II

(Non-legislative acts)

REGULATIONS

COMMISSION IMPLEMENTING REGULATION (EU) 2019/1799

of 22 October 2019

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

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2019/788 of the European Parliament and of the Council of 17 April 2019 on the European citizens' initiative ([1]), and in particular Article 11(5) thereof,

Whereas:

(1) Regulation (EU) 2019/788 lays down revised rules on the European citizens' initiative and repeals Regulation (EU) No 211/2011 of the European Parliament and of the Council ([2]).

(2) Regulation (EU) 2019/788 provides that for the online collection of statements of support for registered citizens' initiatives, organisers have to make use of the central online collection system that is set up and operated by the Commission. However, to facilitate the transition, for initiatives registered under Regulation (EU) 2019/788 before the end of 2022, organisers may choose to use their own individual online collection system.

(3) Under Regulation (EU) 2019/788 an individual system that is used for the online collection of statements of support should have adequate technical and security features in place to ensure that the data are securely collected, stored and transferred throughout the collection procedure. The Commission should define, together with the Member States, the technical specifications to implement the requirements for individual online collection systems.

(4) The rules laid down in this Regulation replace those set out in Commission Implementing Regulation (EU) No 1179/2011 ([3]), which will therefore become obsolete.

(5) The technical and organisational measures to be implemented should aim to prevent, both at the time of the design of the system and throughout the collection period, any unauthorised processing of personal data and protect them against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

([1]) OJ L 130, 17.5.2019, p. 55.
([2]) Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative (OJ L 65, 11.3.2011, p. 1).
([3]) 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 (OJ L 301, 18.11.2011, p. 3).

(6) To that end, organisers should apply adequate risk management processes to identify the risks to their systems and to determine the appropriate and proportional countermeasures to reduce those risks to acceptable levels. Organisers should properly document the identified security and data protection risks and the measures taken to counter those risks, having regard to the security rules and requirements applied by the certifying authority. The security rules and requirements should be in line with Regulation (EU) 2019/788 and should be made available by the certifying authority upon request.

(7) Implementation of the technical specifications set out in this Regulation should be without prejudice to the obligation for the organisers to comply with the data protection requirements that follow from Regulation (EU) 2016/679 of the European Parliament and of the Council ([4]), including the possible need for a data protection impact assessment.

(8) The representative of a group of organisers or, as the case may be, a legal entity referred to in Article 5(7) of that Regulation are considered as data controllers under Regulation (EU) 2016/679 in relation to the processing of personal data in an individual online collection system.

(9) Organisers that introduce changes in their individual online collection system after the system has been certified should notify without undue delay the relevant certifying authority thereof if the change could affect the assessment underlying the certification. Before doing so, the organisers may seek the advice of the certifying authority to verify if the change may have such impact and thus should be notified.

(10) The European Data Protection Supervisor was consulted in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([5]), and delivered comments on 16 September 2019. The European Network Information Security Agency was consulted and provided comments on 18 July 2019.

(11) The measures provided for in this Regulation are in accordance with the opinion of the Committee established under Article 22 of Regulation (EU) 2019/788,

HAS ADOPTED THIS REGULATION:

Article 1

The technical specifications referred to in Article 11(5) of Regulation (EU) 2019/788 shall be as set out in the Annex to this Regulation.

Article 2

1. Organisers shall ensure that their individual online collection system complies with the technical specifications set out in the Annex throughout the collection period.

2. The organisers shall notify without undue delay to the competent authority of the Member State referred to in Article 11(3) of Regulation (EU) 2019/788, changes which are introduced in the system or in the supporting organisational measures after the system has been certified by that authority, when those changes may impact the assessment underlying the certification. Before doing so, the organisers may seek the advice of the competent authority as to whether the change may have such an impact.

([4]) 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 L 119, 4.5.2016, p. 1).

([5]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Article 3

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 1 January 2020.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 22 October 2019.

For the Commission
The President
Jean-Claude JUNCKER

ANNEX

1. **Technical specifications aiming at implementing Article 11(4)(a) of Regulation (EU) 2019/788**

The system shall implement technical measures to ensure that only natural persons can submit statements of support. The technical measures shall not require that more personal data is collected and stored than the one which is listed in Annex III to Regulation (EU) 2019/788.

