able to undertake the necessary verification and for some Member States, this option leads to an increase in the number of data points they currently collect (notably for the six Member States who currently collect only the full names, nationality and personal identification document of signatories).

Option 1.2 builds in a level of flexibility to ensure that all citizens are allowed to support an ECI, and to take into account any preference at national level related to the sensitivity to provide

certain data (address vs. last three or four characters of the personal ID (document) number) It would not lead to an increase of the number of data collected in any country, except in Finland where the full address would be required instead of only the country of permanent residence but this would be the case under both options.

Consequently, option 1.2 is the most viable of the two, ensuring all EU citizens can participate in an ECI, that the data to be collected are minimised in all countries and that statements of support can be verified by all competent national authorities.

## VI.3. Policy options allowing to transfer the responsibility for the protection of personal data

Under this set of options the responsibility for the protection of personal data (see section III.3) would be transferred. They relate to the collection of statements of support themselves and are therefore independent and not directly related to the data to be collected discussed under Option 1. As such, the options presented here would make more sense if applied in conjunction with one of the sub-options presented above. Furthermore, as noted above, the sensitivity of certain data points depends to a large extent on the organisation (or type of organisation) in charge of collecting these data (government, private company, European Commission etc.). This finding is reflected in the following two options, discussed below:

- **Option 2** presents the possibility of transferring all responsibility for the collection, storage and transfer of personal data submitted through online statements of support to the European Commission.
- **Option 3** presents two possibilities for amendments to the mechanisms for handling the personal data of signatories submitted through paper statements of support.

### VI.3.1. Option 2: Commission central online collection system

As referred to above, proposed Option 2 relates to the establishment of a sole, central collection system for online statements of support, for which responsibility lies with the European Commission. This includes both the online collection software and the hosting environment and contrasts with the current system where the ECI organisers act as data controller with the Commission as just a processor.

The policy objective on which Option 2 would have the most prominent impact relates to ensuring that the personal data of supporters is safeguarded. From the perspective of ECI organisers, Option 2 would bring a significant positive impact in comparison to the current situation. Not only would all responsibilities and liabilities in relation to the collection of online statements of support be removed from the organisers, significantly reducing the risk of conducting an ECI, but ECI organisers would also not need to implement online collection software and hosting environments, which requires some technical expertise.

From the perspective of the European Commission, however, Option 2 would greatly increase their responsibilities and liabilities in relation to collecting, storing and transferring the personal data submitted by signatories. This change in the ECI mechanisms would also work to mitigate six of the risks assessed in section III.4. More specifically, risks 10-12, which relate to the storage of personal data of signatories submitted online in third party hosting environments, would be avoided; and risks 19-21, which relate to the transfer of online statements of support to national authorities, would be very substantially reduced due to the removal of ECI organisers from the transfer process (reduction in the attack surface) and due to introduction of the secure file transfer mechanism.

Moreover, the use of a central Commission-hosted online collection system would benefit the ECI in bringing the capability to conduct data analytics to potentially detect suspicious statements of support using a consistent methodology (in a similar fashion to the UK petitions

system). The transparent and extensive monitoring and risk analyses conducted on the Commission's hosting environment would also represent a benefit in comparison to current third-party hosting environments, which are certified only once. Furthermore, the implementation of Option 2 would facilitate the introduction of the options listed under Options 4 and 5, below, including, for example, the introduction of a two-step data collection process and the use of eIDs.

From the perspective of ECI signatories and, more generally, EU citizens, Option 2 could instigate mixed feelings. On the one hand, it may be argued that the introduction of hosting by the Commission would allow for a more trusting environment in which signatories have greater faith in the body to which they are submitting data. As discussed in section IV, signatories are reportedly more likely to provide personal data if they trust the authority collecting those data. Furthermore, given the greater capabilities of the Commission as compared with ECI organisers, the implementation of Option 2 may have a dissuasive effect on the submission of fraudulent statements of support. On the other hand, EU citizens may argue that Option 2 represents a removal of freedoms from ECI organisers and a reduction of an organiser's independence.

An existing example is the process for the Finnish national participatory initiative *Kansalaisaloite*, where it is already possible to submit statements of support directly from a government website dedicated to popular initiatives.

Option 2 – Ways in which the option addresses the policy objectives

| Policy Objective | Option 2 |
|---|---|
| **To simplify the data requirements for signatories** | Not relevant - dealt with under Option 1 |
| **To ensure all eligible EU citizens are able to support an ECI** | Not relevant - dealt with under Option 1 |
| **To ensure only eligible citizens are allowed to support an ECI with a minimal burden of verification** | Although Option 2 does not directly impact verification, it will likely allow for greater identification of suspicious statements of support and will increase the security of the process for transferring statements of support to national authorities |
| **To ensure that the personal data of supporters is safeguarded** | Option 2 has a significant positive impact on the safeguarding of supporter's personal data. As described above, the transference of data handling responsibilities and liabilities from ECI organisers to the Commission delivers significant benefits to the former. Furthermore, the Commission hosting environment allows for greater control, monitoring and an ability to improve the data storage and transfer processes.<br><br>These benefits also translate to the risk assessment. **R10-12**, related to third party hosting are avoided, and **R19-21**, related to the transfer of statements of support collected *online*, will be substantially reduced due to the use of secure file transfer mechanism. |

Option 2 – Changes to the Annex III or the Regulation

The Regulation would need to be modified to remove the possibility for ECI organisers to establish, and receive certification for, third party online collection systems (including both hosting environments and online collection software). Instead, the Regulation text would need to clearly outline the role of the Commission's system as the sole collection system.

More specifically, points 15 and 16 of the ECI Regulation's pre-amble will no longer be needed and significant amendments to article 6 will be required.

Option 2 – Conclusions

Option 2 only improves the implementation of the ECI in relation to the policy objectives (if implemented in addition to paper collection), although there are minor challenges that will be faced. Most prominently, in relation to the amplification of hosting being undertaken by the Commission in comparison with the existing process, and less so with regard to how the removal of the option to host an online collection system from ECI organisers may be perceived by the organisers and EU citizens.

Beyond these minor challenges, it is clear that significant benefits, in particular for the policy objective related to safeguarding the personal data of supporters will be achieved by the implementation of Option 2.

Furthermore, this option facilitates the introduction of the options discussed under Options 4 and 5, and can be implemented alongside Option 3 and either of the options presented under Option 1.

### VI.3.2. Option 3: Relating to the collection of paper statements of support

The following options only relate to the collection of paper statements of support. It is crucial to consider this element for two main reasons; firstly, is to avoid discriminating against those segments of the population who do not have access to the internet or are not computer literate; secondly, as evidenced by our in-depth interviews with relevant stakeholders, ECI organisers see the collection of paper statements of support as an important aspect of campaigning. These options do not relate to which data are collected but to the way in which paper-based statements of support would then be processed. There are two different possibilities:

- Option 3.1 – once collected and the verification stage reached, the paper statements of support are scanned by the organisers such that they are automatically uploaded onto an online collection system;
- Option 3.2 - once collected and the verification stage reached, the information contained in the paper statements of support are manually entered by the organisers in an online collection system;

The case of Lithuania highlights an existing example of Option 3.1 as, for both the ECI and the similar national participatory instruments (i.e. the citizens' right of legislative initiative, the right of petition and the referenda), the verification of paper statements of support is facilitated by the scanning by the verifying authority of these statements of support such that the data is contained electronically (i.e. each set of personal data, submitted through paper statements of support, exists as if it were submitted via an online statement of support).

Options 3.1 and 3.2 have an impact on the data protection responsibilities and liabilities, in that it replaces the transfer of the paper statements of support from the organisers to the verification authorities with the inputting of the paper forms or of the data from the paper forms directly into the online collection system. To maximise the benefits of such options, the system should be under the responsibility of the Commission who would also be in charge of transferring the statements of support to the national authorities via a secure file transfer mechanism.

(see option 2 above). The upload function in the system would also be provided by the Commission as part of the system. Under these options, **the organisers would be responsible for ensuring that those data are correctly entered into the Online Collection System; and they would assume new liabilities in relation to any errors, erroneous deletions or data losses in this process.**

Additional effort for organisers will be required due to the need to upload (by some means) paper statements of support to the system. Option 3.1 would require that ECI organisers have

the capability to scan paper statements of support. This represents a limited technical and financial burden for ECI organisers. Option 3.2 presents no additional technical requirements. Financially, however, it will likely have implications due to the significant resource needed on the organisers' side to manually enter data from the paper statements of support.

However, the advantages of both options for organisers are the increased data security, the limitation of their liability and the removal of the burden and associated risks (notably risks of data loss) related to the submission of the statements of support to each national authority for verification.

As regards national authorities in charge of the verification of statements of support, the verification will be easier especially in the case of option 3.2 as they would only have to deal with an electronic database. Option 3.1 would also facilitate the verification, especially if Member State has software to digitalise the scanned statements of support. This could however be limited by the technical risk of the quality of the scans.

Option 3 – Ways in which the option addresses the policy objectives

| Policy Objective | Option 3.1 | Option 3.2 |
|---|---|---|
| **To simplify the data requirements for signatories** | Not relevant - dealt with under Option 1 | |
| **To ensure all eligible EU citizens are able to support and ECI** | Not relevant - dealt with under Option 1 | |
| **To ensure only eligible citizens are allowed to support an ECI with a minimal burden of verification** | Reduction in risks related to transfer of paper statements of support and benefits to national authorities of only verifying online statements of support if they can use optical recognition tools to extract the data from the scanned statements – a process which can, and has, been automated by Member States.<br><br>Additional risk related to the accuracy of the scanning and optical recognition tool technology. | Reduction in risks related to transfer of paper statements of support and benefits to national authorities of only verifying online statements of support – a process which can, and has, been automated by Member States.<br><br>However, additional risks to this policy objective due to the accuracy of data capture at the point where paper copies are manually encoded; and there is increased opportunity to perpetrate the submission of fraudulent statements of support, bypassing existing mitigation measures |
| **To ensure that the personal data of supporters is safeguarded** | Additional risk related to the accuracy of data capture but risks 16-18, which relate to the transfer of on paper statements of support to national authorities, would be significantly reduced. | |

These options would affect the following risks to the ECI (as identified by the Risk Assessment presented in section III.3) as follows:

**Table 22: Impact of Options 3 on risks to the ECI, and the rationales for the determined impacts.**

| Impact of Option 3 on the key risks identified in the risk assessment | |
|---|---|
| **Risk 4:** Fraudulent activities to increase support for an ECI | |
| **Rationale:** | **Applicable only to Option 3.2:**<br><br>The fact that the digitalisation of paper statements of support would be conducted by ECI organisers provides increased opportunity for fraudulent addition of signatories (i.e. without paper equivalents).<br><br>Furthermore, paper statements of support would still not benefit from all of the control measures placed on online statements of support as the typing of statements of support would not allow for the identification of fraudulent submissions that examine the data for the patterns of submissions from the same location / IP address or those submitted within a short period of time from the same location (i.e. hallmarks of bot attacks). This is because the typing in relation to the digitalisation of paper statements of support would bear the hallmarks of fraudulent behaviour.<br><br>As such, the likelihood of this risk being realised increases from unlikely to a moderate likelihood; the impact, however, would remain the same (moderate). |

| **Risks 7-9:** Risks to the security of stored citizen data – paper | |
|---|---|
| **Rationale:** | Given the digitalisation of paper statements of support under this option, and the associated increases in the coverage of these statements of support by many of the security mitigation measures of the online collection system, there is an overall positive impact on **R7-9**. The impact remains very high but the likelihood reduces from low (for R7 and R9) to very low (now for all three). |

| **Risks 16-18:** Risks to the security of citizen data in transit – paper | |
|---|---|
| **Rationale:** | Given the digitalisation of paper statements of support under this option, and the associated increases in the coverage of these statements of support by many of the security mitigation measures of the online collection system, there is an overall positive impact on **R16-18**. The impact remains very high but the likelihood reduces from low to very low, due to the use of a secure file transfer mechanism. |

| **Risk 5:** Fraudulent activities to undermine an ECI | |
|---|---|
| **Rationale:** | **Applicable only to Option 3.2:**<br><br>Option 3.2 would provide ECI organisers with a significant opportunity to undermine an ECI through the addition of obviously fraudulent statements of support (i.e. without paper equivalents) to the online collection system, thereby increasing the likelihood of **Risk 5** being realised from very low to low; the impact, however, remains low. |

<u>Option 3 – Changes to the Annex III or the Regulation</u>

The Regulation would need to be modified to allow the upload of paper statements of support into the online collection system. If the system, as well as the transfer of statements of support, are to be under the responsibility of the Commission, this would also require a change in the Regulation.

Option 3 – Conclusion

Overall, particularly in relation to option 3.2, a trade-off exists regarding the policy options surrounding paper collection of statements of support between shifting the current risk of data loss from organisers to competent national authorities and the resulting increase in the risk of fraudulent activities by organisers to increase support for or to undermine an ECI.

Options 3.1 and 3.2 significantly reduce the substantial risk of data loss in transit by moving to uploading these paper statements of support. Similarly, these options substantially reduce the burden on Member States' competent national authorities in the verification of paper statements of support, especially given the significant number of Member States who physically verify every single paper statement of support. Undertaking option 3.1 would enable the use of image recognition software to complete verification, whilst option 3.2 would enable both paper and online statements of support to be collectively verified through the same electronic files.

Given the substantial risk to organisers in terms of data loss in transit and storage of the current paper statements of support verification system, any reduction in this liability for organisers represents a substantial improvement. As supported by extensive interviews with relevant stakeholders, the high liability of organisers has played a significant role in reducing the number of ECI's registered each year, and, as such, reducing the risks of data loss in transit will likely have an impact on organisers' decision to undertake an ECI and to collect paper based statements of support. Thereby limiting the exclusion of citizens without access to the internet or that are not computer literate.

The added value of Option 3 would be the reduction of the data protection risk associated with paper statements of support for organisers and national authorities, both in the storage and transit, and the reduction in the burden of verification through the elimination of paper statements of support.

## VI.4. Other options applicable to online collection only

The set of options presented here relate only to online collection and represent very different approaches to the processes for the collection and verification of online statements of support. They can be summarised as follows:

- **Option 4** describes possibilities for: i) two-step data collection systems where signatories initially submit minimal personal data before submitting further personal data at a later date (option 4.1); and ii) two-step systems whereby signatories register with an entity (e.g. the Commission), which allows them to support ECIs at later dates with just one-click (option 4.2).
- **Option 5** describes possible implementations of the ECI that make use of eID or available e-government portals.

### VI.4.1. Option 4: Two step systems

We propose an option of two step-systems, where supporters would first be asked to submit limited data at the initial point of support. Additional data would then be requested electronically (either by e-mail or using an online form at a later stage to provide a level of robustness to the verification of the statements of support). The point at which the second batch of data is requested can vary depending on the sub-options presented below.

They include:

- Option 4.1 – Two-step data collection (limited and harmonised data collected at the point of support, with additional data collected at a later stage). The initial data collected might not be enough to undertake the verification. This option contains different sub-options relating to (i) the moment at which the additional data is collected

(i.e. immediately after support is expressed or only once a sufficient number of statements of support have been collected), and (ii) the scope of the collection of the second batch of data to be collected (for all statements of support or only a sample). These two variables produce three sets of options[51]:

  - Option 4.1.1 – Two step data collection with the second batch of data collected immediately after support is expressed for all statements of support;
  - Option 4.1.2 - Two step data collection with the second batch of data collected once over a million statements of support have been collected for all statements of support;
  - Option 4.1.3 - Two step data collection with the second batch of data collected once over a million statements of support have been collected for a sample of statements of support.

