070383/EU XXVII. GP
Eingelangt am 28/07/21

Council of the
European Union

Brussels, 28 July 2021
(OR. en)

11094/21

AG 73

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2021) 208 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Data protection guidance for the organisers of European citizens' initiatives

Delegations will find attached document SWD(2021) 208 final.

Encl.: SWD(2021) 208 final

www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 16.7.2021
SWD(2021) 208 final

COMMISSION STAFF WORKING DOCUMENT

Data protection guidance for the organisers of European citizens' initiatives

www.parlament.gv.at

COMMISSION STAFF WORKING DOCUMENT

Data protection guidance for the organisers of European citizens' initiatives

DISCLAIMER[1]

The present guidance is intended to contribute to a better understanding of EU data protection requirements applying to processing operations provided for under Regulation (EU) 2019/788 on the European Citizens' Initiative (ECI Regulation). Only the texts of the Regulation on the European citizens' initiative[2], the General Data Protection Regulation (GDPR)[3] and the Regulation on the protection of natural persons with regard to the processing of personal data by the EU institutions (EUDPR)[4] have legal value. This guidance cannot replace the applicable legal framework, including, where applicable, binding contracts such as joint controllership agreements.

This guidance provides practical information to organisers of citizens' initiatives and should not be seen as giving rise to any enforceable right or legitimate expectation. In particular, this guidance is without prejudice to the responsibility of the representative of the group of organisers, as data controller, pursuant to Article 5(2) of the GDPR, to comply and ensure compliance with the obligations and rules of the GDPR.

The binding interpretation of EU legislation is the exclusive competence of the Court of Justice of the European Union. The views expressed in this guidance are without prejudice to the position that the Commission might take before the Court of Justice.

As this guidance reflects the state of the art at the time of its drafting, it should be regarded as a 'living tool' open for improvement and its content may be subject to modifications without notice.

[1] This document will be published as a web document at: https://europa.eu/citizens-initiative/how-it-works/data-protection_en. It will be published without footnotes, but it will include the links and cross-references as described therein. These links may be updated in the future so that they remain up to date, without the need to update the present staff working document.
[2] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[3] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[4] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725

www.parlament.gv.at

Key principles

When collecting statements of support[5] for their initiative, organisers process signatories' personal data on a potentially large scale. The representative of the group of organisers (or the legal entity specifically created to manage the initiative, if any) is responsible for processing these personal data and is the so-called data controller.

Where the collection and/or submission of the collected statements of support is carried out through the Commission provided IT tools, notably the central online collection system[6], the European Commission steps in to alleviate the responsibility of the organisers by acting as a joint data controller for these processing operations.

In case the required number of statements of support has been collected by the group of organisers, these statements are then submitted to the competent national authorities for verification and certification[7]. The national authorities are considered to be data controllers as regards these processing operations.

Key terms

Take a look at theData **protection glossary**[8] related to data protection in the context of the European citizens' initiative.

Which are the processing operations the organisers are expected to carry out under the ECI Regulation?

- **Processing of signatories' statements of support:**

In order to support an initiative, a signatory needs to complete a statement of support form, providing a set of their personal data[9]. In case of statements of support signed online using eID, these data are imported from a national eID system.

If an initiative successfully collects the required number of statements of support, these statements are submitted to Member States for verification and certification. Personal data collected as part of statements of support cannot be used for any other purpose, such as support for initiatives other than the one for which it has been given, or transferring of the collected data to any other organisation.

- **Processing of signatories' email addresses:**

Optional collection of email addresses of those signatories who wish to be further informed on the progress of the initiative they have signed is also allowed.

[5] https://europa.eu/citizens-initiative/how-it-works_en#inline-nav-3
[6] https://europa.eu/citizens-initiative/online-collection-system_en#Commission-collection-system
[7] https://europa.eu/citizens-initiative/authorities-verification-and-certification-statements-support_en
[8] Cross-reference link to Data Protection Glossary
[9] https://europa.eu/citizens-initiative/faq_en#Giving-support

www.parlament.gv.at

Email addresses may not be collected as part of the statement of support forms, but they may be collected simultaneously, provided the signatories are informed that their right to support an initiative is not conditional on giving their consent to collecting their email address.

These email addresses can be only used to inform signatories wishing so on the progress of the initiative they have signed. They cannot be used for other purposes, such as providing signatories with commercial offers or information on a different initiative. They are not subject to Member States' verification.

- **Processing of personal data of initiative sponsors:**

Moreover, the Regulation on the European citizens' initiative provides some rules regarding the

18. Support and funding – **what should you be aware of, when processing personal data?**[10].
Articles 17, 18, 19(1) and 19(3) of the Regulation on the European citizens' initiative[11] specify how these data can be processed.

Data controllership: case scenarios for collection and submission of statements of support

There are 2 broad case scenarios:

- **Case scenario 1:**
    - **collection** of statements of support is carried out via the Commission central online collection system[12] (joint controllership between the Commission and the representative of the group of organisers)
    - **submission** of statements of support to Member States' competent authorities for verification is operated using the Commission's file exchange service[13] (joint controllership between the Commission and the representative of the group of organisers).

- **Case scenario 2:**
    - **collection** of statements of support is carried out using paper forms[14] and/or via the group of organisers' own (individual) online collection system[15] (sole controllership of the representative of the group of organisers)
    - **submission** of statements of support to Member States' competent authorities for verification is operated either by the group of organisers' own means (sole controllership of the representative of the group of organisers) OR using the Commission's file exchange service[16] (joint controllership between the Commission and the representative of the group of organisers).