2. **Technical specifications aiming at implementing Article 11(4)(b) of Regulation (EU) 2019/788**

Organisers shall put in place adequate and effective technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations, to ensure that the information provided on the initiative in the online collection system and as presented online to the public corresponds to the information published on the initiative in the register that is referred to in Article 6(5) of Regulation (EU) 2019/788.

Organisers shall make sure that:

(a) the information provided on the initiative in the online collection system corresponds to the information published in the register;

(b) the system presents the information on the initiative published in the register before the citizen submits the statement of support;

(c) security measures are in place to ensure that the data entry fields in the statements of support are presented together with the information on the initiative, in order to prevent the risk that statements of support are submitted on a different initiative through a misrepresentation of the initiative;

(d) the system ensures that after the submission the data in the statements of support are saved together with the information on the initiative;

(e) security measures are in place to prevent that unauthorised changes can be made to the information provided on the initiative in the online collection system.

3. **Technical specifications aiming at implementing Article 11(4)(c) of Regulation (EU) 2019/788**

The system shall ensure that statements of support are submitted in accordance with the data fields in Annex III to Regulation (EU) 2019/788.

The system shall ensure that a person can only submit a statement of support after having confirmed that it has read the privacy statement of Annex III to Regulation (EU) 2019/788.

4. **Technical specifications aiming at implementing Article 11(4)(d) of Regulation (EU) 2019/788:**

4.1. **Governance**

4.1.1. The group of organisers shall nominate a security officer who shall be responsible for the security of the system and the secure transmission of the collected statements of support to the competent authority of the responsible Member State. The security officer shall oversee the information assurance processes and the technical and organisational security measures to ensure the secure collection, storage and transmission of the data provided by signatories.

4.1.2. Organisers may ask the national competent authority referred to in Article 11(3) of Regulation (EU) 2019/788 to provide the applicable security rules and requirements for the certification of individual online collection systems. The competent authority shall provide the security rules and requirements, as a rule within one month upon having received the request. The applicable security rules and requirements shall be in line with existing appropriate national or international security standards.

4.1.3. The security rules and requirements for the certification of the system shall address the risks defined in section 4.2 and have regard to the specifications in section 4.3.

4.2. **Information Assurance**

4.2.1. Organisers shall use risk management processes to identify the risks linked to the use of their systems, including for the rights and freedoms of signatories, and to determine the appropriate and proportional measures to prevent and mitigate the impact of incidents affecting the security of the network and information systems that they use in their operations.

The risk management process shall focus particularly on the risks related to the confidentiality and integrity of the information in the system. These risks can be the result of threats, including:

(a) user errors;

(b) system/security administrator errors;

(c) configuration errors;

(d) malware infection;

(e) accidental alteration of information;

(f) information disclosure or leaks;

(g) software vulnerabilities;

(h) unauthorised access;

(i) interception or eavesdropping of traffic;

(j) data protection risks.

4.2.2. Organisers shall provide documentation showing that they:

(a) have assessed the risks of the system;

(b) have determined appropriate measures to prevent and mitigate the impact of incidents affecting the security of the system;

(c) have identified the residual risks;

(d) have implemented the measures and verified their implementation;

(e) have provided the organisational means to receive information on new threats and security improvements;

(f) comply throughout the collection process with the certification requirements laid down in Article 11(4) of Regulation (EU) 2019/788, including having in place the necessary processes to ensure this.

4.2.3. The measures to prevent and mitigate the impact of incidents affecting the security of the systems shall cover the following domains:

(a) human resource security;

(b) access control;

(c) cryptographic controls;

(d) physical and environmental security;

(e) operations security;

(f) communications security;

(g) system acquisition, development and maintenance;

(h) information security incident management;

(i) compliance.

Application of these security measures may be limited to the parts of the organisation that are relevant for the online collection system. For instance, human resources security may be limited to any staff that has physical or logical access to the online collection system, and physical/environmental security may be limited to the building(s) hosting the system.

4.2.4. Where organisers make use of a processor for the development or deployment of the online collection systems or parts thereof, the organisers shall provide documentation to allow the certifying authority to ascertain that the necessary security controls are in place.

4.3. **Encryption of data**

The system shall provide for the following encryption of data:

(a) personal data in electronic format shall be encrypted when stored or transferred to the competent authorities of the Member States in accordance with Regulation (EU) 2019/788, the keys being managed and backed up separately;

(b) adequate standard algorithms and adequate keys shall be used in line with international standards (such as the ETSI standard). Key management shall be in place;

(c) all keys and passwords shall be protected from unauthorised access.