- Option 4.2 – another form of "two-step" data collection, but where the initial batch of data provided in the context of an ECI is kept by the Commission or a private platform for their possible re-use in the context of other initiatives that the signatory would also like to support. This option can be divided between:
  - Option 4.2.1 – The Commission could offer the possibility, to "register" ECI supporters in a system. When individuals complete a statement of support for the first time, they could be presented with an option whereby the Commission would keep these data in case they would like to support other ECIs in the future. In such cases, the supporter would only need to provide a login and/or a password in order to support subsequent initiatives. The supporter is also offered the possibility to update his/her personal data if needed or to remove his/her registration in the system. The verification of such provided data could take place each time they support an ECI.
  - Option 4.2.2 – The option would be the same but offered by a private platform (e.g. e-petitioning platforms). In that case, they could even offer the registration in the platform to the citizens before they support any initiative.

Data to be collected and impact on potential signatories:

Options under 4.1: Under these options, the data to be collected would be the ones under the current Regulation (such an approach would not be needed if the data described in Option 1 are applied given data are so limited). From the point of view of the supporters, the data to be provided would be minimised at the point of support. They would then need to provide additional data in all cases under 4.1.1, if the initiative reaches the required number of signatories under 4.1.2 but only a sample of them in option 4.1.3.

Reduced initial data requirements are likely to improve initial participation experience in comparison to current ECI process. In addition to the reduced initial data requirements, option 4.1.3 has additional benefits due to the fact that only a sample of signatories are asked to provide further data. On the other hand, there are risks that the signatories will not provide the additional data in the second step. This could impact the organisers' campaign, especially if the signatories are asked to provide the additional data only after the required number of statements of support is reached (options 4.1.2 and 4.1.3) and organisers do not have the possibility to collect more statements of support to compensate.

These options contribute to the objective of simplification of the data requirements in the first step but over the course of the data collection period, this is unlikely to have a large impact as those unwilling to share data from the second batch of data would still be reluctant to do so.

[51] The option where the second batch of data is collected immediately after support is expressed for a sample of statements of support is discarded given the difficulty in developing a robust sampling strategy covering all Member States.

Options under 4.2: Those options could be applied with any sets of data. The one-time input of personal data improves experience for the signatories.

For the options under 4.1, organisers would have **increased responsibilities to ensure the email system they use to send out requests for follow-up data, and to receive those follow-up data, was secure**. In particular, they would have to take reasonable (but state of the art) measures to ensure that such systems would not be used by 'botnets' to support large numbers of fraudulent statements of support. Under options 4.1.2 and 4.1.3 they would have to store the additional data for a shorter period and in the case of 4.1.3, only for a sample of signatories.

For the options under 4.2, either the Commission (4.2.1) or the private platform provider (4.2.2) will need to secure the collection and storage of data and their transfer to the competent national authorities. The storage can take place over a long period of time (until the de-registration of the supporter) even if the citizens' data are rarely used to support initiatives. This entails increased risks and costs. The private platform provider (or the Commission under 4.2.1) should apply security measures comparable to the ones currently applicable to the online collection systems. Otherwise, there might be a potential higher negative impact related to the potentially less stringent data protection and data security requirements of some online platforms.

Option 4 – Ways in which the option addresses the policy objectives

| Policy Objective | Option 4.1 | Option 4.2 |
|---|---|---|
| **To simplify the data requirements for signatories** | Not relevant - dealt with under Option 1 | |
| **To ensure all eligible EU citizens are able to support and ECI** | Not relevant - dealt with under Option 1 | |
| **To ensure only eligible citizens are allowed to support an ECI with a minimal burden of verification** | No direct impact, as the verification would essentially remain the same, with the exception of option 4.1.3, which would limit the number of statements of support to be verified by national authorities. | |
| **To ensure that the personal data of supporters is safeguarded** | Option 4.1 would, in the first instance, positively impact the personal data of signatories, as they would not be required to provide the full set. This is most relevant for options 4.1.2 and 4.1.3. | Option 4.2 would require that organisations store the personal data of citizens on a longer term basis, thereby increasing the risk associated to those data. |

Option 4 – Impact of the options on the risk assessment

These options would affect the following risks to the ECI (as identified by the Risk Assessment presented in section III.3) as follows:

**Table 3: Impact of Options 4 on risks to the ECI, and the rationales for the determined impacts.**

| Impact of Option 4 on the key risks identified in the risk assessment | |
|---|---|
| **Risk 2:** Reduced ECI participation as citizens are required to provide too many data | |
| **Rationale:** | 4.1.1 and 4.1.2: Weighing the initially reduced data requirements against the fact |

| | |
|---|---|
| | that signatories are still required to provide significant data (as per Annex III), the likelihood of **Risk 2** being realised reduces from very high to moderate; the impact remains moderate.<br><br>4.1.3: Given that only a sample of signatories are required to provide the full set of personal data, the likelihood of **Risk 2** being realised reduces from very high to low and the impact if realised reduces from moderate to low.<br><br>Furthermore, for options 4.1.1, 4.1.2 and 4.1.3, there is an additional risk introduced that signatories will not be willing to provide the second batch of data, if and when required.<br><br>4.2: The one-time submission of statement of support data reduces the envisaged impact of **Risk 2** from very high to moderate; the impact remains moderate. |

| **Risk 3:** Reduced ECI participation as citizens are required to provide too sensitive data | |
|---|---|
| **Rationale:** | 4.1.1 and 4.1.2: Weighing the initially reduced data requirements against the fact that signatories are still required to provide significant, and in some cases sensitive, data (as per Annex III), the likelihood of **Risk 3** being realised reduces from moderate to low; the impact remains moderate.<br><br>4.1.3: Given that only a sample of signatories are required to provide the full set of personal data, the likelihood of **Risk 3** being realised reduces from moderate to low and the impact if realised reduces from moderate to low.<br><br>4.2: The one-time submission of statement of support data reduces the envisaged impact of **Risk 3** from moderate to low; the impact remains moderate. |

| **Risk 4:** Fraudulent activities to increase support for an ECI | |
|---|---|
| **Rationale:** | 4.1.3: Given that only a sample of signatories are required to provide the full set of personal data, the likelihood of success for the submission of fraudulent statements of support increases. As such, the likelihood of **Risk 4** being realised increases from low to moderate; the impact remains moderate. |

| **Risks 10-15:** Risks to the security of stored citizen data – online | |
|---|---|
| **Rationale:** | 4.1.2: Given the reduced storage of the personal data of EU citizens, the impact if **Risks 10-15** are realised reduces from very high to high; the likelihood remains low.<br><br>4.1.3: Given the reduced storage of the personal data of EU citizens, the impact if **Risks 10-15** are realised reduces from very high to high; the likelihood remains low.<br><br>4.2: The one-time submission of statement of support data results in longer storage periods, thereby increasing the likelihood of **Risks 10-15** being realised. However, it is considered that this impact is not sufficient to amend the low (**R10-12**) and very low (**R13-15**) likelihood ratings; the impact remains very high. |

| **Risks 19-21:** Risks to the security of citizen data in transit – online | |
|---|---|
| **Rationale:** | **4.1.3:** Given that only a sample of signatories are required to provide the full set of personal data, the amount of data being transferred will be significantly reduced. As such, the impact if **Risks 19-21** are realised reduces from very high to high; the likelihood remains very low. |

Option 4 – Changes to the Annex III or the Regulation

All the sub-options to Option 4 would require changes to the text of the ECI Regulation. Sub-options under Option 4.2 would entail a shift in who is liable for the protection of personal data (Art. 12) away from organisers of ECI's. These sub-options would entail similar shifts in the burden of the online collection system (Art. 6), the liability of organisers (Art. 13). Similarly,

amendments to the text surrounding verification (Art. 8) would be required in order to implement each of the sub-options.

Option 4 – Conclusion

Overall, the sub-options presented under this policy option offer two two-step methods. The first, covered by the options under 4.1, requires the initial submission of limited data (step 1) followed by the submission of the remaining data requirements at a later date (step 2). The second, covered by the options under 4.2, requires that, in an EU citizens first engagement with the relevant entity (e.g. Commission platform or private e-petitioning platform) they will provide the full set of required data (step 1). These data are then stored by the entity for use at a later data, i.e. in the support of an ECI (step 2).

Whilst options 4.1.1, 4.1.2, 4.2.1 and 4.2.2 do not represent a reduction in the total data requirements of signing a statement of support from current levels, these options present an opportunity to have the data requirements minimised at the point of signing a statement of support for signatories. The impact of these options on the participation of ECI's will vary depending on the option.

The success of the options 4.2 depends on whether the signatory is made aware of the ECI in general or just through that particular statement of support.

The impact on participation will depend on the response rate of signatories to the second step, which will require further investigation.

Options 4.2.1 and 4.2.2 present an increased risk to the data safeguards as the signatories' data would be stored indefinitely and not bound to a particular ECI. Holding this personal data carries additional costs and risks in securing this data by the Commission (option 4.2.1). However, moving towards a system in which all ECI online statements of support are collected and stored only on an EU Commission-maintained system could be helpful with regard to this issue of trust.

The added value of these options is substantially diminished if the set of data is minimised in accordance with Option 1.

### VI.4.2. Option 5: Options involving the use eIDs or e-government portals

The following options involve "pre-registration", either through an existing portal (possibly an e-government portal), or a bespoke Commission system. Unlike the situation under Option 4.2, where the aim of the pre-registration would be to store the relevant data, under these option, the pre-registration would open the possibility of also "pre-verifying" whether the "[pre]-registered" individuals fulfilled the conditions to be eligible to participate in ECIs. That would both facilitate "one-click" participation in ECIs and greatly reduce verification requirements after an ECI. This would be easiest for "[pre]registration" schemes linked to e-government websites accessed with formal eIDs, but could also be arranged for a Commission website and even for private petition websites (as is already the case in Germany in relation to *Bundestag* petitions). Different sub-options can be considered under this option:

- Option 5.1 - Online submission of a statement of support, using an existing eID. Supporters of an ECI connect with an online system, and indicate their support for the ECI using an officially recognised/state-provided eID;
- Option 5.2 - Online submission of a statement of support, using Member States' e-Government websites - Member States could offer this same possibility to their own citizens through their own e-government websites (which are usually used with an official eID).

There is considerable support for the use of eID in the ECI across several Member States. Online submission of statements of support is felt by some to be inherently more secure than signing paper forms (highlighted in Croatia), and thus likely to increase participation, especially if it

were to be made possible to submit statements of support using an eID (as noted in Cyprus, Denmark, Estonia, Finland, Germany, the Netherlands, Slovenia).

In Germany and Luxembourg, it was stressed that any eID-supported system would have to fit in with the EU eIDAS scheme. This would also meet the concern in Slovenia that such a scheme would require special security assurances.

Slovenia further develops the capabilities on offer in the Finnish system for its national participatory instrument. More specifically, for the popular initiative, statements of support are collected through the *e-uprava portal*, which requires a secure e-signature, verified by a qualified certificate.

As shown in Appendix VIII.5.1, option 5.2 would currently be possible in 20 Member States, and clearly not in five (the potential use of the remaining three for the purposes for supporting an ECI is unclear).

For a detailed description of possibilities offered by the use of eID (option 5.1), see specific study on the use of eID for the European citizens' initiative commissioned by the Commission.

Under option 5.2, visitors to an e-government website, which they have securely entered using a state-issued eID, can pre-register for ECIs, and then, as and when there is an ECI that they wish to support, submit their statement of support through a "one-click" button, from that secure website. Here, the entity in charge of that website (i.e. a public authority) will "pre-verify" that the person wishing to "pre-register" meets the condition for participation in ECIs (i.e. check that that person is an EU citizen and check the individual's age). The latter may require formal authorisation to carry out such checks (matches). The entity in charge of the e-government website carries responsibilities and liabilities for the processing of the relevant personal data under the country's general data protection law (and, in future, under the GDPR), rather than under the ECI Regulation since this "pre-registration"/ "pre-verification" process takes place outside (i.e. prior to) the submission of the statement of support (through "one-click"), but those responsibilities and liabilities already exist in any case. Option 5.2 significantly reduces the responsibilities and liabilities of organisers, the Commission and the verification authorities, since ideally all they would receive would be the eID number of the supporter; however, given that other ways of supporting an initiative will remain in place in parallel (on paper/online without eID), there might be a need to collect additional data to be able to check for duplicate statements. However, there would be no need for the usual verifications of these statement of support using eID, since any person who submitted the statement of support through the "one-click" system was already "pre-verified" as being an EU citizen of voting age.

For signatories, there is a potential increased complication due to difficulty of using eID and/or e-government portals. However, there is also an increased feeling of security as reduced data will have to be provided.

Option 5 – Technical and financial feasibility

For option 5.1, see specific study on the use of eID for the European citizens' initiative commissioned by the Commission.

Option 5.2 would require that an appropriate e-government portal exist in each Member State with the additional functionality to support an ECI using secure sign-in. In reality, as listed in Appendix VIII.5, two Member States have no existing e-government portal (Czech Republic, Greece), three could not use their existing portal to allow citizens to support an ECI (Hungary, Ireland, UK) and this situation is unclear for a further three (Luxembourg, Romania, Slovenia). As such, these Member States would bear significantly greater costs in the implementation of this option than other Member States.