Please note:

- The organisers may choose to collect statements of support on paper and online or by using only one of these collection modes
- While collecting online, the organisers need to choose between using a central online collection system or an individual one, as those two cannot be combined
- In case the organisers collect statements of support online using the central online collection system and in parallel on paper, different rules may apply to these different

[10] Cross-reference link to Question 18
[11] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[12] https://europa.eu/citizens-initiative/online-collection-system_en#Commission-collection-system
[13] https://europa.eu/citizens-initiative/how-it-works_en#inline-nav-4
[14] https://europa.eu/citizens-initiative/how-it-works_en#inline-nav-3
[15] https://europa.eu/citizens-initiative/online-collection-system_en#Own-collection-system
[16] https://europa.eu/citizens-initiative/how-it-works_en#inline-nav-4

www.parlament.gv.at

collection modes (as described in this document with regard to Case scenario 1 and Case scenario 2).

What are the rules to comply with when processing personal data?

- The Regulation on the European citizens' initiative[17] and its specific provisions on data protection (see Article 19)
- For the representative: the General Data Protection Regulation (GDPR)[18] and the relevant national provisions
- For the European Commission: the Regulation on the protection of natural persons with regard to the processing of personal data by the EU institutions (EUDPR)[19].

Contacts at national level

- The contact details of the national authorities responsible for verifying and certifying statements of support are available here[20]
- The contact details of the national data protection authorities are available here[21].

Questions and answers on data protection for signatories

See our relevant FAQ page[22]

[17] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[18] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[19] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725
[20] https://europa.eu/citizens-initiative/authorities-verification-and-certification-statements-support_en
[21] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080
[22] https://europa.eu/citizens-initiative/faq_en#Giving-support

www.parlament.gv.at

Questions and answers on data protection for the organisers[23]

1. **1. Central online collection system – what are the obligations of the Commission and the representative of the group of organisers as joint controllers?**
2.

[23] The subsequent list of Q&A will show on the web as a 'Collapsable' list, i.e. the questions will be visible but the replies will only appear if you click/hover with your mouse on a given question. The questions will not be numbered on the web.

3. **2. Individual online collection system and collection on paper forms - what are the obligations of the representative of the group of organisers as sole data controller?**
4.

5. **3. ‘Sensitive data’ - when do the signatories’ data qualify as a special category of data?**
6.

7. **4. Security – what steps should you take when collecting signatories' data on paper?**
8. **5. Security – what are the requirements when collecting signatories' data using an individual online collection system?**
9. **6. When and how should you carry out a data protection impact assessment?**
10. **7. How should you prepare a data processing record?**
11. **8. What is the role of a Protection Officer (DPO)?**
12. **9. What information should you give to citizens when collecting their data?**
13. **10. What should you do when handling data processing-related requests from signatories?**
14. **11. What should you do in case of a personal data breach?**
15. **12. What is your liability as data controller?**
16. **13. Submission of the collected statements of support to Member States for verification - who is data controller?**
17.

19. **14. Submission of the collected statements of support to Member States for verification – what are the security recommendations?**
20. **15. Submission of the collected statements of support to Member States for verification – what are the roles and responsibilities when using the Commission file exchange service?**
21. **16. What are the data retention time limits?**
22. **17. Which national supervisory authority should you contact for issues relating to the processing of personal data?**
23.

1. Central online collection system – what are the obligations of the Commission and the representative of the group of organisers as joint controllers?

Applies to Case scenario 1:[24]

As a group of organisers, you may choose to use the Commission's central online collection system for the online collection of statements of support and the submission of the collected statements of support to Member States for verification.

In such case, the representative and the European Commission act as joint data controllers, based on a standard **joint controllership agreement**. The Commission services are provided free of charge.

Under the **joint controllership agreement**, the **Commission** takes on the majority of the obligations of controllers, among which:

- It operates and maintains the relevant IT systems allowing the collection and storage of statements of support and (optionally) signatories' emails
- It may send email messages to those signatories who have subscribed to receive information on the initiative progress
- It provides 6. When and how should **you carry out a data protection impact assessment?**[25] and 7. How **should you prepare a data processing record?**[26] of the processing activities
- It ensures that the signatories are presented with the appropriate 9. What **information should you give to citizens when collecting their data?**[27] and that their questions and 10. **What should you do when handling data processing-related requests from signatories?**under GDPR/EUDPR are given a proper follow-up
- It ensures the submission[28] of the collected statements of support to Member States for verification and destroys the collected data in line with the applicable 16. What **are the data retention time limits?**periods.

With regard to the processing operations for which the Commission is responsible under the joint controllership, the 8. What is **the role of a Protection Officer (DPO)?** of the Commission monitors the implementation by the Commission of its obligations under EUDPR[29].

The representative/organisers' tasks are typically limited to the following:

- They decide the start date and the end date of the collection of statements of support, as well as the date of submission of the collected statements of support to Member State authorities
- They may send email messages to those signatories who have subscribed to receive information on the initiative progress

[24] Cross-reference link to Case scenario 1 on page 3
[25] Cross-reference link to Question 6
[26] Cross-reference link to Question 7
[27] Cross-reference link to Question 9
[28] Cross-reference link to Question 15
[29] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725

www.parlament.gv.at

- They refer to the Commission the 10. What should **you do when handling data processing-related requests from signatories?** for further handling
- They inform the Commission in case standard 16. What **are the data retention time limits?**time limits need to be adjusted in accordance with Article 19 of the Regulation on the European citizens' initiative.

The obligations of both joint controllers are further detailed in the relevant joint controllership agreements.

References:

- Articles 10, 12, 18 and 19 of the Regulation on the European citizens' initiative[30]
- Articles 24 and 26 of GDPR[31], Articles 26 and 28 of EUDPR[32]

[30] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[31] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[32] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725

2. Individual online collection system and collection on paper forms - what are the obligations of the representative of the group of organisers as sole data controller?