Option 5 – Ways in which the option addresses the policy objectives

| Policy Objective | Option 5.1 | Option 5.2 |
|---|---|---|
| **To simplify the data requirements for** | Under Option 5.2., potential signatories would not have to provide additional data once they are securely logged in the | |

| Policy Objective | Option 5.1 | Option 5.2 |
|---|---|---|
| **signatories** | system, which contributes towards the simplification of the data requirements.<br>Under Option 5.1., only the eID number of the supporter would be collected.<br>However, under both options, if other ways of supporting an initiative are kept in parallel (on paper/online without the use of eID), there might be a need to collect additional data to be able to check for duplicates. | |
| **To ensure all eligible EU citizens are able to support and ECI** | Not relevant - dealt with under Option 1 | |
| **To ensure only eligible citizens are allowed to support an ECI with a minimal burden of verification** | The verification mechanism would include an additional guarantee against impersonation. The burden of verification could be reduced in the case no data needs to be further collected and verified by national authorities (i.e. there would only be automatic checking). | |
| **To ensure that the personal data of supporters is safeguarded** | All data to be used for verification would be stored in secure systems and no additional data would need to be collected. This contributes to ensuring that the personal data of supporters is safeguarded. | |

Option 5 – Impact of the options on the risk assessment

These options would affect the following risks to the ECI (as identified by the Risk Assessment presented in section III.3) as follows:

**Table 23: Impact of Options 5 on risks to the ECI, and the rationales for the determined impacts.**

| Impact of Option 5 on the key risks identified in the risk assessment | |
|---|---|
| **Risk 1:** Formulation of a fake ECI in order to collect and misuse personal data | |
| **Rationale:** | Given the replacement of data requirements in the current sense with eID under option 5.1 and the direct engagement with e-government portals under option 5.2, the impact if **Risk 1** is realised reduces from very high to low; the likelihood remains very low. |

| **Risk 2:** Reduced ECI participation as citizens are required to provide too many data | |
|---|---|
| **Rationale:** | Given the replacement of data requirements in the current sense with eID under option 5.1 and the direct engagement with e-government portals under option 5.2, the impact if R**isk 2** is realised reduces from moderate to low; the likelihood also reduces from very high to low. |

| **Risk 3:** Reduced ECI participation as citizens are required to provide too sensitive data | |
|---|---|
| **Rationale:** | Given the replacement of data requirements in the current sense with eID under option 5.1 and the direct engagement with e-government portals under option 5.2, the impact if **Risk 3** is realised reduces from moderate to low; the likelihood also reduces from moderate to low. |

| **Risk 4:** Fraudulent activities to increase support for an ECI | |
|---|---|
| **Rationale:** | Given the replacement of data requirements in the current sense with eID under option 5.1 and the direct engagement with e-government portals under option 5.2, the impact if **Risk 4** is realised reduces from moderate to low; the likelihood |

| | |
|---|---|
| | reduces from low to very low. |

| **Risks 10-15:** Risks to the security of stored citizen data – online | |
|---|---|
| **Rationale:** | The replacement of data requirements in the current sense with eID under option 5.1 and the direct engagement with e-government portals under option 5.2 reduces **Risks 10-12** related to storage of online statements of support as only limited data would need to be stored. The impact if Risks 10-12 are realised reduces from very high to high; the likelihood for all risks is now very low. However, if other ways of supporting an initiative are kept in parallel the risk would still exist depending on the amount of data to be stored in order to check for duplicates. |

| **Risks 19-21:** Risks to the security of citizen data in transit – online | |
|---|---|
| **Rationale:** | The replacement of data requirements in the current sense with eID under option 5.1 and the direct engagement with e-government portals under option 5.2 results in the avoidance of **Risks 19-21** (i.e. those related to the transit of online statements of support). However, if other ways of supporting an initiative are kept in parallel the risk would still exist depending on the amount of data to be stored in order to check for duplicates. |

Option 5 – Changes to the Annex III or the Regulation

The Regulation would need to be amended. As described in detail above, the necessary amendments to the ECI Regulation would focus on the impact of the sub-options on the party liable for the protection of personal data (Art. 12), the inclusion of pre-verification under Article 8 and on the resulting shift in liability for the organisers to the national authorities and to the Commission if support through those options are possible in a system provided by the Commission.

Option 5 – Conclusion

Overall, the two sub options that comprise option 5 present an interesting case in the use of eID systems for pre-signing verification. Following the analysis provided in Appendix VIII.5, the fact that an existing e-government portal that is capable of use in the ECI for the purpose of signing or verifying statements of support is not available in all Member States, lends credence to option 5.1 and the use of a dedicated portal hosted by the Commission.

Using the example of the Finnish Kansalaisaloite instrument and their use of the local online government portal to host and to sign statements of support, the use of a dedicated online platform in conjunction with other non-aligned platforms to create discussion on the initiatives topics, helps to create widespread participation across the population and especially among young citizens.

Whilst difficult to quantify, the use of existing eID that citizens have previous experience using and that hold greater levels of trust than existing online collection systems or paper-based statements of support, would positively impact the level of participation and trust in the ECI by potential signatories.

Following this, the introduction of eID and the associated reduction in the data requirements from signatories at the point of signing could significantly impact the level of participation from citizens, particularly if they are able to use an existing eID they currently use for e-government services without the need for further registration of the eID. However, it should also be noted that eID is currently not implemented across all Member States and the penetration within Member States also varies. As such, this option would not provide a sole solution at present.

# VII. Conclusions

*Chapter VII presents conclusions developed on the basis of the different analyses described above.*

The primary premise of this study is that the current ECI data requirements are impacting the progress of ECIs and that further optimisation of these requirements, and the mechanisms surrounding them is possible. It thus follows that the key study objectives include the provision of insight on the following points:

i) the **sensitivity of the ECI's data requirements**, and the related mechanisms and processes, in light of similar national or regional participatory instruments;

ii) the **scope and possible options for simplifying these data requirements**, and the related mechanisms and processes, also in light of national level systems; and

iii) the **data protection environment in which the ECI operates** presently, the foreseen environment after the GDPR enters into force, and any challenges posed in this respect.

To accurately report on these three objectives, it has been necessary to collect extensive data on the implementation of the ECI across the Member States, as well as the implementation of similar national or regional participatory instruments, undertake a risk assessment, and highlight:

- the **best practices** and **challenges** relating to the ECI data requirements, in terms of: the data required of signatories at step 4 of the ECI process (i.e. collection of statements of support); the mechanisms used to verify statements of support; issues related to the sensitivity to provide data, Contrary to what the term itself suggests, the issue does not simply relate to the question of whether certain data are, in general or in certain countries, seen as inherently 'sensitive'. Rather, the question of 'sensitivity' is closely linked to issues of data security, as perceived by potential supporters of an ECI. The extent to which they are reluctant to provide certain data, such as ID numbers or ID document details, depends on the **context** in which they are asked for these data, and the **identity of the entity to which they are disclosing the data**.
- the **types** of similar national or regional participatory instruments in existence at national level, the **best practices** employed by these instruments and the possible **applicability** of a number of these practices to the ECI, in light of the objectives to simplify the data requirements; and
- the likely **impact of the GDPR** on the processes and mechanisms used to implement the ECI.

This chapter details the study conclusions on these points before summarising the best possible **options for the future of the ECI**, which have been developed and assessed on the basis of these insights and are documented in greater detail in section VI. It should be noted that these alternative options propose changes within, as well as outside, the scope of the current ECI Regulation, which, as announced on 11 April 2017, is going to be revised.[52]

Regarding the ECI data requirements, a term which encompasses the data collected through statements of support as well as the data used to verify the same statements of support, a wide range of **challenges appear to limit the simplicity and efficiency of the ECI**.

[52] On 11th April 2017, First Vice President Frans Timmermans announced a revision of the ECI Regulation, which was followed by the publication of a Roadmap on the Revision of Regulation (EU) No 211/2011 on the citizens' initiative (Ares(2017)2537702).

Primarily, this concerns the significant **variation that exists across the national level data collection requirements for the ECI**. In fact, Annex III of the ECI Regulation details 13 different sets of statement of support data requirements; and six Member States have unique statement of support data requirements (Bulgaria, Greece, Italy, Romania, Finland and Slovenia).

Linked to this overarching issue, the ECI data requirements face criticisms of **excessive data collection**. In particular, this relates to the number and, to a lesser extent, the sensitivity of the data that signatories are required to provide, which varies in Member States. It is worth noting that, as detailed in the study's risk assessment, the risk of reduced ECI participation due to excessive data requirements should be given high priority.

Regarding the number of data points, the majority of stakeholders agree that, in many Member States, supporters of an ECI are required to provide too much data. This perception is further supported by the comparison of the ECI with similar national or regional participatory instruments, which finds that, for the most part, similar national or regional instruments require signatories to provide fewer data than the ECI. More specifically, 75% of the Member States where national or regional participatory instruments have been examined require signatories to provide fewer data for those instruments than for the ECI.

Regarding the sensitivity of data, stakeholders in most Member States (21) have no concerns over the sensitivity of the ECI data requirements. However, where concerns have been raised, they primarily relate to the collection of personal ID (document) numbers. For these concerns, and the issue of data sensitivity more generally, the key challenge is ensuring trust in the entities or individuals collecting, controlling and processing the data. To illustrate, key reasons for the concerns raised regarding the collection of personal ID (document) numbers include a lack of trust in both national authorities and 'unknown' ECI organisers.

The challenge of excessive data collection is even more pertinent when considered against the type of outcome achieved by an ECI. It is generally considered, upon the analysis of national and regional participatory instruments, that **the requirements of an instrument** imposed on supporters **should reflect the outcome achieved by that instrument** (i.e. the greater the impact, the greater the requirements). However, national and regional instruments which realise similar outcomes to the ECI have greatly reduced data requirements in comparison to many Member States for the EU's instrument. As such, the **ECIs data requirements are not considered to be proportional** to its outcome.

These challenges are further complicated by the fact that supporters can choose (in most cases) to provide the data required by their country of citizenship or the data required by their country of residence. In practice, this is not possible across all Member States and results in the exclusion of EU citizens from ECI participation.

Moving on from the collection of statements of support, certain challenges also exist in relation to the data used for verification of statements of support and the mechanisms for verification.

The primary issue in this respect is the **limited coherence between the data collected via statements of support and the data used for verification** of those same statements of support; this issue is particularly evident in light of practices employed by similar national or regional participatory instruments. To illustrate, for similar instruments, 85% of Member States verify all and only those data collected, whereas, for the ECI, this is only true for 57% (16) of Member States. Therefore, for the ECI, 12 Member States verify different (fewer or more) data to those collected. The compliance of these practices with the ECI Regulation, which says that the purpose of collecting the data is their subsequent verification by Member States' authorities, is questionable.

Other challenges related to the verification of statements of support include:

i) the absence of specific provisions in the ECI Regulation ensuring the compliance with the data protection legislation as regards **the storage and transfer of paper statements of support** from organisers to Member States' competent authorities – this is particularly pertinent in light of the focus placed on securing online statements of support;

ii) the **circuitous route online statements of support are required to take when being transferred** from the online collection systems to the competent national

authorities for verification (first from the system to the organisers and then from the organisers to the competent national authorities).;

To address the challenges identified in the ECI process, **best practices from similar national and regional participatory instruments**, many of which have been alluded to above, have been identified. These practices can be grouped as follows:

- **Minimised data requirements:** the similar national and regional instruments examined require fewer data at the collection and verification stages than the ECI;
- **Coherent data requirements:** the similar instruments identified across the Member States maintain a better connection between the data collected through statements of support and the data verified than the ECI;
- **Data requirements proportional to outcome:** the data collection and data verification requirements of many of the national and regional participatory instruments are better proportioned in light of the outcome of the instrument, when compared with the ECI.
- **Use of technology:**
    - One beneficial application of technology in this respect is to **facilitate engagement with participants**. For example, the online component of the Finnish citizens' initiative *Kansalaisaloite* is administered through a dedicated government-hosted web platform. This platform is a one-stop shop for all relevant information on participation in, and organisation of, a citizens' initiative. Furthermore, this platform is strongly linked to a complementary debating platform, run by an NGO, which allows participants to engage further with the issues tackled by a particular citizens' initiative. Similarly, in Germany, it is possible to officially state support for public-issue petitions to the Lower House of Parliament (*öffentlichen Petitionen*) through private e-petitioning fora.
    - A second beneficial application of technology, currently in use in the Slovenian popular initiative, relates to the **use of secure e-signatures** to submit support for an initiative. In this initiative, statements of support are collected through a government portal (the *e-uprava* portal). The statements of support require a secure e-signature, verified by a qualified certificate and the signatory is immediately notified if his/her statement of support has been rejected.

In contrast to the above (i.e. extensive challenges faced by the ECI and the best practices extracted from similar national and regional instruments), the following findings indicate the **ECIs positive practices and, in some cases, its advancement beyond the examples found at the national and regional level**:

- As evidenced by this study's risk assessment, the majority of the identified data protection and data security risks to the ECI process are considered to be at an **acceptable level** (10 of 21 risks);
- **Acceptance of both paper and online statements of support:** this practice has a positive impact on engagement with the ECI across the EU and is not common among national and regional participatory instruments (63% of these similar instruments only permit paper collection); and
- **Approach to verification:** the ECI process for verification is well designed in comparison to many similar national and regional instruments. For example, a number of these instruments require in-person authentication of signatures and others require very limited (i.e. no verification of the veracity of data) or even ad-hoc verification of statements of support.
- **Approach to data security:** the ECI has a comprehensive approach to the security of the online collection systems used to store statements of support, as evidenced by the extensive risk mitigation demonstrated in this study's risk assessment including the technical specifications accompanying the ECI Regulation. Furthermore, it is positive that regular risk analyses of the Commission Online Collection Software are conducted; and

- **Use of technology:** in a similar fashion to some of the national and regional instruments, technology has been used to facilitate the ECI process. In particular, the positive use of technology includes: the development of software to automate the verification of online statements of support and the conversion of paper statements of support to electronic format by scanning them, allowing for more secure transfer of statement of support data.

There have been only a few formal assessments of the ECI processes by data protection authorities. In any processing of personal data related to ECIs, the national authorities involved – the certification authorities, the verification authorities and the other public bodies involved in verification – are subject to their own national data protection laws and, in relation to the GDPR, to that instrument and any national rules implementing provisions of that instrument that allow the Member States to define the application of those rules more precisely, and to any further, special data-related restrictions imposed by the ECI Regulation. The Commission is in this regard only subject to Regulation (EC) 45/2001 and the special data-related restrictions in the ECI Regulation.

Organisers are also bound to comply with data protection legislation as regards the statements of support they collect. The situation of organisers is more complex than for the other actors involved in terms of applicable law, and because there will still be differences between the Member States, even after the GDPR comes fully into force in May 2018, this causes difficulties. It would therefore be better if any revised version of the ECI Regulation could expressly stipulate the applicable law for any processing of personal data by ECI organisers within the ECI process. The liabilities of the entities involved in ECIs – organisers, certification authorities, verification authorities and other national bodies involved in verification (such as municipal authorities) and the Commission are limited to their respective processing.

However, there is no need for an open-ended, wide, not-data-protection-related liabilities clause (such as is now contained in the ECI Regulation). If some wider (not data protection-related) liabilities are to be retained, they should be strictly circumscribed and limited to clear civil wrongs (F: *faute*; D: *unerlaubte Handlung*) with appropriate culpability.

As regards the implications of the entry into force of the GDPR, if organisers are given practical guidance on how to perform the tasks required under the GDPR, and follow that guidance, they should be in a position to fulfil their obligations under the GDPR, whereas for the other national actors involved in ECIs (certification authorities, verification authorities and other national bodies involved in verification), the GDPR does not impose any burdens over and above what they, as public authorities, are already under in relation to any processing of personal data by them.

Analysing the above conclusions in light of the study objectives, the following **four operational policy objectives** were developed to ensure proposed amendments to the ECI tackle the challenges identified while maintaining the ECI's positive practices:

1. To simplify the data requirements for signatories of statements of support (proportionally to the outcome);
2. To ensure all eligible EU citizens are able to support an ECI;
3. To ensure only eligible citizens are able to support an ECI while minimising the burden of verification;
4. To ensure that the personal data of supporters is safeguarded.

On the basis of the research undertaken for this study, a number of conclusions can be drawn from the options developed in section VI.

In terms of **data simplification and data harmonisation**, the nationality principle should be followed, ensuring each national verification authority is in charge of verifying statements of support for their own nationals, wherever they reside. While it would require two Member States (UK and Ireland) to adapt their verification mechanisms, it would be the least invasive and obstructive change to the current situation.

While the data required under option 1.1 (**name, surname, residence/address, date of birth** and **nationality**) would fulfil the simplification and harmonisation criteria, it would not

allow all Member States to adequately verify all their nationals and consequently exclude a significant number of EU citizens of supporting an ECI. Consequently, option 1.2 is considered the most viable of the two. Option 1.2 would require two sets of data, either the set of data listed under option 1.1 (**name, surname, residence/address, date of birth** and **nationality),** or a similar set which would not include the address and date of birth, but the passport or ID number instead. The UK and Ireland would have to ask for the first set of data (i.e. including the address) to nationals residing in the country, and the second set of data (including passport number) to their citizens residing abroad.

It would ensure that all EU citizens can participate in an ECI, that the data collected are minimised in all countries and that statements of support can be verified by all competent national authorities.

Other options could also be envisaged to address specific elements of the collection of statements of support.

1. With regards to options allowing the **transfer of the responsibility for the protection of personal data**, Option 2 setting up a sole central collection system for online statements of support, for which responsibility lies with the European Commission has many advantages. Significant benefits, in particular for the policy objective related to safeguarding the personal data of supporters will be achieved by the implementation of Option 2.
2. With regards to the **collection of paper statements of support**, Option 3.1 where organisers are in charge of scanning the paper form in order to upload them directly to the online collection system is preferred over option 3.2 where they would enter this information manually. Both options reduce the substantial risk of data loss in transit by moving to uploading these paper statements of support as well as the burden on Member States' competent national authorities in the verification of paper statements of support, especially given the significant number of Member States who physically verify every single paper statement of support. Option 3.1 has the added advantage of reducing inputting mistakes.
3. The **use of eIDs** would be beneficial in that it would simplify the requirements and significantly reduce the burden of verification by national authorities. However, it should also be noted that eID is currently not implemented across all Member States and the penetration within Member States also varies, making this option unsustainable as the only possibility of signing at the current time.
4. Finally, were the simplification and harmonisation of the data requirements under Option 1.2 not to be achievable at the current time, a two-step system could be setup where supporters would first be asked to submit limited data at the initial point of support, and additional data would then be requested electronically at a later stage to provide a level of robustness to the verification mechanism. Alternatively, a pre-registration system could be setup. These two-step options present an opportunity to have the data requirements minimised at the point of signing a statement of support for signatories. However, the added value of these options is substantially diminished if the set of data is minimised in accordance with Option 1. It is also not clear whether supporters would be willing to provide the additional data in the second stage and whether this would not be particularly prejudicial to the success of citizens' initiatives.

Overall, data simplification and harmonisation would be the most immediate and important goals. In the current situation, these would be achieved by the introduction of Option 1.2. It is possible to imagine a situation where ECIs are supported by EU citizens through the use of eIDs as this would mitigate or cancel a number of risks identified in the risk assessment as well as simplify the process for supporters and national authorities. This will only be possible once all Member States adopt eIDs which is certainly not the case currently.

# VIII. Appendices

## VIII.1. Stakeholders consulted

| Member State | Stakeholder type | Name | Organisation | Role |
|---|---|---|---|---|
| | Civil Society Organisation | Elisa Lironi | European Citizens Action Service | Digital Democracy manager |
| | Civil Society Organisation | Carsten Berg | The ECI Campaign | Director |
| | ECI Organiser | Trevor Glyn Hughes | European Free Movement Instrument | Organiser |
| | ECI Organiser | Pablo Sánchez Centellas | Water and sanitation are a human right! Water is a public good, not a commodity! | Organiser |
| | ECI Organiser | Paul Lambertus Smits | More than education – Shaping active and responsible citizens | Organiser |
| | ECI Organiser | Tiziano Cattaneo | People4Soil: sign the citizens' initiative to save the soils of Europe! | Organiser |
| | National authority | Laura Gruenig | Political Rights Section, Swiss Federal Chancellery | |
| **AT** | Civil Society Organisation | Mag. Georg Markus Kainz | Quintessenz – association for the restoration of civil rights in the information age | President |
| **AT** | National authority | Robert Stein | Ministry of the Interio | Head of Department |
| **BE** | National authority | Isabelle Delhez | Government (Ministry of Internal Affairs) | Assistant |
| **BE** | Civil Society Organisation | Joris Van Hoboken | Institute for Information Law | Senior Researcher |
| **CY** | National authorities | Demetris DEMETRIOU | Ministry of Interior | Head of the Elections Service |
| **CY** | National authorities | George PAPACHARALAMBOUS | Ministry of Interior | IT Officer at the Elections Service |
| **CZ** | National authorities | Mgr. Eva Dianišková | Ministry of the Interior | |
| **CZ** | National authorities | JUDr. Helena Sluková | Ministry of the Interior | |
| **CZ** | National authorities | Eva Dianišková | Ministry of the Interior | |
| **DE** | National Authority | Sabine Eckart | Federal Ministry of Interior | National coordinator |
| **DE** | National Authority | Axel Minrath | Federal Administrative Agency | |
| **DE** | National Authority | Michael Krämer | Federal Agency for ICT-Safety | |
| **DE** | National Authority | Michael Weiß | Parliament of the State of Bremen | |
| **DE** | National Authority | Maik Martin | Interior ministry of Berlin | |
| **DE** | National Authority | Axel Minrath | Bundesverwaltungsamt | |
| **DK** | Civil Society Organisation | Jesper Lund | IT-Political Association of Denmark | Member of EDRi |
| **DK** | National Authority | Jeppe Vestentoft | The Danish Digitisation Agency | |

| Member State | Stakeholder type | Name | Organisation | Role |
|---|---|---|---|---|
| **DK** | National Authority | Anna Nystup | The Danish Ministry for Economic and the Interior | IT and CPR |
| **DK** | Civil Society Organisation | Rikke Frank Jørgensen | Danish Human Rights Association | Researcher |
| **DK** | National Authority | Anna Nystrup | Ministry for Economic Affairs and the Interior | Head of Section, Electoral Dvivion |
| **DK** | National Authority | Katrine McGrath | Ministry for Economic Affairs and the Interior | |
| **EE** | National Authority | Terje Maurer | Ministry of Interior | Head of department on Population Register actions |
| **EE** | National Authority | Mariko Jõeorg-Jurtšenko | Ministry of Justice | Advisor to public law department |
| **EE** | Civil Society Organisation | Siim Tuisk | Eesti Mittetulundusühingute ja Sihtasutuste Liit | Political advisor |
| **EE** | National Authority | Terje Maurer | Ministry of the Interior | Deputy Head of Department for Documentation Population Operations Department |
| **EL** | National Authority | Ioannis Paraskevas | Ministry of Interior Department of E-government | Technical Expert |
| **EL** | National Authority | Athanasios Papanikolaou | Ministry of Justice :- Department of Elections Division | Head of Department |
| **EL** | National Authority | Elias Georgiou | Ministry of Justice :- Department of Elections Division | Head of Department |
| **EL** | National Authority | Eleni Koutouki | Ministry of Justice :- Department of Elections Division | |
| **EL** | National Authority | Evagelia Papadiamantopoulou | Ministry of Justice :- Department of Elections Division | |
| **EL** | National authority | Ioannis Paraskevas | Ministry of Interior | General Directorate of E-government and Elections |
| **ES** | National authority | José Luis Viedma Lozano | Electoral Census Office | General Deputy Director |
| **FI** | National authority | Sina Uotila | Ministry of Justice | |
| **FI** | National authority | Pauli Pekkanen | Population Register Centre of Finland | |
| **FR** | Civil society Organisation | Didier Lopez | La ligue de l'enseignement | In charge of European and International issues |
| **HR** | Civil Society Organisation | Dragan Zelic | GONG | Election Expert |
| **HR** | National authority | Jadranka Jurinjak | Ministry for Public Administration | Chief of sector for political system and the system of country administration |
| **HR** | National authority | Albina Rosandić | State Election Commission | Deputy Secretary of the Commission |
| **HU** | National authority | Attila PÉTERI | National Election Office (also for the National Election Commission) | Advisor to the President |
| **HU** | Civil Society Organisation | Attila MRÁZ | Hungarian Civil Liberties Union | Elections' programme director |
| **HU** | Civil Society | Miklós BARABÁS | European House | Director |

| Member State | Stakeholder type | Name | Organisation | Role |
|---|---|---|---|---|
| | Organisation | | | |
| **HU** | ECI Organiser | Katalin JAKUCS | Turn me Off! | Organiser |
| **HU** | ECI Organiser | Edit FRIVALDSZKY | Mum, Dad & Kids - European Citizens' Initiative to protect Marriage and Family | Organiser |
| **HU** | ECI Organiser | Krisztián PIFKÓ | European Free Vaping Initiative | Organiser |
| **IE** | National authority | Mr. Enda Falvey | Department of Housing, Planning, Community and Local Government | |
| **IE** | National authority | Mr. Alan Byrne | Joint Committee on Public Petitions, The Houses of the Oireachtas Service | Petitions Case Manager |
| **IT** | National authority | Ada Ferrara | Ministry of Interior | |
| **LT** | National authority | Kristina IVANAUSKAITĖ-PETTINARI | Central Electoral Commission | Head of the Training and communication unit |
| **LU** | National authority | Lionel Antunes | Luxembourg Government IT Center (CTIE) | |
| **LU** | National authority | Vera HAAS-GELEJINSKY | Luxembourg Chamber of Deputies | |
| **LU** | National authority | Pierre Trausch | State Information Technology Center | |
| **LV** | National authority | Zane Pērkone | Ministry of Justice | Lawyer |
| **LV** | National authority | Vita Sliede | Permanent Representation of the Republic of Latvia to the EU | Justice Counsellor |
| **LV** | National authority | Renāte Elza Bīlmane | Information Technologies Security Incident Response Institution Cert.lv | Lawyer |
| **LV** | National authority | Edgars Tauriņš | Information Technologies Security Incident Response Institution Cert.lv | IT Security Expert |
| **LV** | National authority | Ritvars Vulis | Central Elections Commission | Secretary of the Central Elections Comission |
| **LV** | National authority | Uldis Apsītis | Citizenship and Migration Department | Personal Data Processing Department Expert |
| **LV** | National authority | Kristine Berzina | Central Election Commission | Head of Information Department |
| **MT** | National Authority | George Saliba | Office of the Electoral Commissioner | Secretary |
| **MT** | National Authority | Michael Borg | Office of the Electoral Commissioner | |
| **NL** | National Authority | Elke Dutman | Ministry of Interior and Kingdom Relations | Senior Policy Officer, responsible for the ECI |
| **NL** | National Authority | Gerard Berg | Court of Audit | |
| **NL** | National Authority | Charles Roovers | Parliament | Registrar at Committee for Requests and |

| Member State | Stakeholder type | Name | Organisation | Role |
|---|---|---|---|---|
| | | | | Petitions of the Parliament |
| **NL** | National Authority | Anke Dutman | Ministry of the Interior and Kingdom Relations | Senior Policy Officer |
| **PL** | National Authority | Adam Rogowski | Ministry of Digital Affairs | |
| **PL** | National authority | Inga Sarnecka | Minstry of Digitzation | Legal Counsel, Department of Systems Maintenintg and Development |
| **PL** | National authority | Katarzyna Kopytowska | Minstry of Digitzation | Head of Department, Department of User Support and Data Quality of Systems Maintenance and Development |
| **PT** | Civil Society | Rui Guimarães | ANSOL | Accounting Officer |
| **PT** | National Authority | Drª Sandra Monteiro | IRN | Contact point for verification on ECI |
| **PT** | National Authority | Drª Ângela Dourado | MFA – Division on European Affairs | Contact Point |
| **PT** | National Authority | TCOR Ana Jorge | GNS | Contact Point |
| **PT** | National Authority | Drª Paula Marcelino | IRN (National initiative) | Contact Point |
| **PT** | National Authority | | Central Registry Office | |
| **RO** | National Authority | | Agency for the Digital Agenda of Romania | |
| **RO** | National Authority | Catalin Guilescu | Directorate for Persons' Records and Databases Management | Empowered Director |
| **SE** | National Authority | Maria Nordström | Swedish Election Authority | ECI Coordinator |
| **SE** | Civil Society Organisation | Per Norbäck | Demoex | Founder |
| **SE** | National Authority | Emma Sjöblom | The Election Authority | Senior Administrative Officer |
| **SI** | National Authority | Iris Jeglič<br>Alenka Colja | Ministry of Interior | Director of Directorate for Administrative Affairs, Migration and Naturalization |
| **SI** | Civil Society Organisation | Majda Marolt | SKVNS | President of SKVNS and ECI campaign organiser and collector of SoS for "Right2Water" |
| **SI** | National Authority | Mag. Andrej Tomšič | Information Commissioner | Deputy Information Commissioner |
| **SI** | National Authority | Anja Hostnik | Ministry of Public Administration | Undersecretary at the Service for transparency, integrity and the political system |
| **SI** | National Authority | Matej Loparič | Ministry of the Interior | Senior Advisor |
| **SK** | National Authority | Ing. Michaela Plavcová, | The Ministry of Interior of the Slovak Republic | |
| **SK** | National Authority | Dr. Iveta Murgašová | The Ministry of Interior of the Slovak Republic | |
| **SK** | Civil Society Organisation | Marián Orávik | Občianske združenie Priama Demokracia (Civic association Direct Democracy) | |
| **UK** | National Authority | | Democratic Engagement, Cabinet Office | |

**List of data protection authorities consulted**

| Member State | Data protection authority |
|---|---|
| **AT** | Osterreichishe Datenschutzbehorde |
| **BG** | Dima Hristova, Commission for Protetion of Personal Data |
| **CY** | Commmissioner for Personal Data Protection |
| **DE** | The Federal Commissioner for Data Protection and Freedom of Information |
| **EE** | Maarja Kirss,Advisor and Raiko Kaur, Senior inspector , Data Protection Inspectorate |
| **ES** | Agencia de Proteccion de Datos |
| **IE** | Cathal Ryan, Assistant Commissioner, Office of the Data Protection Commissioner |
| **LU** | Commission nationale pour la protection des donnees |
| **LV** | Data State Inspectorate of Latvia |
| **NL** | Autoriteit Persoonsgegevens |
| **RO** | National Supervisory Authority for Personal Data Processing |
| **SI** | Eval Kala, State Supervisor for the Protection of Personal Data |
| **SE** | The Swedish Data Protection Authority |
| **UK** | The Information Commissioner's Office |