Applies to Case scenario 1:[33], except as regards the use of the Commission file exchange service

As a representative of the group of organisers, when acting as **sole data controller**, you must ensure that **data are processed in line with the GDPR[34], applicable national law and the Regulation on the European citizens' initiative[35]** and you must be able to demonstrate it.

Among others, you need to:

- Assess the impact of the processing operations on the data subjects' rights and freedoms, which includes the assessment on whether the data collected are sensitive prior to the processing (in case signatories' data are

[33] Cross-reference link to Case scenario 2 on page 3
[34] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[35] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788

www.parlament.gv.at

- **3. 'Sensitive data' - when do the signatories' data qualify as a special category of data?**[36], you should set up a position of 8. What is **the role of a Protection Officer (DPO)?**[37] and carry out a 6. When and how **should you carry out a data protection impact assessment?**[38])
- Establish and maintain 7. How **should you prepare a data processing record?**[39] of processing activities
- Take appropriate measures to protect personal data against unlawful forms of processing (accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, etc.); These may vary depending on whether the collection is carried out

[36] Cross-reference link to Question 3
[37] Cross-reference link to Question 8
[38] Cross-reference link to Question 6
[39] Cross-reference link to Question 7

- 4. **Security – what steps should you take when collecting signatories' data on paper?**[40] or 5. Security – **what are the requirements when collecting signatories' data using an individual online collection system?**
- 9. What information **should you give to citizens when collecting their data?**[41] about the processing of their personal data, how their protection is ensured and what rights the signatories may exercise
- Ensure the appropriate follow-up to signatories' questions and 10. **What should you do when handling data processing-related requests from signatories?**under the GDPR
- Ensure

[40] Cross-reference link to Question 4
[41] Cross-reference link to Question 9

www.parlament.gv.at

- 14. Submission of **the collected statements of support to Member States for verification – what are the security recommendations?**[42] collected statements of support to Member States for verification
- Ensure that personal data collected are not used beyond the purpose defined in the Regulation on the European citizens' initiative
- Notify any 11. What should **you do in case of a personal data breach?**[43] to the competent data protection supervisory authority in principle within 72 hours after having become aware of it and cooperate, on request, with the data protection supervisory authorities
- Ensure that all statements of support and any copies are destroyed within the applicable data retention[44] periods.

The above list is given for information purposes and does not relieve the organisers from fulfilling the obligations directly applicable to them under the GDPR[45].

References:

- Articles 5(7) and 19 of the Regulation on the European citizens' initiative[46]
- Article 24 of GDPR[47]

[42] Cross-reference link to Question 14
[43] Cross-reference link to Question 11
[44] Cross-reference link to Question 16
[45] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[46] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[47] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679

3. 'Sensitive data' - when do the signatories' data qualify as a special category of data?

Data relating to religion, political opinions, health, etc. is considered as a special category ('sensitive data') under GDPR[48] and EUDPR[49] and gets special protection. Sensitive personal data can only be processed by organisations if specific safeguards are in place.

Supporting a European citizens' initiative is a political activity and may reveal signatories' political opinions, religious or philosophical beliefs, orientations, etc.

Recital (12) of the Regulation on the European citizens' initiative[50] explains that:

'While personal data processed in application of this Regulation might include sensitive data, given the nature of the European citizens' initiative as an instrument of participatory democracy, it is justified to require the provision of personal data to support an initiative and to process such data as far as it is necessary in order to allow statements of support to be verified in accordance with national law and practice'.

Where signatories' data qualify as a special category of data ('sensitive data'), **additional measures need to be undertaken to ensure the lawful processing of such data**. Notably, it is mandatory to set up a function of a 8. What is **the role of a Protection Officer (DPO)?**[51]. Where such data are processed on a large scale it is also mandatory to carry out a 6. When and how **should you carry out a data protection impact assessment?**[52].

PLEASE NOTE:
If processing of signatories' data is carried out under joint controllership with the Commission, all Commission services are adapted to the fact that the data concerned may be sensitive. In particular, all data are stored in an encrypted form and the processing is covered by a DPIA. The DPO of the Commission monitors the implementation by the Commission of its obligations under EUDPR with regard to the processing operations for which the Commission is responsible.

References:

- Articles 5(1)(b) and 9 of GDPR[53], Article 10 of EUDPR[54]
- Recital 12 of the Regulation on the European citizens' initiative[55]

[48] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[49] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725
[50] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[51] Cross-reference link to Question 8
[52] Cross-reference link to Question 6
[53] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[54] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725
[55] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788

4. Security – what steps should you take when collecting signatories' data on paper?

Applies to Case scenario 1:[56]

When statements (and email addresses as the case may be) are collected in paper form, they are also considered as personal data protected by the GDPR[57].

Security measures

As a group of organisers, **you must implement technical and organisational security measures** to protect statements in particular against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, taking into account the risks to signatories.

They should include at least:

- Physically securing paper statement forms when stored (preferably locked in safes)
- Submitting collected paper forms to the relevant Member State validation and certification authorities in a secure way; e.g. by registered post, by trusted carrier or using the 15. Submission of the **collected statements of support to Member States for verification – what are the roles and responsibilities when using the Commission file exchange service?**[58].

PLEASE NOTE: Agreements with campaigners

As paper statements of support are normally collected in a decentralised way, the collection is often carried out by voluntary or contracted campaigners, other than the initiative organisers themselves. Such campaigners should be considered as data processors and should act based on a written agreement with the representative.