## VIII.2. Bibliography / source/data files

### VIII.2.1. List of reviewed documents

| Title | Author | Year | Link |
|---|---|---|---|
| Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative | European Commission | 2011 | link |
| Online Collection Software Risk assessment, | European Commission | | |
| Online Collection Software technical documentation | European Commission | | |
| Answers to the second 2014 Commission Questionnaire requesting additional information from Member States | European Commission | 2014 | |
| Answers to the first 2014 Commission Questionnaire relating to the Member State's first experience of verification of statement of support | European Commission | 2014 | |
| Documentation on the Commission hosting service | European Commission | | |
| Potential and challenges of E-participation in the European Union | Elisa Lironi | 2016 | link |
| Report on the application of Regulation (EU) No 211/2011 on the citizens' initiative | European Commission | 2015 | link |
| Assessment of ICT impacts of the Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative | European Commission | 2015 | link |
| European Parliament's Study: Towards a revision of the European Citizens' Initiative? | European Parliament | 2015 | link |
| European Citizen's Initiative | Civitas | 2015 | link |
| European Parliament resolution of 28 October 2015 on the European Citizens' Initiative (2014/2257(INI)) | European Parliament | 2015 | link |
| Decision of the European Ombudsman closing her own-initiative inquiry OI/9/2013/TN concerning the European Commission | European Ombudsman | 2015 | link |
| Opinion of the European Commission in the European | European Ombudsman | 2015 | PDF |

| Title | Author | Year | Link |
|---|---|---|---|
| Ombudsman's own-initiative inquiry OI/9/2013 Into the functioning of the European citizens' initiative (ECI) procedure | | | |
| Implementation of the European Citizens' Initiative: The experience of the three years | European Parliament | 2015 | link |
| Commission Delegated Regulation (EU) 2015/1070 of 31 March 2015 amending Annexes III, V and VII of Regulation (EC) No 211/2011 of the European Parliament and of the Council on the citizens' initiative | European Commission | 2015 | link |
| The ECI Registration: Falling at the First Hurdle? Analysis of the registration requirements and the "subject matters" of the rejected ECIs | ECAS | 2014 | link |
| ECI – First lessons of implementation | European Parliament | 2014 | link |
| Communication from the Commission on the European Citizens' Initiative: 'One of us' (COM(2014) 355 final, 28.5.2014) | European Commission | 2014 | link |
| Commission Delegated Regulation (EU) No 531/2014 of 12 March 2014 amending Annex I of Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative | European Commission | 2014 | link |
| Decision on own initiative inquiry Case: OI/9/2013/TN - Increasing the effectiveness of the European Citizens' Initiative process | European Ombudsman | 2015 | link |
| Communication from the Commission on the European Citizens' Initiative: 'Water and sanitation are a human right! Water is a public good, not a commodity!' (COM(2014) 177 final, 19.3.2014) | European Commission | 2014 | link |
| Corrigendum to Commission Delegated Regulation (EU) No 887/2013 of 11 July 2013 replacing Annexes II and III to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative | European Commission | 2014 | link |
| ECI Support Centre response to the European Ombudsman own inquiry into the functioning of the European citizens' initiative (ECI) OI/9/2013/TN | European Citizen Action Service | 2014 | link |
| An ECI That Works! Learning from the first two years of the European Citizens' Initiative | The ECI Campaign | 2014 | link |
| Commission Delegated Regulation (EU) No 887/2013 of 11 July 2013 replacing Annexes II and III to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative | European Commission | 2013 | link |
| Answers to the 2012 Commission Questionnaire relating to the Member State's readiness | European Commission | 2012 | |
| Towards e-ECIs? European Participation by Online Pan-European Mobilization | Carrara ,Stephane | 2012 | link |
| A Comparative Approach to the Regulation on the European Citizens' Initiative | Cuesta-López, Víctor | 2012 | link |
| Commission Delegated Regulation (EU) No 268/2012 of 25 January 2012 amending Annex I of Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative | European Commission | 2012 | link |
| Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative | European Commission | 2011 | link |
| Answers to the 2010 Commission Questionnaire relating to the implementation of the Regulation | European Commission | 2010 | |
| The European Citizens' Initiative Handbook Your Guide to the World's First Transnational Direct Democratic Tool | GEF | 2010 | link |
| The program of the Government of the Republic of Lithuania 2017 | The Government of the Republic of Lithuania | 2017 | |

| Title | Author | Year | Link |
|---|---|---|---|
| Adults' media use and attitudes | Ofcom | 2016 | |
| Freedom on the Net 2016 – Italy | Freedom House | 2016 | |
| The report on cyber-security of Lithuania of 2016 | Cyber Security and Telecommunications Authority, The Ministry of Defense National Cyber Security Center | 2016 | |
| L'E-Government in Italia: situazione attuale, problemi e prospettive, in Bank of Italy, Questioni di Economia e Finanza | Arpaia C.M., Ferro, P., Giuzio, W., Ivaldi, G., Monacelli, D. | 2016 | |
| eGovernment Benchmark 2016 | Jornal Público | 2016 | |
| Democratic innovations in Finland - Use and effects on local and national level | Christensen, Henrik Serup. et al, Prime Ministers's Office | 2016 | |
| Volksbegehrensbericht 2017 | Mehr Demokratie e.V | 2016 | |
| Europäische Bürgerinitiative Stärken und Schwächen | Mehr Demokratie e.V | 2016 | |
| Analýza Místních Referend 2014 | Jareš, Adam, and Aneta Judová, Transparency International - Česká Republika | 2016 | |
| Europe's Digital Progress Report (EDPR) | European Commission | 2016 | |
| European Citizens' Initiative: any legal leeway for success? | Petrini, Maria Celeste | 2016 | link |
| A state of democracy: Towards Citizens Rights Protection in the EU | Dupouy, Valentin et al | 2015 | link |
| The European Citizens' Initiative - a Misnomer | Buchi, Rolf | 2015 | link |
| The European Citizens Initiative as Democratic Legitimacy Enhancing tool: Towards a Broader Conceptualization | Borońska-Hryniewiecka, Karolina | 2015 | link |
| Legitimation of European Policy: European Citizens' Initiatives | Vertongen, Daan | 2015 | link |
| Direct Democracy for the EU: A Place for Interest Groups in the European Citizens' Initiative | German Institute for International and Security Affairs | 2015 | link |
| Strengthening the Idea of "By Citizens, for Citizens" in the Context of the European Citizens' Initiative -Brief Analysis of Initiatives- | Petrescu, Oana – Măriuca | 2014 | link |
| The promises and pitfalls of the European Citizens' Initiative | Jacobs, Kristof | 2014 | link |
| An Overview of the First Two Years of the European Citizens' Initiative | Głogowski, Paweł | 2014 | link |
| Context clues for the stall of the Citizens' Initiative: lessons for opening up e-participation development practice | Susha, Iryna et al | 2014 | link |
| Power to the Citizens: What conditions for the European Public Space | Versini, Claire | 2014 | link |
| A Small-States Perspective on the European Citizens' Initiative | Maximilian, Conrad | 2013 | link |
| Explaining willingness to use the European Citizens' Initiative: Political cynicism, anti-EU attitudes and voting weight of member states, Department of International Relations and the EU | Kentmen-Cin, Cigdem | 2013 | link |
| The European Citizens' Initiative: Giving Voice to EU citizens | Karatzia, Anastasia | 2013 | link |
| The European Citizens' Initiative – Chances, Constraints and Limits | Głogowski, Paweł et al | 2013 | link |
| The European Citizens' Initiative: An early assessment of the European Union's new participatory democracy instrument | Sangsari, Marcel | 2013 | link |
| The Significance of the European Citizens' Initiative for Pan-European Participatory Democracy | International Institute for Democracy and Electoral | 2013 | link |

| Title | Author | Year | Link |
|---|---|---|---|
| | Assistance | | |
| The European Citizens' Initiative – Empowering European Citizens within the Institutional Triangle: A Political and Legal Analysis | Szeligowska, Dorota et al | 2012 | link |
| Assessing Participation and Democracy in the EU: The Case of the European Citizens' Initiative | Monaghan ,Elizabeth | 2012 | link |
| The European Citizens' Initiative New Opportunities for European Civil Actors? | Hedling, Elsa | 2012 | link |
| Civil Society and Democracy in the EU: The Paradox of the European Citizens' Initiative | Julia De Clerck-Sachsse | 2012 | link |
| The European Citizen's Initiative: A New Era for Democratic Politics in the EU | Sigalas, Emmanuel | 2012 | link |
| The European Citizens' Initiative – Participatory Democracy in the European Union | Carausan, Mihaela | 2011 | link |
| Det reformeradefolkinitiativet – Erfarenheter 2011-2013 | Jungar, Ann-Cathrine | | |
| Petitions and complaints as means of protection of rights of citizens: critical overview and evaluation of effectiveness | Galović, Romina | | |
| diritto di iniziativa dei cittadini europei ed i confermati limiti dell'iniziativa legislativa popolare in Itali | C. Boya | | |
| Problems of e-government in the Republic of Bulgaria | Peter Aleksiev, EUDO Citizenship Observatory | | |
| Study of the legal framework for citizen participation in other Member States of the Council of Europe. Analysis of the possibilities for expanding citizen participation in local governance in Bulgaria and preparation of proposals for legislative changes | Institute of Direct Democracy | | |
| Index of Civic Participation in Bulgaria | Forum Civic Participation and Bulgarian Centre for Non-Profit Law | | |

## VIII.3. Country case studies

### VIII.3.1. United Kingdom

#### Objectives

The UK online petitions website was launched in 2015 by the lower house of the UK Parliament, the House of Commons. It enables British citizens and UK residents to electronically petition the House of Commons.

Petitions that attract 10,000 signatures get a response from the government. At 100,000 signatures, a petition will be considered for a debate in Parliament.

The aim of the scheme (as recommended by the House of Commons Procedure Committee) is to facilitate better public engagement with the work of Government and Parliament.

#### Impact

There have been no less than 31,731 petitions submitted through the system since it was opened in 2015. Of these, 10,950 have closed, and 20,781 were rejected (because the scheme is suspended because of the General Election in May 2017, there are no open petitions at the time of writing). The number of signatures ranged from just over 10,000 to 4,150,262 ("We the undersigned call upon HM Government to implement a rule that if the remain or leave vote is less than 60% based a turnout less than 75% there should be another referendum." The topic was debated in the House of Commons on 5 September 2016).

There was a Government response to 479 petitions that reached the 10,000 threshold. Fifty-six petitions were debated in Parliament; 14 petitions that reached the 100,000 threshold were

nevertheless not debated in Parliament. Eight petitions are awaiting a Government response; nine are awaiting a debate in Parliament.

However, e-petitions have also been criticised as "useless":

> Directgov [the precursor to the current e-petition scheme, which was on the same lines] is rarely more than a farce – and a destructive one at that. Almost half of petition requests submitted to the site by the public are rejected before they reach publication stage. When it promises that "if you collect more than 100,000 signatures, your e-petition could be debated in the House of Commons", few realise the weight of significance behind the word "could". Many petitions exceed this threshold and lead to no debate. In reality, they are passed to the backbench where, in the absence of an MP with a reason to champion the cause, they suffer death by committee.

### Requirements

A petition can be started by any single person (British citizen or UK resident), from the government-maintained website https://www.gov.uk/petition-government. If it is supported by five more members of the public, it will be opened for signature by all British citizens and UK residents.

### Data requirements

| House of Commons petition scheme | Data required |
|---|---|
| **Personal ID / Document Number*** | No |
| **Name** | Yes |
| **Nationality** | No, but only British citizens and UK residents may sign (although this is not verified) |
| **Date of Birth** | No |
| **Place of Birth** | No |
| **Address** | Yes |
| **Name at Birth** | No |
| **Father / Mother's name** | No |
| **E-mail address** | Yes |
| **Other, please specify** | |

### Participation

| Number of petitions since the launch in 2015 | |
|---|---|
| **Submitted** | 31.731 |
| **Withdrawn** | none |
| **Closed** | 10.950 |
| **Rejected** | 20.781 |
| **In process** | none |
| | |
| **Successful:** | |

| Number of petitions since the launch in 2015 | |
|---|---|
| - **>10,000 signatures** | 479 |
| - **>100,000 signatures** | 70 |

### Verification

There is no mention on the House of Commons websites relating to the petition scheme to any verifications of individual signatures. It would appear that, because it is left to the Petition Committee to decide whether to act or not – even as concerns petitions that attract more than 10,000 or even more than 100,000 signatures – it is felt that there is no need for serious individual verification. The data are therefore only checked for duplication.

Although it is considered that steps are taken to check for bots and fraud, the mechanisms involved are not documented or publicised. Existing knowledge of how local councils run their petitioning systems may indicate the approach but it cannot be ascertained whether the national parliamentary petitions scheme uses the same or similar mechanisms. Councils, for example, will likely identify signatures from the same online foreign location and/or IP address batch – these may be subsequently discounted as suspect. Furthermore, speed of signatures submitted from the same location may also be considered.

| House of Commons petition scheme | Data verified |
|---|---|
| There is no individual data verification in the UK scheme | |
| **Personal ID / Document Number*** | No |
| **Name** | No |
| **Nationality** | No |
| **Date of Birth** | No |
| **Place of Birth** | No |
| **Address** | No |
| **Name at Birth** | No |
| **Father / Mother's name** | No |
| **E-mail** | No |
| **Other, please specify** | No |

| Case study rationale |
|---|
| The UK House of Commons online petition scheme has a similar impact profile to the ECI as it is solely an agenda-setting tool and is perceived as quite popular in terms of the number of petitions and signatories (although there are also critics). A major difference from the ECI scheme is that the data are not verified except for duplication. Also instructive for any review of the ECI scheme is the automated system to identify bots and fraud.<br>The scheme therefore provides an interesting limited data- and low verification system. |

### Best practices and applicability to the ECI

The UK online e-petitions scheme is **easy to use and very unbureaucratic**. It is explained in simple language as follows:

**How petitions work**

1. You create a petition. Only British citizens and UK residents can create or sign a petition.

2. You get 5 people to support your petition. We'll tell you how to do this when you've created your petition.
3. We check your petition, then publish it. We only reject petitions that don't meet the standards for petitions.
4. The Petitions Committee reviews all petitions we publish. They select petitions of interest to find out more about the issues raised. They have the power to press for action from government or Parliament.
5. At 10,000 signatures you get a response from the government.
6. At 100,000 signatures your petition will be considered for a debate in Parliament.

**Debates**

Petitions which reach 100,000 signatures are almost always debated. But we may decide not to put a petition forward for debate if the issue has already been debated recently or there's a debate scheduled for the near future. If that's the case, we'll tell you how you can find out more about parliamentary debates on the issue raised by your petition.

MPs might consider your petition for a debate before it reaches 100,000 signatures.

The scheme allows five members of the public to open an online petition, to which all British citizens and UK residents can add their name through a simple, easy to use interface.

Petitions with over 10,000 signatures receive a response from the Government (although this is often just a one sentence response). The H/C Petitions Committee can (but is not required to) recommend that a petition be debated in Parliament and generally considers this for petitions that receive more than 100,000 signatures. Such debates have happened 56 times.

The only data asked for in the course of signing a petition on the e-petition website are: name; nationality (although this is not verified and there is no requirement to support proof of nationality or residence); address; and email address. These data are checked for duplication only: there is no other individual verification of the data. However, the online system does have an automated system to identify bots and fraud built-in.

**The scheme can be said to constitute best practice in terms of ease of use, minimal data requirements and minimal data verification requirements, but with a built-in automated system to identify bots and fraud.**

| Bibliography |
|---|
| Legislation:<br>The UK scheme is an initiative of the lower house of Parliament, the House of Commons. It is not underpinned by legislation. |
| Articles:<br>E-Petitions often worse than useless, Guardian, 24 February 2014, available at:<br>https://www.theguardian.com/commentisfree/2014/feb/24/e-petitions-often-worse-than-useless |
| Governmental websites:<br>https://www.parliament.uk/get-involved/sign-a-petition/e-petitions/<br>https://petition.parliament.uk/help<br>https://www.parliament.uk/get-involved/sign-a-petition/e-petitions/<br>https://www.parliament.uk/business/committees/committees-a-z/commons-select/petitions-committee/news-parliament-2015/new-petitions-website/<br>https://www.parliament.uk/business/committees/committees-a-z/commons-select/petitions-committee/news-parliament-2015/petitions-2017-election--faqs/ |

### VIII.3.2. Finland

#### Objectives

The Finnish citizens' initiative, Kansalaisaloite, is the most important democratic innovation at the national level in Finland. It provides an important governmental platform,

www.kansalaisaloite.fi, which facilitates launching proposals for initiatives and collecting signatures of support online.