*An **agreement with a 'campaigner' is therefore a controller-processor agreement within the meaning of Article 28 GDPR and needs to cover the aspects listed in that Article.***

Indicatively, such an agreement in this context could contain:

- *Representative's authorisation for a campaigner to collect statements of support (and signatories' email addresses) for a given initiative on their behalf*
- *Representative's instructions on how to address possible data protection related questions and requests from signatories*
- *Campaigner's engagement to respect the data protection policy of the organisers and in particular:*
    - *to collect statements of support (and signatories' email addresses) only according to the instructions from the organisers, and only via the forms communicated to them by these organisers*
    - *to refrain from collecting other data*
    - *to inform signatories of the content of the initiative and on their rights according to the 9. What information* **should you give to citizens when collecting their data?**

[56] Cross-reference link to Case scenario 2 on page 3
[57] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[58] Cross-reference link to Question 15

- *to inform signatories that providing email addresses is only optional and does not condition their rights to support the initiative*
- *to store collected statements of support (and email addresses) in a safe place until their transmission to the initiative organisers*
- *to transfer the collected statements of support and email addresses in a secure way; e.g. by registered post or by courier and to the initiative organisers only*

- *Campaigner's confirmation that:*
  - *he/she has read and understood the provisions of the privacy statement defined in Annex III to the Regulation on the European citizens' initiative[59] and has familiarised himself/herself with the initiative's content, as well as with the materials the organisers use to communicate it (website, other relevant documents or information)*
  - *he/she is aware of his/her responsibility for the collected data.*

References:

- Articles 28 and 32 of GDPR[60]

[59] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[60] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679

5. Security – what are the requirements when collecting signatories' data using an individual online collection system?

Applies to Case scenario 1:[61]

As a group of organisers, you may choose to build your **own system** for the online collection of statements of support (only available for initiatives registered until end 2022).

Such systems shall have the **adequate security and technical features** to ensure throughout the collection period that:

- only natural persons are able to sign a statement of support
- the information provided on the initiative corresponds to the information published in the public register
- data are collected from signatories in accordance with Annex III to the Regulation on the European citizens' initiative[62]
- the data provided by signatories are securely collected and stored.

An **individual online collection system must be certified** by the competent authority of the relevant Member State[63] (where the data are effectively stored) **before the collection starts**.

In case you choose to build your own system, and use a **data processor**, you need to ensure that it provides sufficient guarantees to implement appropriate technical and organisational measures to ensure the protection of the rights of data subjects.

Your **relations with a data processor** must be formalised in a **written contract** covering all obligations resulting from Article 28(3) of GDPR[64].

PLEASE NOTE:
*As a group of organisers, you may choose to collect statements of support online using the European Commission's central online collection system. In this case, all security requirements are implemented by the Commission (see Case scenario 1***:**[65]*).*

References:

- Article 28 and 32 of GDPR[66]
- Article 11 of the Regulation on the European citizens' initiative[67]
- Commission Implementing Regulation (EU) 2019/1799 laying down technical specifications for European citizens' initiative individual online collection systems[68]

[61] Cross-reference link to Case scenario 2 on page 3
[62] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[63] https://europa.eu/citizens-initiative/authorities-certification-individual-online-collection-systems_en
[64] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[65] Cross-reference link to Case scenario 1 on page 4
[66] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[67] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[68] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32019R1799

www.parlament.gv.at

6. When and how should you carry out a data protection impact assessment?

Applies to Case scenario 1:[69], except for the use of the Commission's file exchange service

As representative, you need to carry out a **Data Protection Impact Assessment (DPIA)** whenever processing is likely to result in a high risk to the rights and freedoms of individuals. Among others, it is notably required in case of processing of

[69] Cross-reference link to Case scenario 2 on page 3

www.parlament.gv.at

3. 'Sensitive data' - when do the signatories' data qualify as a special category of data?
data[70] on a large scale.

The European Data Protection Board has established Guidelines on Data Protection Impact Assessment[71]. You should also check whether your 17. Which national supervisory authority **should you contact for issues relating to the processing of personal data?**[72] has issued further guidance on when and how to conduct DPIAs.

The DPIA should be conducted before the processing and should be considered as a living tool, not merely as a one-off exercise. Where there are residual risks that can't be mitigated by the measures put in place, 17. Which national supervisory authority should **you contact for issues relating to the processing of personal data?**[73] must be consulted prior to the start of the processing.

PLEASE NOTE:
*You do not need to carry out a DPIA with regard to the processing under joint controllership with the Commission, as such processing is already covered by the DPIA carried out by the Commission (see Case scenario 1***:**[74]*).*

References:

- Article 35 of GDPR[75]
- Article 36 EUDPR[76]
- Guidelines on Data Protection Impact Assessment of the European Data Protection Board[77]

[70] Cross-reference link to Question 3
[71] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[72] Cross-reference link to Question 17
[73] Cross-reference link to Question 17
[74] Cross-reference link to Case scenario 1 on page 3
[75] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[76] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725
[77] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

www.parlament.gv.at

7. How should you prepare a data processing record?

Applies to Case scenario 1:[78], except for the use of the Commission's file exchange service

Keeping of the record is legally required in particular where

[78] Cross-reference link to Case scenario 2 on page 3

www.parlament.gv.at

3. 'Sensitive data' - when do the signatories' data qualify as a special category of data?
data[79] are being processed.

A Record of processing activities is a written document, which needs to include in particular:

- the name and contact details of the data controller, as well as the data protection officer, if any
- the categories of data subjects and the categories of the processed personal data
- the purposes of the processing and the references of the initiative concerned
- the recipients of the personal data; i.e. those to whom the data have been or will be disclosed (here: only the relevant Member State authorities in charge of verification and certification of statements of support[80])
- the dates and channels of such transfers
- the envisaged time limits[81] for erasure of the data
- a general description of the technical and organisational security measures like encryption, ability to restore, testing and measures ensuring confidentiality, integrity, availability and resilience, physical security (See Questions on security in the context of the
- 4. Security – **what steps should you take when collecting signatories' data on paper?**5. Security – what are the requirements **when collecting signatories' data using an individual online collection system?**[82] and
-
- 14. Submission of the collected statements of support to Member States **for verification – what are the security recommendations?**.

PLEASE NOTE:
You do not need to produce a separate record covering processing operations carried out under joint controllership with the Commission, as those are already covered by the record of processing activities established by the Commission[83] (see Case scenario 1: and 15. Submission of the collected statements of support to Member States **for verification – what are the roles and responsibilities when using the Commission file exchange service?***[84]). You should provide a link to the Commission's record in your own documentation/website.*

References:

- Article 30 of GDPR[85]
- Article 31 EUDPR[86]

[79] Cross-reference link to Question 3
[80] https://europa.eu/citizens-initiative/authorities-verification-and-certification-statements-support_en
[81] Cross-reference link to Question 16
[82] Cross-reference link to Question 5
[83] https://ec.europa.eu/dpo-register/detail/DPR-EC-03486
[84] Cross-reference link to Question 15
[85] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[86] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725

www.parlament.gv.at

8. What is the role of a Protection Officer (DPO)?

When should you designate a Data Protection Officer?

The designation of a **Data Protection Officer (DPO)** is legally required in particular when your core activities consist of processing of
3. 'Sensitive data' - when do the signatories' data qualify as a special category of data? data[87] on a large scale.

The DPO may be a staff member of your organisation or may be contracted externally based on a service contact. A DPO can be an individual or an organisation.

What are the tasks and responsibilities of a Data Protection Officer?

The DPO assists the controller in all issues relating to the protection of personal data. The tasks and responsibilities of the DPO are explained in detail the EDPB Guidelines on Data Protection Officers[88].

If this position is established, the contact details of the DPO will be communicated at the web address of the initiative in the European citizens' initiative Register and in the 9. What **information should you give to citizens when collecting their data?**[89] handouts.

PLEASE NOTE:
For the processing operations for which the Commission is responsible under the joint controllership agreement (Case scenario 1), the DPO of the Commission monitors the implementation by the Commission of its obligations under EUDPR. Organisers may appoint a DPO in accordance with Article 37 of GDPR in relation to their responsibilities as a (joint) controller.

References:

- Articles 37-39 of GDPR[90]
- EDPB Guidelines on Data Protection Officers[91]

[87] Cross-reference link to Question 3
[88] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
[89] Cross-reference link to Question 9
[90] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[91] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

9. What information should you give to citizens when collecting their data?

Applies to Case scenario 1:[92], except for the use of the Commission's file exchange service

When a citizen (signatory) submits a statement of support (and optionally provides his/her email address), he/she **needs to be informed of how these personal data are to be processed** (for which purpose, how long, by whom, to whom they may be disclosed, how they are protected, what are his/her rights as a data subject and how he/she can exercise these rights, etc.).

The statement of support established by the Regulation on the European citizens' initiative[93] includes a standard text for a Privacy Statement. This Privacy Statement corresponds to the information, which the signatories should be given when their data are collected.

Privacy statement for the statements of support collected on paper or via individual online collection systems established by the Regulation on the European citizens' initiative:

In accordance with Regulation (EU) 2016/679 (the General Data Protection Regulation), your personal data provided on this form will only be used for the support of the initiative and made available to the competent national authorities for the purpose of verification and certification. You are entitled to request from the group of organisers of this initiative access to, rectification of, erasure and restriction of processing of your personal data.

Your data will be stored by the group of organisers for a maximum retention period of one month after the submission of the initiative to the European Commission or 21 months after the beginning of the collection period, whichever is the earlier. It might be retained beyond these time limits in the case of administrative or legal proceedings, for a maximum of one month after the date of conclusion of these proceedings.

Without prejudice to any other administrative or judicial remedy, you have the right to lodge at any time a complaint with a data protection authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement if you consider that your data is unlawfully processed.

The representative of the group of organisers of the initiative or, where appropriate, the legal entity created by it, is the controller within the meaning of the General Data Protection Regulation and can be contacted using the details provided on this form.

The contact details of the data protection officer (if any) are available at the web address of this initiative in the European Commission's register, as provided in point 4 of this form.

The contact details of the national authority which will receive and process your personal data and the contact details of the national data protection authorities can be consulted at: http://ec.europa.eu/citizens-initiative/public/data-protection.

When collecting on paper:

When statements of support are collected on paper forms, you should distribute a copy of the privacy statement or a link thereto to signatories in their native language. This privacy

[92] Cross-reference link to Case scenario 2 on page 3
[93] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788

www.parlament.gv.at

statement should be completed with your contact details as data controller, as well as the contact details of the data protection officer, if any, and of the relevant national data protection authorities.

Privacy statement for online collection

When the collection is carried out online, the privacy statement must be either published as part of the statement of support form or available via a link and the signatories need to actively tick a box confirming they have read the text before submitting statement of support.

Privacy statement for email addresses

The Regulation on the European citizens' initiative does not define a similar model for a privacy statement to be used while collecting signatories' email addresses. As representative, you need to set up such a privacy statement in compliance with the requirements of the GDPR[94].

The following minimum information should be provided to the signatory (see Article 13 GDPR[95]):

- the description and purpose of the processing
- the data processed
- the recipients of the data, if any
- the planned duration of storage
- the rights of signatories such as withdrawal of consent, right of access, rectification, erasure or objection
- instructions on the right to lodge a complaint with the authorities.

In case of collection of email addresses, the signatory needs to separately consent to the processing thereof described in the privacy statement.