The citizens' initiative was launched in March 2012 with the objective of promoting free civic activity. The legal basis for the citizens' initiative is laid down in the Finnish Constitution, which provides that at least 50,000 Finnish citizens entitled to vote have the right to submit an initiative for the enactment of an Act to the Parliament. The relevant rules and provisions for the procedure on the citizens' initiative are laid down in Act on Citizens' Initiative (12/2012).

### Impact

When the collection of at least 50,000 signatures is completed, the organisers of the initiative shall submit the statements of support to the Population Register Centre, which checks their validity and verifies the number of valid statements of support. If the number of valid statements meets the minimum participation requirements, the organisers may submit the initiative to the Parliament for consideration. If the initiative has not been submitted to the Parliament within six months from the date of verification by the Population Register Centre, it lapses.

"If the initiative is in the form of a legal text, it will be treated as a bill. If it is an initiative to start drafting legislation, it will receive a full reading in a plenary session of the Parliament of Finland, which will consider whether it accepts or dismisses the citizens' initiative"[53]. The Parliament is obliged to take the citizens' initiative up for consideration, but thereafter it is at the Parliament's discretion whether the initiative will be approved or if it shall be amended in some way. If the Parliament decides to reject the initiative, a new initiative on the same subject matter may be submitted.

### Requirements

A citizens' initiative may be organised by one or several Finnish citizens who are entitled to vote. One person must be named as the representative of the initiative and one as a substitute.

The Ministry of Justice maintains and manages the online platform. The use of online platform is free of charge, accessible and safe to use. It is available in Finnish and Swedish. Statements of support may be collected via this service also for such initiatives for which the collection has already been started in other online services or on paper. A specific form, which has been certified by the Ministry of Justice before the entry into force of the Act, shall be used for the collection of statements of support in paper form.

An initiative that is instituted online and for which the statements of support are collected online always require so called strong e-identification, for example the use of online banking codes.

The Ministry of Justice checks that the initiatives submitted by citizens contain the required information and that they do not contain such material that is not suitable for publication on the Internet. Thereafter, the collection of statements of supports may be started. Statements of support for an initiative must be collected within six months.

The initiative must be for a proposal for law or a proposal to start drafting a legislative act. An initiative may also concern amending or repealing an effective Act. If the initiative is formulated as a legislative act, it shall include the actual sections of the proposed legislation. The subject matter of the initiative must fall within the legislative competences of the parliament.

### Data requirements

The personal data collected for the statement of support includes name, date of birth, current home municipality and a statement that this person is a Finnish national, eligible to vote, and that this is the only statement of support given by him/her regarding the initiative in question. If statement of support is given through strong electronic identification, the only data that can

[53] http://vrk.fi/en/finnish-citizens-initiative

be stored in the online collection is the name, date of birth and home municipality, even though that the strong electronic identification may contain also other data. Only data that is necessary for identifying a person in the Population Information System is required.

| Kansalaisaloite | Data required |
|---|---|
| **Personal ID / Document Number*** | No |
| **Name** | Yes |
| **Nationality** | No, but through a statement that the participant is a Finnish national, this information is indirectly provided. |
| **Date of Birth** | Yes |
| **Place of Birth** | No |
| **Address** | No |
| **Name at Birth** | No |
| **Father / Mother's name** | No |
| **E-mail** | No |
| **Other, please specify** | Current municipality |

### Participation

The national citizens' initiative has existed for five years now and, to date, 18 initiatives have reached the required national minimum of 50 000 signatures. More than 600 initiatives have been launched in total.

| Number of citizens' initiative Finland has verified since 2012 | |
|---|---|
| **Submitted** | 600 |
| **Withdrawn** | n.i.a. |
| **In process** | 34 |
| **Successfully verified** | 18 |
| **Rejected at verification** | n.i.a. |

Approximately one third of those eligible to vote have signed at least one initiative and some groups which may be politically more passive, like younger citizens, are actively taking part. The citizens' initiative is possible to launch without official registration.

### Verification

The purpose of verification for signatories of the Kansalaisaloiteis to ensure the signatories eligibility to support an initiative. As discussed above, only data that is necessary for identifying a person in the Population Information System is required to sign a statement of support. Thus, the requirements for the name and date of birth is the minimum data required to enable identification in the Population Information System and the request for the relevant municipality of signatories is to ensure accurate identification, in rare cases where that data is matching with

two separate persons. The inclusion of the statement confirming the Finnish nationality of signatories indirectly requests the nationality of signatories to ensure they are eligible to sign a statement of support.

| Kansalaisaloite | Data verified |
|---|---|
| **Personal ID / Document Number*** | No |
| **Name** | Yes |
| **Nationality** | No |
| **Date of Birth** | Yes |
| **Place of Birth** | No |
| **Address** | No |
| **Name at Birth** | No |
| **Father / Mother's name** | No |
| **E-mail** | No |
| **Other, please specify** | Yes, current municipality |

| Case study rationale |
|---|
| **Finland** has introduced a system of citizen's initiative very similar in style and structure to the ECI. The use of *Kansalaisaloite* is very popular, with about one third of those eligible to vote having signed at least one initiative. |
| **Relevant criteria:** Finland's Kansalaisaloite petitioning instrument is of interest given it has many similarities with the European Citizens' Initiative, particularly procedurally, and is considered very popular, garnering significant citizen engagement. |

### Best practices and applicability to the ECI

The most significant best practice that could be applied to the ECI is the link between the minimal data requirements of the Kansalaisaloite, the government platform used to host and organise initiatives and their effects on the participation of initiatives.

The minimum data requirements for supporting an initiative has encouraged signatories to support an initiative and participate in the Kansalaisaloite, as no additional documents are required. This is evidenced by the fact that approximately one third of all eligible Finnish citizens have participated in at least one initiative. The process is very much based on the national population register and its content and the relative small population of the country, which makes it possible to have very few data requirements for statements of support. Whilst it is difficult to attribute a statistically significant causal link between the minimum requirements and the high participation in initiatives, the existence of a strong correlation is highlighted by the fact that the Kansalaisaloite is very similar in procedure to the ECI.

Similarly, the government hosted online platform (www.kansalaisaloite.fi) for organising initiatives and collecting signatures has had a significant impact at the level of participation. The effect on participation is especially pronounced amongst younger citizens. In addition, and as this platform does not offer a platform for debating the content of the initiatives, an additional resource that has proved to have a substantial impact on participation is a grassroots website www.avoinministerio.fi, complementing the formal governmental platform. This website was

established subsequent to the introductions of citizens' initiative and ECI, and it allows citizens and nongovernmental organizations (NGOs) to crowdsource and discuss citizens' initiatives. The site launched with the introduction of the Citizens' Initiative in Finland, but not all features were in place before autumn 2012. Such a site is seen as playing a key role in gathering support for citizens' initiatives, in particular those that have reached the necessary 50,000 signatures.

| Bibliography |
|---|
| Legislation: |
| Personal Data Act (523/1999) |
| Act on Citizens' Initiative (12/2012) |
| Local Government Act (410/2015) |
| Criminal Code (39/1889) |
| Government Proposal 46/2011 |
| Henrik Serup Christensen, Maija Jäske, Maija Setälä and Elias Laitinen, Democratic innovations in Finland - Use and effects on local and national level, Prime Minister´s Office, December 2016. Available at http://tietokayttoon.fi/documents/10616/2009122/56_Demokraattiset+innovaatiot+Suomessa_K%C3%A4ytt%C3%B6+ja+vaikutukset+paikallisella+ja+valtakunnallisella+tasolla/e8047013-9727-47d9-b2ef-3fd18603475d?version=1.0 |
| Christensen, Henrik Serup, Karjalainen, Maija; Nurminen, Laura. 2015. Does Crowdsourcing Legislation Increase Political Legitimacy? The Case of Avoin Ministeriö in Finland. Policy and Internet, 7:1, 25–45 |
| Governmental websites: |
| Demokratia.fi |
| Kansalaisaloite.fi |
| Väestörekisterikeskus.fi |
| Finland, national Agenda (setting) initiative [PAX] – Kansalaisaloite. Direct Democracy Navigator. Available at: http://www.direct-democracy-navigator.org/legal_designs/finland-national-kansalaisaloite |
| Suomen eduskuntavaalitutkimus 2015 (FNES2015), Available at |
| http://www.vaalitutkimus.fi/fi/index.html#eduskuntavaalitutkimus-2015 |
| Citizens' initiatives in Finland. Kuntalaisaloite.fi. Available at: https://www.kansalaisaloite.fi/fi/ohjeet/briefly-in-english |
| Citizens' initiative. Eduskunta Riksdagen. Available at: https://www.eduskunta.fi/EN/lakiensaataminen/kansalaisaloite/Pages/default.aspx |
| Kaufmann, B. From Finland and Switzerland with love. Available at: http://www.swissinfo.ch/eng/directdemocracy/from-finland-and-switzerland-with-love/41144772 |

### VIII.3.3. Berlin

#### Objectives

German law makes the distinction between three types of procedures for civic participation: the Volksinitiative or popular petition, Volksbegehren and Volksentscheid (Referendum).

The Volksinitiative is a procedure of civic participation that allows the citizens to introduce a legislative proposal. When the popular petition received the required number of signatures, the parliament is obliged to take this proposal into consideration. The parliament is, however, free to decide on the outcome it gives to the popular petition. If the parliament decides not to adopt the popular petition, no further steps, such as the organization of a referendum, can be taken.

The Volksbegehren is also a procedure that allows citizens to introduce a legislative proposal. Yet contrary to the popular petition, the *Volksbegehren* is only the first stage of a procedure for a referendum. As the parliament decides not to adopt the proposal of the *Volksbegehren*, a referendum will follow.

**Volksinitiative**

The Volksinitiative is an instrument of direct democracy in Berlin where a law or concern can be submitted to the local Abgeordnetenhaus or House of Representatives. The objective of the People's initiative is laid out in Act on National Initiatives, Referendums, and National Decisions (AbstG): "A Volksinitiative is aimed at addressing the House of Representatives as part of its decision-making powers with certain objects of political will formation, which concern Berlin (Article 61 para. 1 sentence 1 of the Berlin Constitution)."

Similar to the ECI, several conditions exist on the content of the popular initiative, with the requirement that the House of Representatives is responsible for this decision and is a matter concerning Berlin. Initiatives addressing the constitution or the budget of the city are prohibited. Similarly, initiatives dealing directly or indirectly with the economy, including taxation and the salaries of politicians and officials, are excluded.

The Volksinitiative is a petition mechanism, which obligates the House of Representatives of Berlin to discuss certain issues and topics. The initiative is designed to draw attention to specific problems in a simple procedure with a relatively small number of signatories (a minimum of 20,000) and to enable Berlin residents to submit proposals directly to the House of Representatives. A Volksinitiative or popular initiative can be a change of law or a particular political decision.

**Volksbegehren**

The objective of the Volksbegehren is laid out in Act on National Initiatives, Referendums, and National Decisions: "(1) Referenda may be made to enact, amend or repeal laws, provided that the State of Berlin has legislative competence. They may also be directed to take other decisions within the framework of the decision-making authority of the House of Representatives on matters of political will which concern Berlin. They are only permitted once within one election period (Article 62 (1) of the Berlin Constitution). (2) The referendum may also be referred to the premature termination of the election period of the House of Representatives (Article 62 (6) of the Berlin Constitution)."

Similarly, to the Volksinitiative, and as laid out in Article 62 (2) of the Constitution of Berlin:

- "(1) The petitions for the Landesshaltsgesetz, the employment and pensions, the tariffs, the tariffs of the public enterprises and personnel decisions are inadmissible;
- (2) People who oppose the Basic Law, other Federal Law or the Constitution of Berlin are prohibited;
- (3) Referendums on the early termination of the election period of the Chamber of Deputies shall be inadmissible if the application is submitted later than 46 months after the beginning of the election period.[54]"

[54] http://gesetze.berlin.de/jportal/?quelle=jlink&query=VAbstG+BE&psml=bsbeprod.psml&max=true&aiz=true#jlr-VAbstGBEV2P12

## Impact

### Volksinitiative

After the submission of a people's initiative and its successful verification and examination, the House of Representatives must address and vote on the proposed draft legislation within a period of four months. The legislation must be discussed by the President, or, the President of the lower chamber. Following the hearing in the relevant committees, a debate must be held in the House of Representatives after which a vote is held. The House of Representatives can vote to accept or reject the People's Initiative, but it is not legally entitled to change the content of the initiative before it is voted upon. The organisers can participate in the deliberations in the Chamber of Deputies. Once the House of Representatives have voted on the matter and adopted or rejected the proposal, the Volksinitative is considered concluded.

In contrast to several federal states in Germany, If the parliament decides not to adopt the popular petition, a Volksinitative cannot initiate a referendum and popular decision in Berlin.

### Volksbegehren

The Volksbegehren instrument enables the electorate of Berlin to contribute directly to technical questions, to decide on laws or to bring about a premature termination of the election period. However, referenda are only permissible if the state of Berlin also has the legal competence to act on the content of the referendum.

At least 20,000 valid signatures are required for the application for a Volksbegehren and at least 50,000 signatures for an intended amendment to the Berlin Constitution or the early termination of the election period. Once organisers have successfully collected the required number of signatures and after examination and verification of these signatories, the Volksbegehren must be debated in the House of Representatives.

The Volksbegehren is only the first stage in the process for a referendum. Should the House of representatives accept the proposal without any proposed amendments, no referendum needs to be held. However, should the proposal be rejected, the issue is taken to a referendum and the House of Representatives has the right to make a competing alternative legislative proposal.

If a referendum has been reached, Article 62 of the Constitution requires that a decision be taken within four months.

## Requirements

The major requirements governing the content of the Volksiniative and Volksbegehren are that the House of Representatives is responsible for this decision and that is a matter concerning Berlin. As discussed above, initiatives addressing the constitution or the budget of the city are prohibited and initiatives dealing directly or indirectly with the economy, including taxation and the salaries of politicians and officials, are excluded.

All citizens of Berlin, who are at least 16 years of age at the time of their support signature, can support a Volksinitiative by signing. In contrast, the age to support a Volksbegehren is increased to 18 years of age. Signatories must have their sole dwelling or principal domicile in Berlin. There is no requirement for signatories to have German citizenship and nationality is not requested from signatories. Signatories are required to submit their full date of birth as this allows the national authority to ensure that they have met the full age requirements and do not just require the year of birth, as this would not ensure signatories were born in the correct month of that year to be over 16 or over 18.