PLEASE NOTE:
In case statements of support and email addresses are collected using the central online collection system, the relevant privacy statements are established by the European Commission. The texts of these privacy statements are published on the Commission ECI website[96]

References:

- Article 13 of GDPR[97]
- Annex III of the Regulation on the European citizens' initiative[98]

10. What should you do when handling data processing-related requests from signatories?

Applies to Case scenario 1:[99], except for the use of the Commission's file exchange service

[94] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[95] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[96] https://europa.eu/citizens-initiative/privacy-policy_en
[97] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[98] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[99] Cross-reference link to Case scenario 2 on page 3

As data subject, a **citizen giving support to a citizens' initiative (signatory)** is entitled to request from the representative of the group of organisers:

- access to,
- rectification of
- erasure of, and
- restriction of processing of

the personal data they process as part of **statements of support**.

As regards the **email address**, a signatory can also withdraw his/her consent to further process these personal data (request to 'unsubscribe').

What should you check after receiving such a request?

- **Whether any personal data of the signatory is being processed**, i.e. whether the applicant has submitted (either on paper or online) a statement of support for the initiative (and an email address to receive updates on the progress of the initiative, where applicable).
  For this, the representative may request the signatory to provide any information allowing them to retrieve the data (for example: Member State where data have been collected, approximate date of collection, etc.) However, irrespective of whether the data subject provides (further) information in this regard or not, the representative must make a reasonable effort in answering the request within the time limits.
- **Whether the applicant is the data subject concerned**, or a legal representative of him/her, thus a person entitled to present the request.
  For this purpose, the representative may request proof of identity or a unique identifier of the submitted statement, in case the online collection system used generates such identifiers.

How should you reply to the request?

The **actual request must be handled** after it is confirmed that the answer to both questions above is positive. Information can be provided to the data subject **in writing, electronically or even verbally**. It must be provided without delay and **at the latest within one month**.
As a rule, when requests from the relevant signatory are not manifestly unfounded or excessive (in particular repetitive requests), the information has to be provided free of charge.

PLEASE NOTE:
In case of signatories' data collected using the central online collection system under joint controllership with the Commission, signatories' requests are handled by the Commission. The obligation of the representative is limited to forwarding to the Commission of any received requests of this kind.

References:

- Chapter III Section 2 and 3 of GDPR[100]

11. What should you do in case of a personal data breach?

Applies to Case scenario 1:[101], except for the use of the Commission's file exchange service

[100] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679

www.parlament.gv.at

A **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or processed.

Notification of the data breach

In case of personal data breach, the representative of the group of organisers should **without delay and in principle no later than 72 hours** after having become aware of it **notify the personal data breach to the competent 17. Which national supervisory authority should you contact for issues relating to the processing of personal data?**[102], unless it is unlikely to result in a risk to the rights and freedoms of natural persons.

The **notification must include at least**:

- a description of the data breach, including the numbers of signatories affected and the categories of data affected
- the name and contact details of the Data Protection Officer (or other relevant point of contact)
- the likely consequences of the data breach after considering the subject matter and
- any measures taken by the controller to remedy or mitigate the breach.

Where it is not possible to provide the information at the same time, the information may be provided in phases without delay.
The representative must also document the facts, their effects and the remedial actions already taken (or to be taken urgently, providing the planning for them).

Risks to rights and freedoms

Moreover, when the breach is likely to result in a **high risk to the rights and freedoms of signatories**, they must be informed accordingly', except when:

- the implemented measures (like encryption, provided the key is not compromised) have made the data unintelligible or ensure that risks are not likely to materialise anymore, or
- individual communication to signatories would involve disproportionate efforts. In such case, a public notice of the breach, whereby the signatories are informed could be made instead.

PLEASE NOTE:
In case of data processing under joint controllership with the Commission, and unless the data breach is imputable to the conduct of the members of the group of organisers, the obligations above are fulfilled by the Commission. The group of organisers should assist, if necessary and to the extent possible, the Commission in managing personal data breaches.

References:

- Article 33 and 34 of GDPR[103]
- Commission FAQ on data protection - 'What is a data breach and what do we have to do in case of a data breach?'[104]

---

[101] Cross-reference link to Case scenario 2 on page 3
[102] https://edpb.europa.eu/about-edpb/board/members_en
[103] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679

[104] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en

12. What is your liability as data controller?

Applies to Case scenario 1:[105], except for the use of the Commission's file exchange service

As representative of the group of organisers, you may have to compensate signatories in case they suffer any **material** (i.e. direct costs) or **non-material damages** (i.e. reputation, image), caused by the processing and resulting of an **infringement of the GDPR[106].**

Examples:

- In case you disclose (acting intentionally or by negligence) that Mr Smith, employee and manager in the chemical industry, supports initiatives for prohibiting the use of pesticides produced by his employer: this may generate material damages such as losing job and **non-material damages** such as losing reputation or job opportunities
- In case you would make available the collected data to the group of organisers of another initiative or to some organisation that will use it for political analysis, profiling or lobbying: this may generate **non-material damages**.

This liability extends to a **data processor** for the damage caused by processing where this data processor has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Both yourself and the data processor shall be **exempted from liability** for the damage caused by processing, **if you can prove that you are not in any way responsible for the event giving rise to the damage**.

Without prejudice to your liability as representative, the **members of the group of organisers shall be jointly and severally liable** for any damage caused in the organisation of an initiative by unlawful acts committed intentionally or with serious negligence, under applicable national law.

In case a **legal entity** is created to manage the initiative, the liability is transferred to the legal entity, together with the function of data controller.

PLEASE NOTE:
Under Case scenario 1:[107] your liability is materially diminished as the key responsibilities with regard to the processing of signatories' data are transferred to the Commission

References:

- Article 5 of the Regulation on the European citizens' initiative[108]
- Chapter VIII of GDPR[109]

[105] Cross-reference link to Case scenario 2 on page 3
[106] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32016R0679
[107] Cross-reference link to Case scenario 1 on page 3
[108] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[109] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679

www.parlament.gv.at

13. Submission of the collected statements of support to Member States for verification - who is data controller?

Case scenario 1:[110]:
When you collect statements of support using the **Commission's central online collection system**, the submission of statements of support is operated directly by the Commission through its **file exchange service**.