Regarding the requirements for a successful Volksbegehren or Volksinitiative, organisers must obtain at least 20,000 signatures of support that have been signed within 6 months of the submission to the House of Representatives.

| | Data required |
|---|---|
| **Personal ID / Document Number*** | No |
| **Name** | Yes |
| **Nationality** | No |
| **Date of Birth** | Yes |
| **Place of Birth** | No |
| **Address** | Yes |
| **Name at Birth** | No |
| **Father / Mother's name** | No |
| **E-mail** | No |
| **Other, please specify** | Date of signature |

### Participation

To date, there have been three successful Volksinitiative collecting a total of 74,337 signatures and one successful initiative that was rejected at the verification stage due to initiative not reaching the required number of signatures.

| Volksinitiative | Year of registration | Number of signatories in MS | |
|---|---|---|---|
| | | Paper | Total |
| Volksinitiative „Verfassungskonforme Alimentation | 2015 | 21,671 | 21,671 |
| Volksinitiative „Offences Schloss | 2014 | Did not reach the minimum number of statement of support | Did not reach the minimum number of statement of support |
| Volksinitiative „Schule in Freiheit II | 2013 | 29,000 | 29,000 |
| Volksinitiative „Nachtflugverbot von 22 bis 6 Uhr – Verhandlungen mit Brandenburg. Jetzt | 2013 | 23,666 | 23,666 |

### Verification

The purpose of verification for signatories of the Volksinitiative and the Volksbegehren is to ensure the signatories eligibility to support an initiative. The request for the date of birth of signatories is used by national authorities to determine if the signatory is the minimum age for participation in the population petition. Similarly, the inclusion of the address of the signatory is used to verify that the signatory meets the requirement that his/her main residence is in the

state in order to participate in the popular petition. The inclusion of the name of the signatory is used to identify the signatory in order to assess the points mentioned above.

The organisers will first submit the signatures to a central authority in Berlin, the office of the president of the state House of Representatives. This central authority checks the admissibility of the petition and it will count the number of statements of support. If the required number of signatures is reached, the statements of support will be sent to the interior minister, who will disseminate them to the relevant municipal authorities, who have access to resident's registers. The municipal authorities will check the eligibility criteria for participating to the popular petition. On the down part of the statements of support form, a confirmation form is inserted. The municipal authorities will state their verification on this confirmation form. After this verification is finished, the statements of support will be sent back to the office of the president of the state parliament.

| | **Data verified** |
|---|---|
| **Personal ID / Document Number*** | No |
| **Name** | Yes |
| **Nationality** | No |
| **Date of Birth** | Yes |
| **Place of Birth** | No |
| **Address** | Yes |
| **Name at Birth** | No |
| **Father / Mother's name** | No |
| **E-mail** | No |
| **Other, please specify** | Date of signature |

| **Case study rationale** |
|---|
| **Berlin**: The state constitution of Berlin allows citizens to make legislative proposals, through a petition. There are different levels of "impact" base on the number of successful signatories.<br>- Volksinitiative - It is necessary for such a petition to collect statements of support from 20,000 inhabitants of the state of Berlin (0.8% of the electorate). Entitled to participate in a Volksinitiative (i.e. popular petition) are all persons older than 16 years who have their main residence in the state of Berlin. The statement of support must be signed by completing a paper form. When a person is signing the statement of support he/she has to submit following data: name, full date of birth, address, date of signature. The statement of support will become invalid when the data on the full date of birth is unreadable or incorrect. The other data serve the identification of the signatory. In the case that these other data are unreadable or incorrect, the statement of support will become invalid, when it is impossible to identify the signatory. The verification of a statement of support is the responsibility of the district government (Bezirke). The success of a popular petition in collecting the relevant valid signatures does not initiate a direct change of law but, instead, ensures that Parliament deals with the petition in a public debate. Furthermore, the leaders of the petition have the right to be heard in the relevant parliamentary committees.<br>- Volksbegehren - which requires a larger number of signatories (around 50,000) and can lead to a popular referendum if the regional parliament does not pass the proposal as law. The data requirements are similar to those of the Volksinitiative except for |

| Case study rationale |
|---|
| the minimum age which is increased to 18 years old. |
| **Relevant criteria:** the petitioning instruments of the German Länder are relevant cases due to the relationship between the data requirements and the objective of the instruments. Although limited data are required, One of these schemes (Volksbegehren) can lead to high impact outcomes. |

### Best practices and applicability to the ECI

The most significant best practice that could be applied to the ECI is the link between proportional data requirements and impact of the instrument. As discussed above, when a Berlin resident signs a statement of support for a Volksinitiative or Volksbegehren, they are required to submit only the following data: name, date of birth, address and date of signature. This is in stark contrast to the significantly increased data that is required by several Member States to sign an ECI. In order to sign an ECI in Germany, you are required to submit the additional data on your nationality and place of birth.

The Volksinitiative holds a similar level of impact and legal effect as the ECI, with an obligation for the House of Representatives to debate the proposed legislative changes but no obligation to accept this proposal and no further actions should they reject the initiative. The reduced data requirements for participation and a similar level of impact in comparison to the ECI offer a best practice example in the link between proportional data requirements and subsequent impact of the instrument.

In contrast, the Volksbegehren goes further than the Volksinitiative, offering a binding referendum in response to a rejection of the legislative proposal. Another best practice example from the Volksbegehren is the fact that the instrument acts as the first stage of a referendum, requiring a small number of signatures to bring the proposal to the House of Representatives and an option to further pursue this proposal through a referendum should the authorities reject the legislative proposal.

Similarly, the fact that only data which is necessary for the identification and for checking the eligibility of signatories, is required to support an Volksinitiative or Volksbegehren. This can be seen as a good practice as it limits the chance for invalidated statements of support. In contrast to the verification of statements of support in the majority of Member States, verification is decentralised and undertaken by the relevant municipalities. This is nevertheless the approach followed by Germany for the ECI as well.

Given the requirement to submit statements of support only in paper format, there are concerns about an increased potential for fraud in the Berlin regional instruments. However, as reported by the competent national authorities no incidents with regard to the protection of data could be found.

| Bibliography |
|---|
| European Commission, *Europe's Digital Progress Report (EDPR)*, 2016 (available at: https://ec.europa.eu/digital-single-market/en/scoreboard/germany ) |
| BSI*, Erteilung von Bescheinigungen über die Übereinstimmung von Online-Sammelsystemen mit der Verordnung (EU) Nr. 211/2011 –Verfahrensbeschreibung* |
| Interview between an official of the German competent authority (*Bundesverwaltungsamt*) and Mr Carsten Berg of ECI Campaign, 2014 (available at: http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_ZMV/EuropaeischeBuergerinitiative/FAQ/Fragen/ebi_interview.pdf?__blob=publicationFile&v=2 ) |
| Berlin State Referendum Commissioner, *Direkte Demokratie in Berlin* (brochure), 2011. |
| Ministry of Interior North-Rhine-Westphalia*, Direkte Demokratie, Leitfaden: Volksinitiative -* |

| Bibliography |
|---|
| *Volksbegehren – Volksentscheid,* 2012. |
| Mehr Demokratie e.V., *Volksbegehrensbericht 2017*, 2016. |
| Mehr Demokratie e.V*., Europäische Bürgerinitiative Stärken und Schwächen*, 2016. |
| Mehr Demokratie e.V*., Stellungnahme zum Entwurf eines Gesetzes zur Durchführung Europäischer Bürgerinitiativen*, 2011. |
| Wikipedia: *Volkspetition* (available at: https://de.wikipedia.org/wiki/Volkspetition ). |
| Berlin, Germany, regional Popular or citizens initiative and authorities counter-proposal [PCI+] – Volksbegehren. Direct democracy navigator. Available at: http://www.direct-democracy-navigator.org/legal_designs/berlin-germany-regional-volksbegehren |

### VIII.3.4. Switzerland

## Objectives & Impact

The Swiss Federal Popular Initiative is an instrument of direct democracy in Switzerland. The instrument enables citizens to propose changes to the Swiss Federal Constitution through 100,000 citizens signing a form in support within 18 months. The federal Parliament is obliged to discuss the initiative and to decide to recommend or to reject the initiative, or to propose an alternative. Whatever the Parliament chooses, all citizens will decide in a referendum whether to accept the initiative, the alternate proposal or to reject any changes.

Citizens may launch a federal popular initiative to request a full or partial amendment to the Swiss Federal Constitution. However, a federal popular initiative cannot be launched to request the revision or the introduction of a new federal law.

An initiative can be presented in the form of a specific draft article amendment or a general proposal for an amendment, of which the specific draft article is the most commonly used. A successful initiative must collect signatures from 100,000 citizens eligible to vote, approximately 2.5% of the electorate, within the time limit.

Parliament is then responsible for determining whether the initiative respects the principles of consistency of form, unity of subject matter and the mandatory rules of international law. Should this not be the case, Parliament may declare the initiative partially or totally invalid.

It is important to highlight that "an initiative is not put to a vote immediately. After an initiative has been handed in, the government writes a report on behalf of the parliament in which the government expresses its view on the proposal. The parliament will then in turn debate the initiative and take a position."

Should Parliament declare the initiative valid, it is then put to the popular vote. As previously mentioned, The Federal Council and Parliament may propose a direct or indirect counter-proposal to the initiative.

The two types of counter-proposal are:

- "The direct counter-proposal: Parliament proposes a different constitutional article in response to an initiative. If the initiative committee does not withdraw its initiative, the counter-proposal is put to the vote at the same time as the popular initiative at issue.
- The in-direct counter proposal: In response to the initiative, Parliament does not propose an amendment to the Constitution, but an amendment to the act in question, or even a new act. An indirect counter-proposal allows the authorities to propose an alternative without directly amending the Constitution. If the initiative committee does not withdraw its initiative, the indirect counter-proposal enters into force in the event that the initiative is rejected."

There is a possibility that voters may approve both the initiative and the counter-proposal. Therefore, a deciding question determines which of the proposals will enter into force should both initiatives secure a popular majority and a majority of the States. "If, in response to the third question one proposal to amend the Constitution receives more votes from the people and the other more votes from the cantons, the proposal that comes into force is that which achieves the higher sum if the percentage of votes of the people and the percentage of votes of the cantons in the third question are added together."

The Swiss Federal Constitution defines all areas subject to federal legislation and areas not explicitly mentioned is left to the legislation of the Cantons. "Therefore, it is necessary to update the constitution from time to time to take account of changes in society and technology that demand for standardised solutions throughout the country." This is evidenced by the fact that "minor changes to the Swiss constitution are quite frequent without affecting the basic ideas nor the stability of Switzerland's Political System."

## Requirements

Anyone who is entitled to vote in Switzerland can sign an initiative, including Swiss citizens who live abroad. Swiss citizens living abroad may sign federal popular initiatives if they are at least 18 years old and are registered at the embassy of the country where they reside.

The requirements for signatories to sign a federal popular initiative are in line with the Member States that require the minimum data needed to identify signatories for ECI's, requiring citizens to provide just a name, date of birth, address and signature.

## Participation

A total of 281 initiatives were handed in by 2010, with 29% of these withdrawn at a later stage. Just four initiatives were declared invalid up to 2010, highlighting a very low rejection rate of initiatives regarding the content of the initiative.

Whilst 174 initiatives had made it to the polls by 2010, just 10% of these were approved by voters, typically against significant opposition from the Government and Parliament on the content of the initiatives. The most famous of these successful initiatives made Switzerland the first country in the world to vote to join the United Nations.

However, this must take into account the fact that a substantial portion of the initiatives withdrawn at a later stage were withdrawn by their committee's as the Parliament and Government proposed a compromise that met some of the initiatives demands.

## Verification

Verification of the signatures of citizens supporting federal popular initiatives is undertaken by the Commune authorities who have access to the relevant electoral roll. Following the decision by the Federal Chancellery on whether the signature lists conform with legal requirements, the initiative committee has 18 months to collect at least 100,000 signatures, have them validated by the communes and submit them to the Federal Chancellery.

It has been noted that verification by the Communes can take a considerable amount of time within that 18-month deadline and it is advised to finish the collection of signatures as quickly as possible and to submit the signature lists on continuous basis until the deadline.

The purpose of verification in this regard is for the Communes authorities to check whether the people who have signed are registered on the electoral roll, whether anyone has signed more than once and for the Federal Chancellery to check whether signatures fulfil the legal requirements.

Once collection of signatures has been completed and the initiative submitted, the signatures are verified by the local government office/Commune authorities and given a certificate of eligibility. The committee of the organisers of the initiative then passes the signatures on to the Swiss federal chancellery. Should 100,000 signatures have been collected by the organisers, the

initiative is declared to formally exist. Following this, the initiative goes to Parliament to be checked for validity.

| Case study rationale |
| --- |
| **Switzerland** was outlined in the Terms of Reference for this study as a case of interest; it is a country where the concept of citizens or popular initiatives emerged (in the confederation's' 1848 constitution). Popular initiatives were at the inception of some of the most high-profile and controversial decisions of recent years in Switzerland, which, for example, led to a ban on the construction of Mosque minarets and the accepted referendum, "against mass immigration". For federal popular initiatives, 'parliament is responsible for examining whether the initiative respects the principles of consistency of form, unity of subject matter and the mandatory rules of international law' (https://www.ch.ch/en/demokratie/political-rights/popular-initiative/what-is-a-federal-popular-initiative) and can declare an initiative invalid on these bases. If a popular initiative is determined to be valid by parliament, it has 18-months to collect 100,000 valid signatures (i.e. 1.9% of registered voters). If achieved, a votation on the initiative is organised. It is also possible for the Federal Assembly to present a (direct or indirect) counter-project to a popular initiative, which also forms part of the vote.<br><br>Signatories of popular initiatives must be at least 18 years old and entitled to vote in Switzerland (including Swiss citizens residing abroad); they are only required to provide their first and last names, date of birth, address and their signature. Each canton validates its signatories by checking whether signatories are registered on the electoral roll and whether they have signed the initiative more than once. The Federal Chancellery then verifies if the signatures fulfil the legal requirements. |
| **Relevant criteria:** the Swiss system of popular initiatives is of key relevance as it is an instrument of direct democracy that can have a high political impact. |

## Best practices and applicability to the ECI

The most significant best practice is the link between the high level of potential impact of the instrument of direct democracy and the high level of participation in initiatives that this has fed into.

Whilst the federal popular initiative carries a substantially higher requirement for the number of signatories respective to their relative population size than the ECI, there is a deep understanding in Switzerland of this and other direct democracy instruments role in agenda-setting due in part to its long history of local and federal initiatives.

As discussed above, the relatively low success rate of initiatives at the ballot box can be attributed to the instruments effectiveness as an agenda-setting tool by forcing the Government and Parliament to acknowledge the content raised in the initiative and offer a suitable counter-proposal that takes into account the issue raised. Similarly, the high-profile successes of the initiative, including the initiative for Switzerland to join the United Nations, have a significant impact at the national level in an area where citizens typically have minimal input.

Significantly, the extended period between the successful collection and verification of the signatures for an initiative and the popular vote on the initiative that it triggers, assists in helping to ensure no changes are made to the Constitution based on temporary electoral pressures such as the recent upswing in nationalist feeling across Europe.

The binding nature of the subsequent vote on a successful initiative and its subsequent permanent changes to the Swiss Federal Constitution offer an instrument that carries real impact but is sheltered from short term electoral pressures.

| Bibliography |
|---|
| Popular vote. Swiss Federal Chancellery. Available at: https://www.admin.ch/gov/en/start/documentation/votes.html |
| How to launch a federal popular initiative. Swiss Federal Chancellery. Available at: https://www.ch.ch/en/demokratie/political-rights/popular-initiative/how-to-launch-a-federal-popular-initiative/ |
| Initiatives populaires. Swiss Federal Chancellery. Available at: https://www.bk.admin.ch/themen/pore/vi/index.html?lang=fr |
| Ruppen, P. "Direct Democracy in Switzerland". "Direct democracy in Europe: A Comprehensive Reference Guide to the Initiative and Referendum Process in Europe. |
| Switzerland's Direct Democracy. Direct democracy. Available at: http://direct-democracy.geschichte-schweiz.ch/ |
| Rachwał, M. "Citizens' initiatives in Switzerland". DOI : 10.14746/pp.2014.19.3.3. |
| Kaufmann, B. From Finland and Switzerland with love. Available at: http://www.swissinfo.ch/eng/directdemocracy/from-finland-and-switzerland-with-love/41144772 |


### VIII.3.5. Slovenia

## Objectives & Impact

There are two participatory instruments in Slovenia similar to the ECI; both called the "popular initiative". They are recognised at local and national level as a citizens' participatory tool in public decision-making, including the possibility to suggest proposals amending the Constitution.