The submission is covered by a relevant 1. Central online **collection system – what are the obligations of the Commission and the representative of the group of organisers as joint controllers?**[111].

Case scenario 2::
When you collect statements of support using an **individual online collection system** or **on paper** you may choose to submit them either

- **by your own means** – please check the security recommendations[112] or
- **via the Commission's file exchange service**. In this case the submission is operated under the relevant 15. Submission of **the collected statements of support to Member States for verification – what are the roles and responsibilities when using the Commission file exchange service?**[113].

[110] Cross-reference link to Case scenario 1 on page 3
[111] Cross-reference link to Question 1
[112] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32019R1799
[113] Cross-reference link to Question 15

www.parlament.gv.at

14. Submission of the collected statements of support to Member States for verification – what are the security recommendations?

Applies under Case scenario 1:[114] when submission of statements of support is done by your own means

After having collected the required number of statements of support on paper or online via your own system, you need to submit them to the competent national authorities for verification and certification.

For this, you need to split statements of support collected in paper form and those collected through your online collection system.

Under the specific rules[115] on the individual online collection systems, such systems shall provide for the encryption of personal data in electronic format for their submission to the competent authorities of the Member States.

Statements of support collected on paper may be submitted in paper form but they may also be scanned and submitted using electronic transmission or physically such as via a DVD. If **statements of support are submitted in physical form** (paper or DVD) this needs also to be done securely, e.g. sent by registered post or delivered by courier.

PLEASE NOTE:
You may choose to submit statements of support collected using an individual online collection system as well as those collected in paper 15. Submission of the collected statements **of support to Member States for verification – what are the roles and responsibilities when using the Commission file exchange service?**[116]*. In such case, a substantial part of the relevant security requirements is implemented by the Commission*

References:

- Article 4(3) of the European citizens' initiative Implementing Regulation[117]
- Articles 33 and possibly 29 of GDPR[118]

[114] Cross-reference link to Case scenario 2 on page 3
[115] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32019R1799
[116] Cross-reference link to Question 15
[117] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32019R1799
[118] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679

www.parlament.gv.at

15. Submission of the collected statements of support to Member States for verification – what are the roles and responsibilities when using the Commission file exchange service?

Applies under Case scenario 1:[119] when submission of statements of support is done via the Commission file exchange service.

You may choose to **ask the Commission to submit statements of support** to Member States for verification even if these have been collected either in paper form or online using an individual online collection system (under the sole data controllership of the representative).

What are the roles and responsibilities of the Commission?

- Makes available to the organisers the relevant IT system, pre-configured for the initiative
- Makes available to them the encryption facility
- Ensures secure and confidential submission to Member States of statements of support encrypted and uploaded by the organisers
- Deletes the files stored in the submission facility once it has ensured with the Group of Organisers and Member States, that the submission has been completed
- Transmits to the group of organisers data subjects' requests for further handling
- Provides a data protection impact assessment, a record of the processing activities and the services of its Data Protection Officer with regard to this processing operation

What are the roles and responsibilities of the representative?

- Encrypts the statements of support (after scanning those collected in paper form)
- Uploads the encrypted statements of support in the file exchange service
- Decides on the date of submission to Member States' competent authorities
- Handles under GDPR/EUDPR any data subjects requests received at that stage of processing.

Full information as regards the obligations of both joint controllers is to be found in the relevant joint controllership agreements

PLEASE NOTE:
You may also choose to submit statements of support collected using an individual online collection system as well as those collected in paper form, using your own means

References:

- Articles 4(3), 10 and 12 of the Regulation on the European citizens' initiative[120]

[119] Cross-reference link to Case scenario 2 on page 3
[120] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788

www.parlament.gv.at

16. What are the data retention time limits?

Statements of support:

Both the group of organisers and the Commission must destroy all statements of support signed for a given initiative (and any copies) by whichever of these dates comes first:

- **1 month** after the organisers submit the initiative to the Commission
- **21 months** after the collection period starts.

However, if you withdraw the initiative after the beginning of the collection period, the statements (and any copies) must be destroyed within 1 month after the withdrawal.

The national authorities called on to verify statements of support must destroy all the statements (and any copies) by **3 months** after completing this process.

Exceptions:

- if you are involved in any legal or administrative proceedings linked to your initiative, you may retain the statements of support (and copies) for longer than these time limits, where they are required for these proceedings.
- For initiatives, which have their collection period extended due to COVID-19 pandemic crisis[121], data retention periods are extended accordingly.

Email addresses:

The group of organisers and the Commission must destroy all records of email addresses by:

- **1 month** after withdrawing your initiative or
- **12 months** after the end of the collection period or
- **12 months** after submitting the initiative to the Commission.

However, if the Commission responds to a valid initiative with a formal communication, the retention period for the email addresses ends **3 years** after the communication is published.

References:

- Articles 19(5) to 19(8) of the Regulation on the European citizens' initiative[122]

[121] https://eur-lex.europa.eu/legal-content/TXT/?uri=uriserv%3AOJ.L_.2020.231.01.0007.01.ENG
[122] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788

17. Which national supervisory authority should you contact for issues relating to the processing of personal data?

By its nature, the process of collecting statements support in at least seven Member States is cross-border and **several data protection authorities** ('DPA') may be competent.

For all actors concerned, it is easier to deal with only one DPA, which is feasible under the concept of a **'lead supervisory authority' or 'LSA'** under the GDPR[123]. The lead DPA is defined as the supervisory authority of the Member State of the main establishment or of the single establishment of the controller.

However, **signatories** may lodge a complaint with the LSA or with the DPA of the Member State where they usually reside, their place of work or the place of the alleged infringement if they consider that their data is unlawfully processed.

References:

- Articles 55 and 56 of GDPR[124]
- List of Data Protection Authorities[125] in all EU Member States.

[123] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[124] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32016R0679
[125] https://edpb.europa.eu/about-edpb/board/members_en

18. Support and funding – what should you be aware of, when processing personal data?

As a group of organisers, you must indicate, for the European citizens' initiative public register and where appropriate on your campaign website, clear, accurate and comprehensive **information on the sources of support and funding for your initiative.**

Information to be provided on support and funding:

- The support and funding received from any source that exceeds EUR 500 per sponsor (this covers both financial support and support in kind)
- The organisations assisting it on a voluntary basis, where such support is not economically quantifiable.

Therefore, you need to **collect personal data of natural persons** which supported initiatives with amounts exceeding EUR 500, and namely:

- full name of sponsor
- date of donation
- amount of donation (exceeding EUR 500).

Timeline to provide information on support and sponsors:

This information needs to be provided in particular **at the time of registration** of a proposed initiative and **at the time of its submission** to the European Commission (when the required 1 million signatures have been certified), but should also be **updated every two months**. You should communicate these data to the European Commission via a dedicated form in your organiser account in view of its publication in the public register.

Rules and roles related to data protection:

As regards these data, the **representative of the group of organisers is a sole data controller**, and the European Commission plays the role of data processor while publishing this information in the register.

The processing of personal data of sponsors being natural persons is subject to the requirements of the GDPR[126] similar to those applicable to the signatories' data.

If they are natural persons, sponsors shall be provided with an **appropriate privacy statement** by the group of organisers at the time their data are collected. They should in particular be made aware by the organisers that their data will be published in the register.

Under the Regulation on the European citizens' initiative, **sponsors are entitled to object to the publication of their personal data** on compelling legitimate grounds relating to their particular situation, and to request the rectification of that data at any time.

References:

- Article 17 and Annexes II and VII of the Regulation on the European citizens' initiative[127]

[126] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32016R0679
[127] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788

www.parlament.gv.at

Data protection glossary

Central Online Collection System (COCS)	A secured IT system set up and operated by the European Commission under the explicit provision of Regulation on the European citizens' initiative[128] (Article 10). It allows for the collection (including by webforms and by eID) of statements of support, their storage and secured submission to Member States for verification, as well as the collection and further processing of signatories' email addresses.
Data controller	A natural or legal person or other body responsible for the personal data processing and that determines the purpose and means thereof. See also 'Joint controllers'
Data Protection Impact Assessment (DPIA)	An assessment of the impact of the envisaged processing operations on the rights and freedoms of data subjects. See Regulation (EU) 2018/1725[129], Article 39 and Regulation (EU) 2016/679[130], Article 35.
Data subject	A natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an ID number, etc. See also 'Personal data' and 'Sensitive data'
'EU Data Protection Regulation' (EUDPR)	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data[131].
File exchange service	An IT solution provided by the Commission to allow secure submission of statements of support to Member States for their verification and certification, operated using the existing Commission IT system S-CircaBC. This term is also used on this site with regard to the submission of statements of support collected on paper (instead of the term 'central online collection system' used in Article 10(1)(5) of the Regulation on the European citizens' initiative[132]).
General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 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[133].
Joint controllers	Where two or more controllers jointly determine the purpose and means of processing. A transparent arrangement is needed to determine their respective responsibilities regarding personal data processing. The essence of the arrangement shall be made available to the data subject. In the context of the European Citizens' Initiative, this relates in particular to the Central Online Collection System.

[128] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[129] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725
[130] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32016R0679
[131] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32018R1725
[132] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[133] https://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX%3A32016R0679

www.parlament.gv.at

Legal entity	In the context of the European Citizens' Initiative, a legal entity can be created for the purpose of managing the initiative. In such case, this legal entity shall be considered as a group of organisers or its members. It shall also replace the representative in its role of data controller.
Organisers (Group of)	Natural persons responsible for the preparation and management of a citizens' initiative throughout its lifecycle. The Regulation on the European citizens' initiative[134] provides that different data processing operations are managed by the group of organisers (notably: collection, submission for verification and destruction). When carried out by the group of organisers as a whole or its concrete members other than the representative, these data processing operations are deemed performed under the control of the representative.
Personal data	Any information relating to an identified or identifiable natural person ('data subject')
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Representative	A member (leader) of the group of organisers of a citizens' initiative, holding the function of data controller or joint data controller with regard to all data processing operations carried out with regard to personal data processed by the group of organisers Where this guidance refers to the representative of the group of organisers as data controller, it is to be understood as referring to a legal entity managing the initiative in case such entity has been created
Sensitive data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data or data concerning a natural person's sex life or sexual orientation. Also referred to as 'special categories of personal data'. 3. **'Sensitive data' - when do the signatories' data qualify as a special category of data?**[135]
Signatory	A citizen of the Union who has supported a given initiative by completing a statement of support form for that initiative; signatories are the main group of data subjects concerned by this guidance.
Statement of support	A declaration by which a signatory supports a European citizens' initiative, which can be either filled in and signed on paper, filled in online using a webform or signed online with an eID. In the first two cases, statements of support need to follow a model provided for in the regulation on the European citizens' initiative. In all cases, they contain a set of signatory's personal data.

[134] https://eur-lex.europa.eu/legal-content/TXT/?qid=1558082143592&uri=CELEX:32019R0788
[135] Cross-reference link to Question 3

www.parlament.gv.at