Slovenian citizens can propose a draft law to the National Assembly and participate in the legislative process that they originate. The proposed draft law must be supported by a minimum of 5,000 citizens/voters and it must be presented in writing to the National Assembly.

Two potential objectives and impacts exist in Slovenia regarding the popular initiatives, which offers potential organisers opportunity to decide whether they aim to propose a draft law, with significantly reduced requirements in the number of supporters of the initiative, or whether they wish to push for a full constitutional amendment, which entails far greater requirements for organisers.

Any voter, political party or citizen's association/organisation may request voters to submit an initiative for amending the constitution or the draft law.

As laid out in the Referendum and People's Initiative Act, adopted in 1994, "At least five thousand voters may submit a bill to the National Assembly. The bill must contain the elements defined by the Rules of Procedure of the National Assembly".

Similarly, "At least thirty thousand voters may make a proposal to start a procedure for amending the constitution. The proposal must state, in what and how the constitution should change, and the reasons for the change"[55].

The deadline for collecting the minimum number of required signatures of voters to support the proposal is sixty days.

[55] Referendum and People's Initiative Act, Official Gazette of the Republic of Slovenia, no. 15/1994 of 18 March 1994. Available at: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlid=199415&stevilka=561

## Requirements

Both the national level and local level instruments require the name, date of birth, address (including municipality) of the signatory, as well as a signature and date of signature, in order for citizens to support an initiative. This is in line with the Member States with the lowest data requirements for signing an ECI. However, support shall be given by citizens in person before the competent authority, i.e. administrative unit on a special form or with a secured digital signature.

| | Data required |
|---|---|
| **Personal ID / Document Number*** | No |
| **Name** | Yes |
| **Nationality** | No |
| **Date of Birth** | Yes |
| **Place of Birth** | No |
| **Address** | Yes, together with the municipality. |
| **Name at Birth** | No |
| **Father / Mother's name** | No |
| **E-mail** | No |
| **Other, please specify** | Handwritten signature and date of signature. |

The registration procedure of the national and local "popular initiative" (regulated by the same legal provisions) in Slovenia differs from the ECI in few aspects. The representative of signatories submits the initiative to the President of the National Assembly. When it comes to the necessary requirements, the initiative needs to contain fixed number of signatures (5.000 to propose a law and 30.000 to amend a Constitution) and the following supporter's data: name, address and municipality of the permanent residence, date of birth, together with the handwritten signature and the date of signature. The proposed draft law – object of the popular initiative – shall be attached to the initiative.

As concerns the collection of signatures, the President of the National Assembly determines a date – in 3 days after receiving the initiative – when the collection of signatures shall start and that it will remain open for 60 days. If these 60 days would partly or fully collide with the period between 15.7. - 31.8. or 25.12. - 2.1., the first date of the collection should be fixed for the 1st September or the 3rd January of the following year – if requested by the representative of the voters. The President informs the national authority responsible for the Voting Rights Register and the organiser of the petition of his decision. Additionally, the collection and the final deadline are publicly announced in the media.

Signatures can be collected electronically, via "e-uprava" with a secured digital signature (the person is notified if his statement of support is refused after the verification) or in person before the competent authority, i.e. administrative unit on a special form. The data registered is classified information and only a Court can access it. In addition, giving support to a "popular initiative" is widely accessible to different categories of people, e.g. an authorised person can sign a statement of support in the name of a prisoner, elderly person. Moreover, the officer of an administrative unit can visit an elderly or sick person at home in this respect.

## Participation

To date at the national level, 22 popular initiatives have been submitted, with 12 successfully verified. National authorities noted that the level of participation in national or local participatory instruments was typically dependent on the topic of the initiative and how well it had been promoted amongst citizens.

| Number of popular initiatives (national level) the country has verified since 2012 | |
|---|---|
| **Submitted** | 22 |
| **Withdrawn** | 1 |
| **In process** | / |
| **Successfully verified** | 12 |
| **Rejected at verification** | 3 |

## Verification

The competent national authorities verify the name, date of birth and address of the signatory for both the national popular initiatives and local popular initiatives. The verification process of the statements of support for the national participatory instruments submitted in paper form is slightly different from the procedure of verification of statements of Support submitted for ECI. Namely, as the statement of support for "popular initiative" is already verified by the officer of the administrative unit when collected. In comparison to the ECI, for which statement of support are collected by a private person, e.g. organiser of the ECI campaign, which also facilitates the collection of statement of support and makes the procedure less stringent.

| | Data verified |
|---|---|
| **Personal ID / Document Number*** | No |
| **Name** | Yes |
| **Nationality** | No |
| **Date of Birth** | Yes |
| **Place of Birth** | No |
| **Address** | Yes |
| **Name at Birth** | No |
| **Father / Mother's name** | No |
| **E-mail** | No |
| **Other, please specify** | X. |

The officer of the administrative unit verifies the statements of support submitted in paper at the time of the signing. The Ministry responsible for the Voting Rights Register verifies electronically signed support forms and whether the voter/supporter really exists. If the data submitted by the supporter does not match with the evidence in the Voting Rights Register, the Ministry rejects such a support form.

Competent national authorities noted that the likelihood of a large-scale fraud in Slovenia is very low. The duplication of signatories by supporters in the collection phase appears as the most serious breach envisaged, albeit it has so far occurred in very few cases.

| Case study rationale |
|---|
| **Slovenia** has participatory instruments (i.e. popular initiatives) at both the national and local level. These initiatives provide citizens with the opportunity to suggest proposals amending the Slovenian Constitution or existing laws. The number of signatories required, the eligibility criteria and the procedure are stipulated by law. Regarding the former, 5,000 signatures are required for a proposal to change a law and 30,000 are required for a proposal to amend the Constitution. The time period for collection of signatures is only 60 days. The data signatories are required to provide are: full name, date of birth, address and municipality of permanent residence, signature and date of signature. Signatures can be collected through the online portal e-uprava, where a secure e-signature, verified by a qualified certificate, is required. Alternatively, paper statements of support can be signed in person at the administrative unit. Verification of paper statements is done on the spot at the administrative unit; verification of e-signatures is done via the interconnection of the appropriate e-signature with the information required to confirm the validity of the signatory from the Voting Rights Register. |
| **Relevant criteria:** the case of Slovenia will be relevant in illustrating potential ways of pre-verification through the use of alternative systems an additional technical means (use of e-signature). |

## Best practices and applicability to the ECI

The best practice that could be applied to the ECI is the introduction of an eID for statements of support, which is currently used as a pre-verification mechanism in the Slovenia popular initiative. The use of the national e-government portal to securely register signatures of support presents an interesting case for the Member States that have existing e-government portals that use eID verification methods for citizens to access other government services. National level stakeholders consulted in Slovenia believe that the introduction of an eID would increase the public participation in the ECI. The use of existing national e-government systems offers the higher level of security against fraud that can eID can provide as well as potentially improving signatories' confidence in the security of their data and any resulting impact on participation that would incur.

| Bibliography |
|---|
| Information Commissioner website https://www.ip-rs.si/en/ |
| Act Amending the Electronic Commerce and Electronic Signature Act http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6795 |
| Constitutional decision regarding Referendum and Popular Initiative Act https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlid=200524&stevilka=842 |
| Order on the support form of a voter http://www.pisrs.si/Pis.web/pregledPredpisa?id=ODRE759 |
| Guidelines for public participation in the preparation of regulations: http://www.stopbirokraciji.si/fileadmin/user_upload/mju/Boljsi_predpisi/Vkljucevanje_javnosti/MJU-SMERNICE-FINAL_842015.pdf |

| Bibliography |
|---|
| Referendum and People's Initiative Act, Official Gazette of the Republic of Slovenia, no. 15/1994 of 18 March 1994. Available at: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlid=199415&stevilka=561 |
| Podolnjak, R. "Constitutional Reforms of Citizen-Initiated Referendum". *Revus*, 26 \| 2015, 129-149. |
| Podolnjak, R. "Citizens' Initiatives in Slovenia and Croatia: Constitutional Design, Experiences, and Perspectives". 23rd World Congress of International Political Science Association in Montreal |
| Butković, H. 'The Rise of Direct Democracy in Croatia: Balancing or Challenging Parliamentary Representation?'. CIRR XXIII (77) 2017, 39-80 |

## VIII.4. e-Government and e-Identity schemes and national registries

### VIII.4.1. eGovernment scheme

| Member State | Is there an existing e-government portal? | Could it be used by citizens to give support to an ECI? | Sources |
|---|---|---|---|
| **AT** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Austria_March_2017_v_4_00.pdf |
| **BE** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Belgium_March_2017_v3_00.pdf |
| **BG** | **Yes** | **Yes** | Country Fiche |
| **CY** | **Yes** | **Yes** | Country Fiche |
| **CZ** | **No** | **No** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Czech_Republic_March%202017_v3_00.pdf |
| **DE** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Germany%20_March_2017_v2_00.pdf |
| **DK** | **Yes** | **Yes** | Country Fiche |
| **EE** | **Yes** | **Yes** | Country Fiche |
| **EL** | **No** | **No** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Greece_March_2017_v2_00.pdf |
| **ES** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Spain_March_2017_v3_00.pdf |

| Member State | Is there an existing e-government portal? | Could it be used by citizens to give support to an ECI? | Sources |
|---|---|---|---|
| **FI** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Finland_March_2017_v1_00.pdf |
| **FR** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_France%20_March%20_2017_v6_00.pdf |
| **HR** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Croatia_March_2017_v3_00.pdf |
| **HU** | **Yes** | **No** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Hungary_March_2017_v3_00.pdf |
| **IE** | **Yes** | **No** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernemnt_in_Ireland_March_2017_v2_00.pdf |
| **IT** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Italy_March_2017_v3_0.pdf |
| **LT** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Lithuania_March_2017_v4_00.pdf |
| **LU** | **Yes** | **Not clear** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment%20in%20Luxembourg%20-%20February%202016-%2018_00_v4_00.pdf |
| **LV** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Latvia_March_2017_v1_00.pdf |
| **MT** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Malta_March_2017_v2_00.pdf |
| **NL** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Netherlands_March_2017_v2_00(1).pdf |
| **PL** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Poland_April_2017_v4_00.pdf |
| **PT** | **Yes** | **Yes** | Country Fiche |
| **RO** | **Yes** | **Not clear** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Romania_March_2017_v2_00.pdf |
| **SE** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Sweden_ |

| Member State | Is there an existing e-government portal? | Could it be used by citizens to give support to an ECI? | Sources |
|---|---|---|---|
| | | | March_2017_v2_00.pdf |
| **SI** | **Yes** | **Not clear** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Slovenia_March_2017_v3_00.pdf |
| **SK** | **Yes** | **Yes** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Slovakia_March_2017_v2_00.pdf |
| **UK** | **Yes** | **No** | https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_United_Kingdom_March_2017_v3_00.pdf |

### VIII.4.2. National registers

The table below provides a list of registers available to national authorities for verification purposes. The list differs from that of table 7 presenting only the databases used for verification of ECIs.

| Member State | Name of the register(s) available | Sources |
|---|---|---|
| **AT** | ·Zentrales Melderegister / Central Residence Register<br>·Identitätsdokumentenregister / Identity Document Register) | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **BE** | Registre national des personnes physiques / National register of natural persons | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **BG** | ·Unified System for Civil Registration and Administrative Service of the Population (ESGRAON) | ·European Parliament, Life in Cross-Border Situations in the EU - A Comparative Study on Civil Status |
| **CY** | ·Civil registry | ·Civil Registry and Migration Department |
| **CZ** | ·Fundamental Register of Inhabitants (ROB)<br>·Register of Identity Cards<br>·Register of Passports | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **DE** | · Melderegister / Residents Registers of the States<br>· Melderegister / Population Registers | ·European Parliament, Life in Cross-Border Situations in the EU - A Comparative Study on Civil Status |
| **DK** | ·Det Centrale Personregister (CPR) / Danish Civil Registry | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification.<br>·Executive Order on the Civil Registration System Act |
| **EE** | ·Rahvastikuregister / Population Register | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **EL** | ·National electoral rolls | Information concerning the registers used for verification and other national registers is confirmed by the national |

| Member State | Name of the register(s) available | Sources |
|---|---|---|
| | | authority in charge of verification. |
| **ES** | Electoral Census (or Population register) | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. National authorities provided conflicting information over the title of the register used, giving both population register and electoral census. |
| **FI** | ·Väestötietojärjestelmä / Population Information System | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **FR** | ·Repertoire National (RNIAM) d'identificaiton des personnes physiques / National Directory (RNIAM) of identifying natural persons<br>·Les listes électorales / Electoral roll | ·Institut national de la statistique (INSEE)<br>·European Parliament, Life in Cross-Border Situations in the EU - A Comparative Study on Civil Status |
| **HR** | ·Registar birača / Voters Register | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **HU** | · Lakossági nyilvántartás / Population Register<br>Útiokmány-nyilvántartás / Passport register | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **IE** | ·Local Electoral rolls | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **IT** | • · Municipal civil registries<br>• Indice Nazionale delle Anagrafi (INA) / National Register of Indices | ·European Parliament, Life in Cross-Border Situations in the EU - A Comparative Study on Civil Status |
| **LT** | ·Residents' Register of the Republic of Lithuania | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **LU** | ·Registre National des Personnes Physiques / National register of natural persons | ·Confirmed by the national authority |
| **LV** | ·Population Register | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification.<br>·European Parliament, Life in Cross-Border Situations in the EU - A Comparative Study on Civil Status |
| **MT** | . National identity database<br>·General Elections Electoral Register (made up of 13 regional registers) | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **NL** | · The Municipal Personal Records Database (BRP) | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification.<br>·European Parliament, Life in Cross-Border Situations in the EU - A Comparative Study on Civil Status |
| **PL** | ·Powszechny Elektroniczny System Ewidencji Ludności (PESEL) / Universal Electronic Registration System | ·Ministry of the Interior and Administration |

| Member State | Name of the register(s) available | Sources |
|---|---|---|
| **PT** | · National register of civil identification | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **RO** | · National Registry of Persons' Records (RNEP) | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **SE** | Folkbokföringen / Population Register | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **SI** | • · Voting Rights Register<br>• Permanent Residence Register<br>• Register of Foreigners | ·European Parliament, Life in Cross-Border Situations in the EU - A Comparative Study on Civil Status<br>·National Data Collection Systems and Practices: Country Report Slovenia, 2009. Prominstat. |
| **SK** | ·Register obyvatel'ov Slovenskej republiky / Register of Residents of the Slovak Republic | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |
| **UK** | ·Local Electoral Registers | Information concerning the registers used for verification and other national registers is confirmed by the national authority in charge of verification. |


European
Commission